CISOs INVESTIGATE:

ENDPOINT SECURITY

Peer-authored Research

SECURITY CURRENT

Sponsor

Gold

Table of Contents

Introduction

The rise of the cloud and mobile computing has rapidly changed the nature of enterprise cybersecurity. The old paradigm, where all work was done behind a company firewall, has been breaking down.

Employees work not just at the office, but also on the road and at home, on mobile devices and on their own personal computers. They're no longer using a limited stack of enterprise applications. Instead, they increasingly require access to a wide variety of apps, cloud services, and new communication platforms.

The result is a much larger attack surface, one that is hard to protect with traditional approaches – and one that is growing faster than ever before as users adopt new types of devices, new applications, and new services. Often, companies don't even know all the tools that their employees are using.

At the same time, the potential threats that enterprises are facing have grown significantly in variety, capabilities, and size. Today, companies are beset not only by hackers looking for a thrill, but also by nation-state actors, hacktivists, corporate spies, small time crooks, and large criminal organizations. These adversaries have at their disposal an ever-growing collection of open-source hacking tools and commercial software. There are also online services offering ready-to-go ransomware campaigns.

Meanwhile, with zero-days and other stealthy attacks, enterprises have less and less time to spot intrusions and take steps to contain them.

Today's malware, once it gets a foothold, can spread quickly. Once in an enterprise, attackers can secretly infiltrate more and more systems and collect more and more data. Or they can quickly and immediately launch large-scale ransomware attacks that can take down large numbers of computers and and lock up enterprise data.

As a result, the damage caused by the attacks has also been increasing at a staggering pace, with ransomware alone reportedly crossing the $1 billion revenue threshold in 2016.

In this new age of cyberwar, endpoint devices are the front line.

Traditional antivirus protections are no longer enough. Enterprises of all sizes, and all industry segments, are now looking for better solutions.

In this report, leading security experts examine the new tools that they have at their disposal, including next generation endpoint protection, which may include sandboxing and micro-isolation, and detection solutions built around behaviors, heuristics, and artificial intelligence and machine learning.

They review the business requirements that went into making their technology decisions and how well the solutions actually worked out in practice.

They also offer advice to other security executives facing similar problems.

About CISOs Investigate

The value of peer input cannot be overstated. Authored by leading Chief Information Security Officers, CISOs Investigate is an ongoing series that offers first-hand insights to security leaders as they make business-driven risk and technology decisions.

CISO Contributors

CISOs Investigate: Endpoint Security includes the viewpoints of 13 security leaders who have deployed or are looking to deploy third-party solutions. This report replaces the ad hoc, often informal and time-consuming processes of personally gathering peer insight. Spanning verticals, the CISO contributors share real-world use cases and provide guidance.

Participating Endpoint Solution Providers

The report includes responses to Requests for Information (RFIs) submitted by 19 vendors. Developed by CISOs, the RFI criteria highlight the most important technology aspects of the potential solutions. To qualify, a solution must protect against malware techniques other than signatures as well as safeguard against memory exploitation and support multiple systems.

Participating Companies

Absolute Software
Bromium
Carbon Black
Code42
Comodo
CounterTack
CrowdStrike
Cybereason
Cylance
Endgame
ESET
FireEye
IBM
Kaspersky
Malwarebytes
McAfee
Palo Alto Networks
Red Canary
SentinelOne

LEAD WRITER:

University of Wisconsin-Madison
Bob Turner
Chief Information Security Officer

CONTRIBUTORS:

ADP
V.Jay LaRosa
Vice President, Global Security Architecture

American Bureau Of Shipping
Mike Davis
Chief Information Security Officer

ASRC Federal
Darren Death
Chief Information Security Officer

Freeport-McMoRan Inc.
Vaughn Hazen
Chief Information Security Officer

Madison Gas and Electric
Max Babler
Director, Security, Infrastructure and Operations (CISO Equivilant)

National Life Group
Andrew Speirs
Chief Information Security Officer

The Ohio State University
Helen Patton
Chief Information Security Officer

Oppenheimer & Co.
Henry Jiang
Chief Information Security Officer

Perdue Farms
Tunde Oni-Daniel
Head of Information Security

RWJBarnabas Health
Hussein Syed
Chief Information Security Officer

Western Digital Corporation
Geoffrey Aranoff
Vice President, Information Security

Wisconsin Department of Health Services
Shane Dwyer
Chief Information Security Officer

Graphics are original images based on data from the RFI responses.

A CISO LOOKS AT THE CONTINUING EVOLUTION OF ENDPOINT SECURITY

Bob Turner, ***Chief Information Security Officer, University of Wisconsin-Madison***

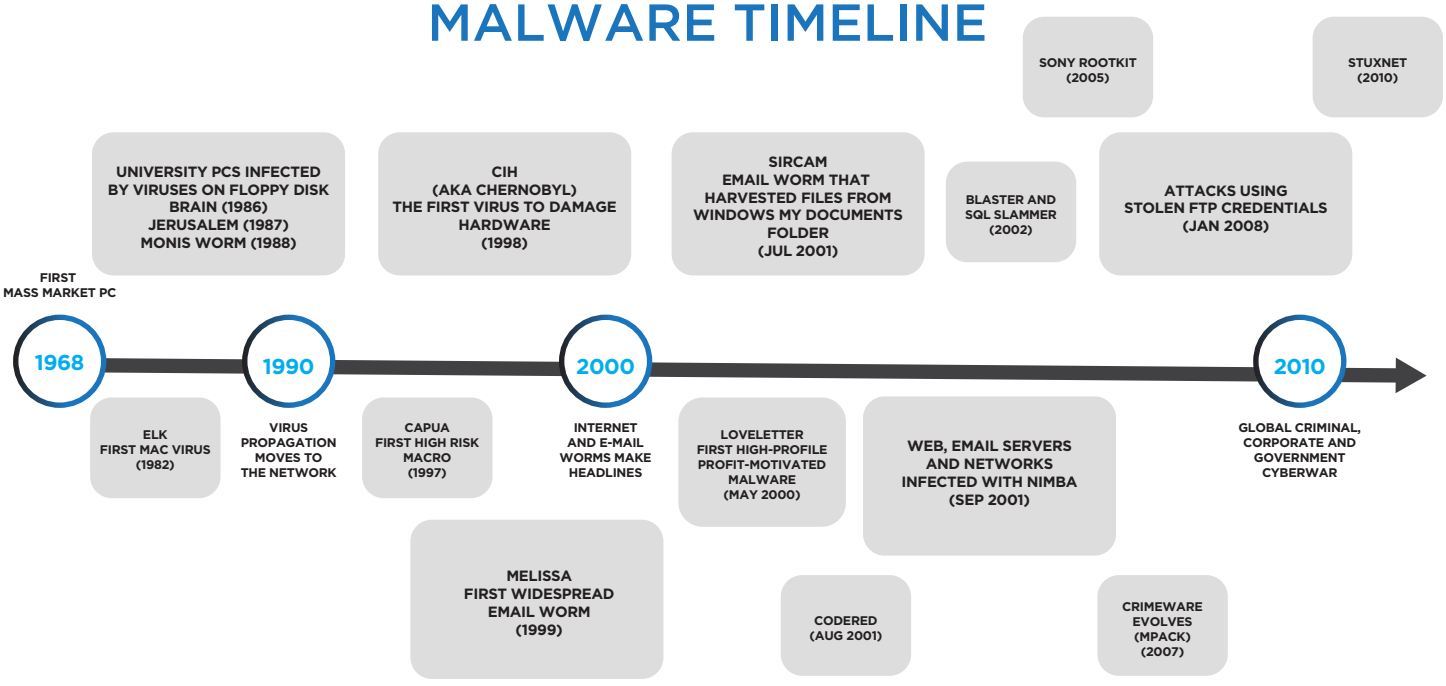
Endpoint security has come a long way since it first became an important issue for companies in the mid-1980s, when they began to struggle with viruses and malicious code transferred between computers on floppy disks. Which endpoint security tool was actually the first may be a hotly debated topic. Since then, there has been a proliferation of antivirus tools with startups and enterprises devising ways to combat Trojans, worms, viruses and other malicious code.

The attackers became cleverer and found other ways to antagonize administrators and users with boot sector viruses. Then they moved on to macro viruses targeting Microsoft products, email worms taking out mail servers, and network worms that indiscriminately attacked unprotected endpoints. We gave this malware interesting names like Brain, Blaster, Code Red, Chameleon, Ghostball, Happy99, ILOVEYOU, Nimda, Ping Pong, SQL Slammer, Stoned, and Welchia. The malware attacked all forms of personal computers, data and web servers, printers, handheld personal digital assistants, digital photo frames, and it continues today to target all manner of Internet connected digital devices, up to and including your refrigerator!

Playing the catch up game, network and information security professionals were caught in a never-ending cycle as they tried to address the ever-changing adversarial tactics. Defensive tools evolved, and architects layered them with strategies that focus on data protection. Over the past 10 to 15 years, the cybersecurity industry has moved toward technologies now called "advanced threat protection."

The adversaries evolved as well. Criminal syndicates used the malicious tools of the trade to steal marketable information or extort money. Nation-states and cyber terror syndicates found easy ways to advance their causes with viruses and code that defaced websites and locked up data with ransomware. Attackers continued to increase the scope and volume of data they were able to extract and exploit. The cyber adversary got smarter and the Chief Information Security Officer (CISO) had to sprint to get ahead. But even with the best-of-breed intrusion protection technologies blocking threats from entering the network in the first place, the processes and tools used in securing network endpoints remain a vital link in the information security chain.

MALWARE TIMELINE



WHERE DOES ENDPOINT PROTECTION FIT IN THE CYBER EVENT AND INCIDENT RESPONSE LIFE CYCLE?

The National Institute for Standards and Technology (NIST) describes the Cybersecurity Framework as a series of activities that manage risk. As shown in the graphic , cybersecurity teams improve security by:

1. Identifying corporate data and assets,
2. protecting assets by applying the appropriate security controls,
3. detecting threat behaviors as they occur,
4. responding quickly to limit damage that impacts data availability, integrity and confidentiality, and
5. recovering the systems and endpoints in time to fight the next threat actor's tools and techniques.

Many CISOs are adopting the framework as a set of operational imperatives – those activities we must do! Simplified, these activities include:

- Know where your data is – and where the backups live – test the data security controls frequently
- Tune surveillance tools to sound the early alert
- Monitor for Indications of Compromise (IOCs) as a constant activity
- Understand what normal behaviors means and look closely at critical components
- Monitor privilege escalation for early warning of insider threats
- React quickly!!! You may only get one chance…

NIST CYBERSECURITY FRAMEWORK INCIDENT RESPONSE CYCLE

IDENTIFY	PROTECT	DETECT	RESPOND
ENDPOINTS ✓	Block high risk websites and isolate malware infections	Known Bad Domains	REGULAR STATIC ANALYSIS ✓
Data	Segmentation and isolation of High Risk data	EXPLOITS ✓	DYNAMIC ANALYSIS ✓
USERS ✓	VERIFY USERS ✓	MALWARE ✓	STUDY EXPLOITS TO LEARN NEW TECHNIQUES ✓
Applications	BLOCK KNOWN BAD APPLICATIONS ✓	Command and Control Traffic	UNDERSTAND MALWARE TECHNOLOGIES ✓
SaaS	Limit Services	Malicious Websites	Engage Machine Learning
Cloud Infrastructure	LIMIT TO STANDARD BUILDS ✓	REVOKE COMPROMISED OR STOLEN CRENDENTIALS ✓	Advanced Anomaly Detection
MOBILE DEVICES ✓	Control sharing		BEHAVIOR ANALYTICS ✓

CISOs and their security teams should take these activities, extract the behaviors that specifically impact endpoint security and create a nice checklist of things to do that tie to endpoint security as shown (highlighted in blue) in the graphic.

VARIATIONS IN ENDPOINT THEORY

Endpoint detection and response (EDR) technology addresses the notion that most endpoint systems or appliances are potential launch pads for cyberattacks. Aficionados believe that these security products should be more than antivirus support tools – and considering those same supporters claim antivirus is yesterday's news, they believe endpoint protection should provide everything from checks on file reputation to behavioral analysis and integrate artificial intelligence (AI) and advanced machine learning. They rightfully believe the growing attack surface associated with mixing personal and corporate mobile devices, multiplied with the wide variety of Internet of Things (IoT) devices and sensors, should drive corporate programs to embrace continuous endpoint discovery. 24 by 7 monitoring of devices with assessment and prioritization of vulnerabilities will significantly reduce endpoint attack surfaces.

Another approach is endpoint protection platforms (EPP) that combine anti-malware, personal firewalls and manage ports and devices. These are typically managed at a central console based on enterprise policies. Endpoint protection platform vendors tout their products as complete packages that address everything from assessing vulnerabilities to managing mobile platforms to data loss prevention. Gartner estimates revenue in this market in the low $3 billion range and projects that it will continue growing slowly, noting that emerging vendors are pushing solutions that are not signature-based as a defense against the fast moving threat landscape.

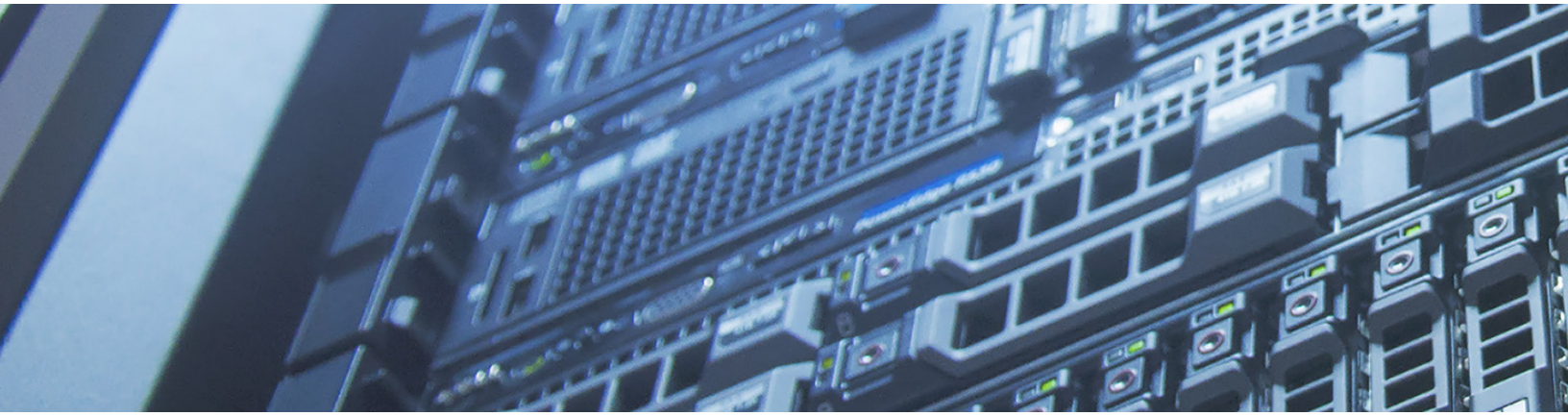
What I want is an endpoint protection platform that flashes a warning when your users are about to execute malicious code or are falling victim to a social engineering attack by pressing the wrong key or accessing a malicious website – accompanied by the sound of my third grade teacher screaming "Bobby (insert your name here), you had better not do that!" – followed by a period of detention in the principal's office if they do not heed the warning.

There are also those who advocate employing multiple solutions, combining older signature-based tools with whitelisting and trust modeling.
Finally, what you do with the malware once detected is also a hot debate. Do you detonate and analyze at the point of discovery? Or do you deny binary files that execute from odd locations on the endpoint such as the Recycle Bin and try to detect code that is trying to mess with basic functions of the operating system? Do you employ multiple tools from competing vendors and see which common binaries are lurking in the corners?

WHAT ABOUT THE INTERNET OF THINGS?

There is a strong cyber hygiene argument to be made when addressing the Internet of Things. Of primary importance is the device itself. From the initial power-up, IoT devices start to talk to their neighbors and exchange information that may cause calamity down the road. Since many IoT endpoints do not have any endpoint security solutions available, they often are placed outside of a defined physical security perimeter. In these cases, knowing what that power-up data exchange is supposed to look like is important. Security controls that focus on encryption, device authentication, key management, VLAN segregation, and code signing can go a long way to ensuring a more secure IoT environment – unless, of course, speed, deployment agility and cost are important factors for those developing or deploying the endpoints.

The Embedded Microprocessor Benchmark Consortium notes that engineers and developers are currently developing the next wave of technologies for IoT environments. This means billions of new IoT devices are coming on board—devices that are a challenge to secure against the many threats that existing systems may already be defended against. To meet the threat, an end-to-end and systems-based security approach is needed. Developers and engineers must create solutions that engage numerous hardware and software, algorithm and protocols, lifecycle and process challenges. Unfortunately, secure development of IoT has not always been a priority for application developers who are typically concerned that implementing security functions within their IoT devices will hurt performance and lower battery life.



RECOMMENDATIONS TO PEERS

From my (Bob Turner's) "one among many" CISO perspective, I need to continue to focus my efforts on an endpoint security strategy based on available and scalable technology while I continually seek to understand the use case diversity found in higher education. I am sure the other CISOs who assisted in development of this report and those in the cybersecurity community at large will be worried about endpoints in their industry vertical well into the future.

In my reading of *Measuring and Managing Information Risk* by Jack Freund and Jack Jones, I learned (well, actually I re-learned) that the components that make up information security risk constantly evolve. The CISO needs to set strategic and tactical priorities by differentiating between the objective and the subjective data our tools and industry experts provide us. Oddly enough, industry experts tend to over-prescribe on the type and amount of data the CISO needs. The data provided by many of today's vendor-advocated tools tends to skew the reader toward their products. When tuned to match your enterprise, your tools are likely to need information that is more precise. Moreover, while the results vary, they need to give you the true picture of what they see in your environment.

At the University of Wisconsin-Madison, our distributed IT organizations sometimes choose a solution that fits their needs and budgets while centrally supported endpoint solutions are limited to just a few. The Office of Cybersecurity is currently evaluating three separate endpoint solutions, one of which has been in our architecture for a number of years. All three yield useful indications and metrics and all come from industry leading products. The diversity found in our major research university environment's technology, operating procedures and business cases will drive which tool, or tools, will remain after the bake-off is over. We expect to have results and additional information available in late 2017. The harder issue to deal with is whether such diversity in solutions is valuable to address the use cases or whether it is simply adding noise. Performing proof of concept assessments and pilot programs helps the CISO determine what is best for their enterprise.

Three key questions a CISO must consider are ease of deployment and operation, data provided, and scale and cost:

- Does the endpoint security solution fit requirements for monitoring all or most of your technology; and can it be deployed easily by users and operated without too many clunky Knowledge Base articles?
- Does the tool give you reasonable information to determine usefulness and to address the current state of the attacker's tactics, techniques and procedures?
- And, finally, can you afford to buy the endpoint tools all at once under an enterprise license or are you going to buy piece-by-piece so you can easily account for the business unit cost and pass the bill on to your customers?

TO SUM IT ALL UP…

When choosing an endpoint security solution, you need to be prepared to live with it for two to five years. Keeping up with the CISO next door has merit, but ensuring your selection adds value to your users' experience is key to your success. I recommend looking at your current tools and listen to what they are telling you. If you get metrics, look at them and validate the information they provide. If you have endpoint-related risk exposure (i.e., you just got hacked) or your tool does not give you anything useful, consider whether you need to look elsewhere.

Technology Overview

Key Considerations

Among the CISOs who contributed to this report, several significant considerations were voiced as important to the selection of an endpoint security solution. Key among those considerations is the ability to have the solution present a common picture – the so-called "single pane of glass" that shows a clear picture of the threats and how they can be addressed.

CISOs agree that solutions need to demonstrate how the endpoint solutions and sensors add to or improve defense-in-depth alongside the other cyber tools in their tool belt. Other key considerations for endpoint security features that CISOs desire are:

- Collect and preserve forensics data
- Process integrated threat feeds
- Allow security managers to "set and forget" the minimum security baseline
- Provide alerts to changes in critical configuration items
- Support mobility considerations
- Focus on prevention versus detection
- Manage resource intensity
- Flexible for today's variety of attacks and adaptable for future threats
- Have a minimally intrusive footprint and resource usage
- Offer tools to help determine effectiveness of the solution

CISOs are concerned that new endpoint solutions might not be easy to integrate with the enterprise level security stack. New security teams or those with new members have so many different sensors and tools that onboarding of the solutions and orientation of the technologists now takes much longer to get the teams and tools operating at optimal speed and effectiveness. Tools with unneeded capability in the form of additional "bells and whistles" distract from dealing with actual risk. Teams need to focus on evaluating the security issues that require eyes and ears on actual risk barriers, not tackling commodity malware issues that change the team's focus.

Endpoint Security Core Features

Finding the right mix of features within your endpoint security solution is important. Knowing how endpoint security fits in with your information security strategy and architecture will help determine the best solution and will help you control costs and feature creep as you consider other essential security controls and countermeasures.

Across industries, you see breaches occurring at an alarming rate. In the old days, you looked for a frontal assault on your Internet pipes and servers. Today, most attacks originate from endpoints and the majority of large breaches start with phishing attacks.

V. Jay LaRosa, Vice President, Global Security Architecture, ADP

ISSUES TO CONSIDER:

- Virus and malware signature management can be an ongoing activity that will overwhelm you. Choose a vendor and solution with the right intelligence resources and the ability to home in on the right signatures for your technology, instead of one that overwhelms the system with too many signatures. Instead of opting for one that simply matches signatures, consider solutions that provide real-time analysis of the malware and then choose a remediation strategy for the remaining unmatched signatures. Finally, ask the vendor how they calculate a risk score for the endpoint after signature-based remediation takes place.
- Your choice of endpoint security tools should include the ability to vary the scan intervals and therefore change the total time to complete scans. Anything that cannot be accomplished within your network or out-of-band network's resources fails the test.
- Is the vendor giving you the ability to adapt to the effects of polymorphic viruses? Heuristics capability should be in the requirements or desired feature set and include the ability to do work while the heavy thinking and learning takes place in the background. This helps reduce false positives and the extra work they generate.
- Sandboxing is not new. Choose a reliable vendor that understands and provides the ability to access a cloud-based resource or an on premise virtual environment to perform malware analysis. This tells you what the malware is capable of before you choose how to blow it away!
- Don't forget to look at the affordability of the solution in terms of cost per seat, its suitability and its effectiveness.

Once you sort through all of the hype words like breakthrough, first in class, market leading, seamless, most advanced, and award winning, feel confident that cybersecurity solution vendors are happy to provide us with additional features. Among the "new and really cool" features, you will find artificial intelligence, advanced analytics, cloud infrastructures, crowd sourced threat intelligence, and my favorite – the "single pane of glass"! Then you need to look for the differentiators. Does the vendor offer coverage for all your platforms? Can the tool recognize financial and online banking transactions? How fast and easy is the deployment process? Will the tool block file-based and memory-based attacks? The list can go on and on and should include the questions we ask in the Request for Information later in this paper.

A Deeper Dive into Endpoint Security

Good CISOs are backed up by superior professionals. At University of Wisconsin-Madison, I am fortunate to have Allen Monette as one of my Senior Security Analysts and the leader of our Monitoring and Forensics Team, and John Nagler who, while new to the team, has pressed himself to understand the intricacies of novel solutions like using vulnerability scanners as an endpoint patch scanner. I asked Allen and John to provide their perspective to the strategic and tactical aspects of endpoint security. These are their thoughts:

ALLEN MONETTE

Good endpoint security needs to accurately detect attacks and effectively stop them. It must be unobtrusive to end users during normal operations, yet provide useful communications about malicious activity to both end users and system administrators. It must be scalable and resilient, and cannot cost more to own and operate than it would cost to clean up after an endpoint is infected.

Strategically, endpoint security should complement and integrate with several key areas of an overall security strategy. Most obviously, endpoint security and endpoint management mesh together closely enough that it is often difficult to tell which one is which. The most commonly used compliance standards, such as PCI-DSS and NIST, have already incorporated a requirement for endpoint security.

Good security strategy will be aware of the standards required for your industry and will favor endpoint security solutions that help meet those compliance goals. Endpoint security solutions also tend to generate lots of useful data that makes them well suited to integration with security operations center (SOC) activities and should augment general help desk processes. Perhaps less obviously, endpoint security strategy and security awareness activities should be planned to complement each other. Phishing awareness campaigns, for example, are an effort to train end users to be a part of your overall endpoint security solution. Endpoint security strategy needs to be forward looking, always aware of changes in the threat landscape and technology trajectory, even if the endpoint security tools deployed struggle to keep up. At University of Wisconsin-Madison, we are aligning our strategic direction on endpoints with increased use of virtualization and cloud technologies, although our current toolkit is a bit behind this curve.

With the plethora of security tools on the market that claim benefits for endpoints, it's likely that your current toolkit has a few duplicates in it. Some level of tool duplication is impossible to avoid and is even desirable. Consider, for example, the additional granularity and defense-in-depth available to you with both network and host-based firewalls or intrusion detection and prevention solutions running in your enterprise. Newer or "next generation" endpoint security tools take this synergy further by actively sharing malware information between network firewalls and endpoint agents. Another key consideration for when duplicate tools are worth maintaining is coverage for unique environments such as scientific instruments, medical devices, or auto-scaling services built on infrastructure-as-a-service cloud providers. Running several different tools in a bake-off is yet another reason to have duplicate tools, at least for a limited time.

Duplicate tools, even when they are filling a useful role as in the above examples, must be carefully scrutinized for a good return on investment. A unique tool for a unique environment that comes at a unique price will only be worthwhile if it can reduce risk for the environment significantly.

JOHN NAGLER

In a world where zero-days constantly make the news cycle, it is easy to forget that Symantec found that less than 1 percent of all vulnerabilities in 2015 were zero-days (6452 CVEs, 54 zero-days). The Verizon Data Breach Report for 2016 echoed those findings stating that the most common exploits came from 2007, followed by 2011—not exactly zero-day exploits.

With that in mind, endpoint security can now be handled in new and creative ways that are easily accessible to the market. One example of a tool to assist with endpoint security–and specifically the method for compromise mentioned in the security reports–is an endpoint patch scanner. These tools monitor and report on the current level of operating system on any endpoint on which they are installed—be it a laptop that almost never enters the network or a virtual machine that is continually available in the datacenter.

These tools provide asset reporting and verification of patch level across all endpoints on which they are deployed. These tools typically use minimal resources and help to verify that the critical vulnerability that was patched three months ago will not be the avenue that compromises your network. This issue can be addressed somewhat with a central vulnerability scanner; however they often require scan windows and known and working credentials to every endpoint that needs to be scanned, in addition to endpoints that are constantly connected to your network. The new endpoint based agents get around those challenges and report back to a central location making management of both the tool and the endpoints easier for your staff.

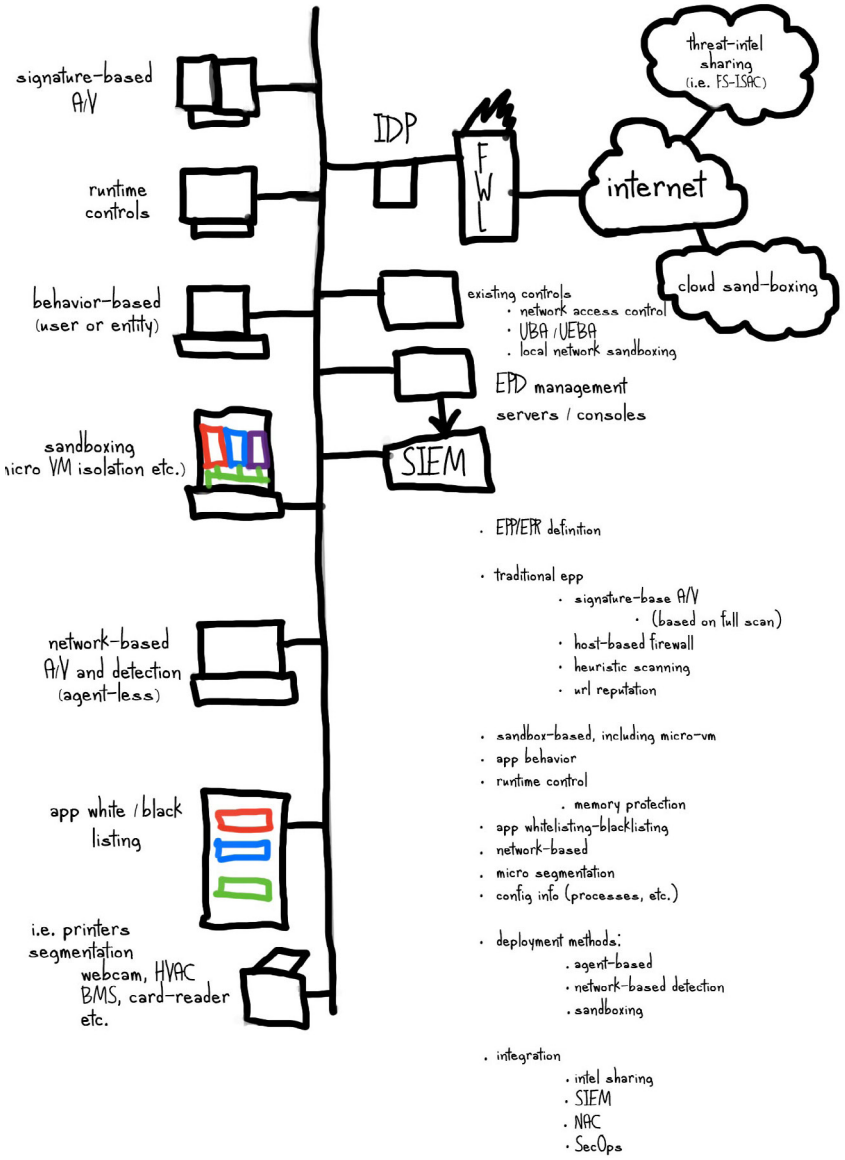
Using these unconventional endpoint scanners is not a silver bullet to stop all OS level vulnerabilities. They are, however, a great step toward verifying the updates are being applied to all endpoints and confirming that the very dangerous bug from 10 years ago will not be the one that bites.

What's in Your Architecture Drawing?

The endpoint protection architecture includes multiple components within a platform that provides security capabilities to protect servers, workstations, smartphones and tablets. CISOs and network architects should agree on the placement of endpoint security components to enable the most secure and efficient use of the selected security controls. The figure below is the raw result of an online collaboration showing contributing CISOs' concerns. The whiteboard drawing shows how some of the more common features interrelate with and impact the quality of security services provided to connected and mobile network components.

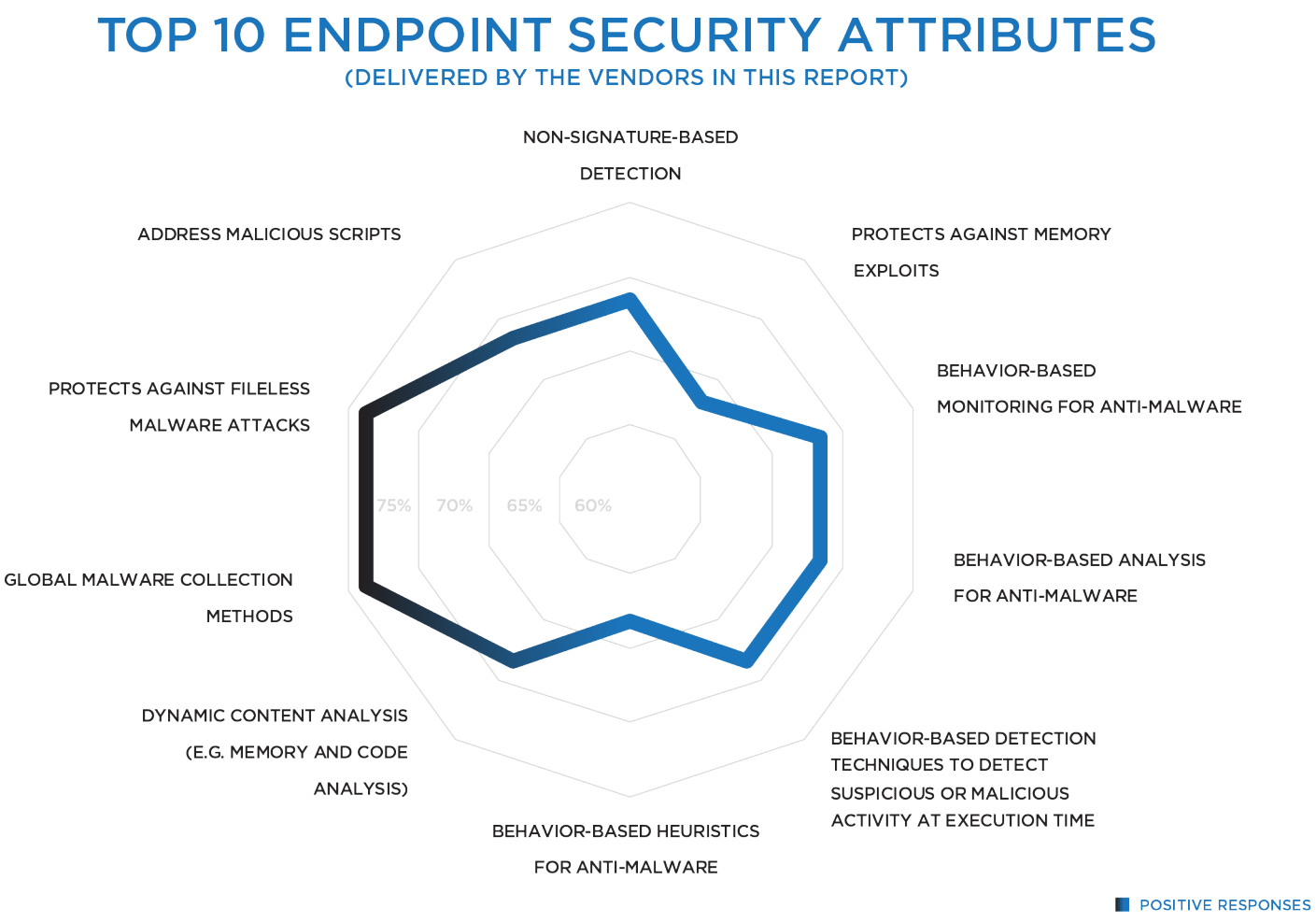
IMPORTANT ARCHITECTURAL CONSIDERATIONS INCLUDE:

- Incorporation of signature based antivirus and agentless network based antivirus scanners
- Use of sandboxing for testing in an operationally representative environment – whether on premise or cloud based
- Application whitelists and blacklists
- Segmentation (or micro-segmentation) for IoT components (i.e., printers, cameras, card access systems, building management systems, etc)
- Integration with other security components (SIEM, NAC, cyber intel, SecOps/DevOps)



What Do Solution Vendors Provide?

We asked a variety of solution vendors to tell us what they can provide based on a list of attributes a group of the contributing CISOs agreed were important. In addition to the operating environments (cloud and on-premise) and the spectrum of endpoint operating systems, the CISOs wanted to understand how vendors go about collecting data (logs, activity and historical), and how data is managed (e.g. local collection, central collection, polling, trigger based), and how the status information and metrics are presented. We then asked how they addressed nearly 40 attributes ranging from signature management to patch management to dynamic content analysis to forensics. The graph shows the percentage of responding vendors for the top ten security attributes.



What's in Your Minimum Security Baseline?

Establishing a minimum security baseline (MSB) helps to quantify the effort needed to set security configuration items and manage an endpoint client profile. CISOs should have a documented MSB for PC, laptops, etc., including Windows and Linux. Internet of Things endpoints need to be included, although it is much more difficult to determine which is by design of the device and which can be considered best practice for the type of IoT component in your architecture. Whichever security strategy or tactical plan you chose to operate within, endpoint security must be a key feature in your organization's baseline. Start with the intelligence – what are the threat feeds telling us and how is the information processed at the endpoint? Next, what configuration information does the solution harvest and display? Does the information support maintenance of a minimum security baseline?

These tables are provided by Mike Davis, CISO at American Bureau of Shipping, and represent related methods and strategies for maintaining a minimum security baseline at the endpoint. Many of these security controls issues and components elements can be part of a delivered endpoint security solution.

METHODS	WEAKNESS VULNERABILITIES AND THREATS	POTENTIAL MITIGATIONS
Use HIPS (re: a host IPS)	Network IDS / security tools address	Use a host IPS to complement network IPS, at least on critical systems
Use Anti-Exploitation Features	Addressed by other AV solutions	Enable MS' EMET
"Boot-Proof" Logon	Don't allow users to bypass logon scripts, start-up programs	Use BIOS to prevent booting from other than hard drive and password protect BIOS
Show file extensions	Allows user to see if an executable is blocked	(continue to block executables as email attachments)
Windows FW is on	Windows FW is on for Public and Private connections but not domain connections, would suggest turning on FW for all connection types	Test in development environment, then deploy
Disable Windows Script Host	This would require testing, could impact applications	Test in development environment, then deploy
Disable Windows PowerShell	PS should be disabled, only a small percentage of users need it	Test in development environment, then deploy

METHODS	WEAKNESS VULNERABILITIES AND THREATS	POTENTIAL MITIGATIONS
Switch off unused wireless	This would require some user education if we did disable unused wireless. Some systems have physical switches and others can be disabled via software	Minimizes remote connections unless user actively turns them on; provide user training on process for activating a wireless connection
Deactivate AutoPlay	Disabled due to an autorun attack years back	Validate setting is still disabled (new systems may have it enabled)
Monitor for host profile changes	Use MS host profile compliance feature	Actively monitor centralized host logging files
Group Policy Object (GPO) settings	Mitigate stealing passwords from memory (mimikatz)	Updating to Windows 8 or 10 makes this much more effective
Windows remote desktop protocol (RDP) – lock down	For example, Crysis malware is using compromised credentials for RDP computers	A common threat vector
Limit shared folders	Compartmentalize as much as possible. Disable files running from AppData/LocalAppData folders.	Minimize the spread of malware

Other client based controls the CISO should pursue include those items in the table below. These items go beyond that implemented in most endpoint security solutions.

METHODS	WEAKNESS VULNERABILITIES AND THREATS	POTENTIAL MITIGATIONS
Secure Backup / not effective (or partially in place)	Backup images poisoned (malware already installed); backup credentials stored on endpoint; backups stored in cloud, but if entire enterprise is encrypted, cloud backup is infeasible	All devices covered. Backups stored offline (onsite and offsite). Periodically test restore. Automatic back-up validated - does not contain malware
Patching effectiveness / weak or ad hoc ITAM / CMDB	Ransomware will leverage entry vectors that zero-days and one-days do, or don't rely on vulnerability exploits to begin with.	Automated / virtual patching. Vulnerability prioritization. Effective CMDB / release management. Actively monitor threat intel for zero-days / prioritize patching.
Lock down end user devices / no process or ineffective	Using local backup administrators' accounts. Service accounts are increasingly being used by adversaries, and these cannot be removed without breaking their respective service(s).	Limit local admins (all types), tightly control exceptions, block local executables install. No user boot bypass. Log activity for any changes to service accounts.

METHODS	WEAKNESS VULNERABILITIES AND THREATS	POTENTIAL MITIGATIONS
Effective antivirus / not effective or integrated	Ransomware markets and RaaS ensure every piece of ransomware ever launched in a campaign has a 1-off unique signature/ hash. Heuristic and behavior (including detonation chambers) are bypassable via evasion and persistence techniques routinely used by malware.	Both host and network AV. Behavior (and reputation) based as primary, in combination with signature based (which is hard to keep up-to-date). Integrate with SIEM
Password policy and operations / not audited or enforced	MFA/2FA is a solid recommendation when it comes to confidentiality, but does not prevent an end user from authenticating to an email application then opening an attachment or clicking on a malicious link and becoming infected via that vector.	Password and privileged account management (PAM) policy with automated enforcement. Conduct periodic audits. Use MFA for sensitive devices ('crown jewels')

Selling to the C-Suite

CISOs are now engaging in conversations with other C-suite leaders at the same level of intensity that they have historically had with department directors. The simple fact is that today, the CISO needs to be able to engage and influence the Chief Executive Officer (CEO), Chief Operations Officer (COO), Chief Financial Officer (CFO), Chief Technology Officer (CTO) and Chief Risk Officer (CRO) to support the most effective and efficient endpoint security solutions as part of the security stack.

Articulating the benefits of security solutions must include supporting the business needs of the company. That means that CISOs need to be able to speak about brand management, productivity, intrusiveness of the solution into the lives of the staff, and total cost of operation. They also must be able to translate CISO-speak about prevention versus detection, integration with other security tools in the stack, sources and use of cyber threat intelligence, and addressing protective measures for corporate data into language understandable by the executives.

Cybersecurity is not a revenue center in most businesses. Funding endpoint security requires that the company already have a cybersecurity strategy and include cybersecurity protections at or near the top of the list, with linkage to business objectives and return on investment. Resource sponsors want to know the risk exposure if they do, or do not, make the investment in cybersecurity tools like endpoint protection. CISOs need to bring answers to the CIO, CEO, CFO, CTO or CRO and other interested members on the top floor. They want to know how this investment reduces potential loss, how the solution fits within the layered cyber defenses and reduces risk, what compliance issues are addressed, and what staffing impacts will be. Remember, they are pulling for a reduction in the bottom line so additional staff need to fit within the overall reduction of cost and loss expectancy.

Does the Board of Directors regularly review your cybersecurity plan? Does your C-suite have the ammunition they need to represent the cost of detective and preventive tools like endpoint security to the board members? If you answered no, why would your top C-level executives make this important investment?

More importantly, what is your slice of the capital expenditure budget? If your company is like many, that slice is less than three percent, and is even less for government agencies. According to the Deloitte *2016 NASCIO Cybersecurity Study: State governments at risk*, while cyber risk has risen in importance in the eyes of governors and other state executives, for most states, cybersecurity is less than two percent of the overall IT budget. Can your endpoint strategy fit in that slice and produce a reasonable return on investment while lowering risk exposure?

Turning strategy and awareness into progress means making the case for a combination of people, process and technology. Protections based solely in policy are not useful when C-level executives talk to the board of directors. What is useful is having a plan that shows quantifiable reduction in risk. Security and compliance solutions need to secure data in the enterprise, while also protecting employees' privacy by blocking any access of IT administrators to non-work related areas on employee-owned devices.

Today's C-Suite dwellers know they must address concerns of the so called power constituents – those members of the workforce who believe they are entitled to work wherever and whenever they want. But that creates a major security threat, which means companies must be able to address security controls and data protection on whatever devices and applications their employees prefer. While endpoint security measures may not turn a profit, they ensure the sustainability of a company by eliminating compliance concerns and reducing risk and impact of data loss, employee productivity and corporate reputation.

In the end, whatever direction the C-Suite goes, they must also be able to stand behind the case that compels the Board of Directors to follow.

Reducing Potential Losses from a Breach

Investments in certain data loss prevention controls and activities such as encryption and endpoint security solutions are important for preventing data breaches, according to the *2016 Cost of Data Breach Study* conducted by the Ponemon Institute. The study revealed a reduction in the cost when companies participated in threat sharing and deployed data loss prevention technologies.

CISOs are learning that combining the detective controls found in many endpoint security solutions with threat intelligence sharing and deployment of data loss prevention technologies could reduce cost almost across the board. Without the endpoint solutions that help to contain a data breach, an incident could lead to higher costs. Without the endpoint solutions that help to contain a data breach, an incident will lead to higher costs. Endpoint solutions cost anywhere from $9 to $70 per seat, so the CISO needs to do the math for return on investment. If you believe that every seat is an attack vector, using simple math with a metric of 1,000 seats in a network and $50 per seat cost of endpoint security, the break-even loss is $50,000. Which means you need small losses to show return. In reality, losses from an endpoint breach could be staggering if the “where’s the data” part of your cybersecurity plan is not specific enough to prevent high risk data from being present at the breached endpoint. That's not a good message to send to the C-suite.

Endpoint Security’s Role in the Defense-in-Depth Approach

At its optimal use, endpoint protection technology must be able to prevent malware attacks and protect users as they conduct normal business within the network, including exchanging emails, browsing the web, conducting Internet research, and using internal business and research applications. That makes the endpoint security suite a business enabler. But equally important, it prevents lateral movement of malicious code to other parts of the network. Today's endpoint anti-malware suites should work with other threat identification and protection tools to provide layered protection. Other important

Advanced endpoint protection is more than just the evolution of antivirus. It's something bigger. It's a way to take that endpoint and prove that I know what it is, that it's still protected, that it hasn't been compromised, that the user is a trusted user, and that they're accessing the data they need and no other data.

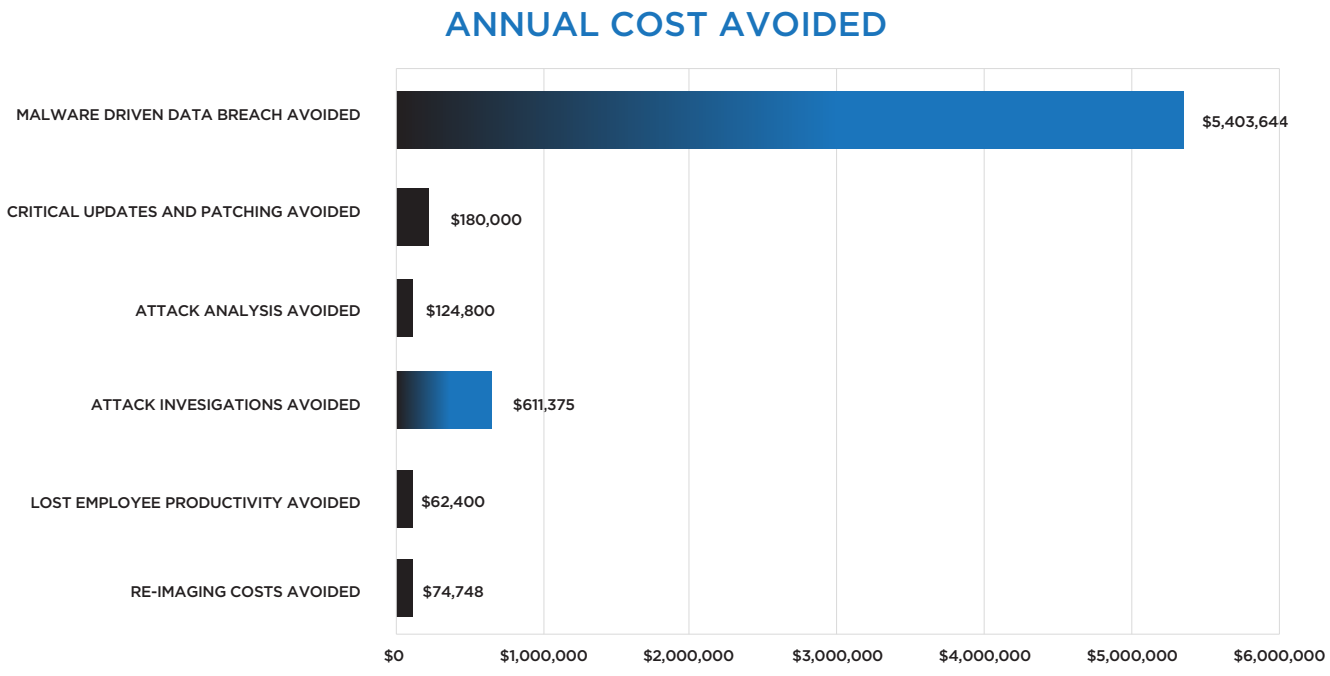
Darren Death, CISO, ASRC Federal

features to consider are the ability to shield against new or otherwise unknown or zero-day threats with the endpoint solution providing host-based firewall, data loss prevention, anti-spyware, email inbox protection, and warnings when visiting websites that could pose security or safety risks.

Calculating Return on Investment

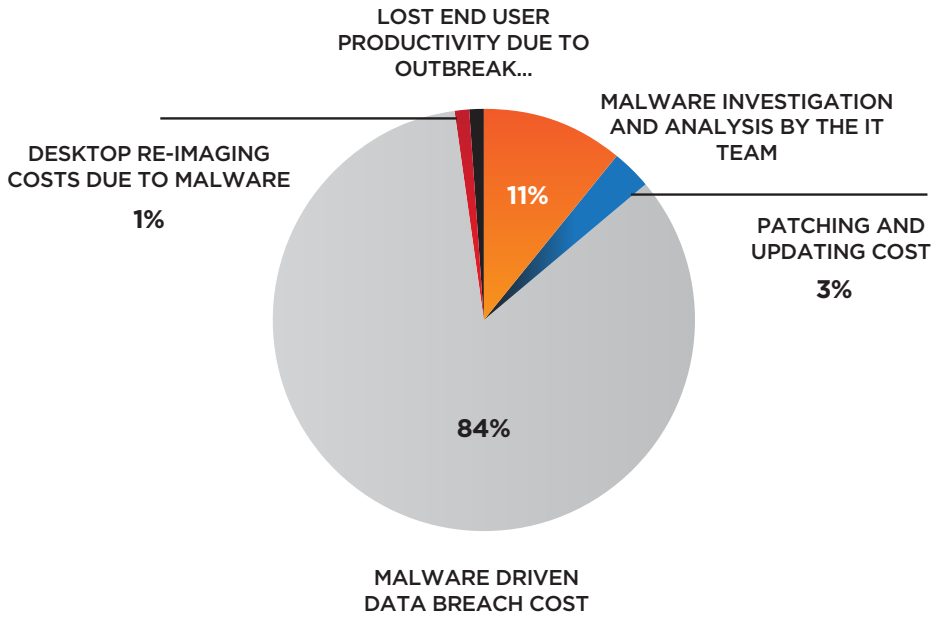
Nothing sells to the C-Suite like a technology investment package that pays for itself in a short period of time. Real dollars saved trumps the potential for cost avoidance. Don't discount the fact that avoiding a $1.5M regulatory fine isn't important; just remember the fine may, or may not actually hit the balance sheet. Show the CIO and CFO how your endpoint security technology initiatives will save labor cost and the associated overhead margins and you will have them wondering why the corporate body waited so long to adopt the solution.

Now – how often does that happen in cash strapped organizations operating in the real world? To justify projects and programs, the CISO must think beyond single or multiple FTE savings to offset the investment. Think about the activities beyond just breach avoidance and the costs that come with it. Many endpoint solutions claim to monitor and facilitate critical patch updates; save you the activity related to attack analysis and forensics, investigating alerts, and reimaging systems; and avoid lost productivity from other projects while your team is knee deep in the investigations.



One of the CISOs contributing to this report invests the time to produce a monthly security report highlighting Key Risk Indicators. The report shows a correlation between machines re-imaged across the years and reduction in risk and disruption. Include this reduction as an offset to the cost of your endpoint solution.

DISTRIBUTION OF THE COSTS AVOIDED



Selling to the C-Suite is just the beginning of the process. C-Suite executives need to be fed information frequently to help them understand the continued cost versus benefit. Show business returns by deriving value from the other benefits of the solution being in place. Highlight the endpoint tool's risk remediation results in the form of the dramatic reduction in downtime costs. Show the increase in productivity largely due to fewer infected machines the technologists have to visit and remediate.

Prevention is key! CISOs and security staff do not have the time to inspect each machine and analyze the findings. Having a solution that saves that time creates benefit…having a solution that stops malicious code saves the expert's time.

Staffing Implications

While many IT leaders are struggling to maintain adequate staff for all security domains and tasks, few believe a next generation endpoint solution is a panacea that will reduce staffing dramatically. One CISO offers that advanced endpoint solutions are an amplifier of productivity – they help make the responders more capable. In other use cases, security solutions do impact a company's bottom line by offering automation that reduces the number of people required to handle security incidents.

There are some CISOs that have to rely on the personnel savings that deployment of solutions are supposed to return. In particular, federal, state and local government CISOs are often locked down on the ability to obtain additional staff. Maintenance of new endpoint solutions in those areas means there likely will be no extra staff to manage the endpoint solution. More than likely, there will be a reduction or

redistribution of staff which means those left behind to manage the solution will have to be leaner and smarter. One CISO remarked that implementing technology that detects and blocks malware from executing and that minimizes false positives enabled his team to redirect attention to act on true indicators of compromise as well as focus on more strategic projects.

Before you transition to any advanced endpoint solution, you have to consider whether your organization has the maturity to be ready for such tools, and whether you will get value from them.

Helen Patton, Chief Information Security Officer, The Ohio State University

However, there is no such thing as a perfect fire-and-forget endpoint security solution. In order to work, such solutions require the right talent to deploy the infrastructure; the staff to manage workstations, laptops and mobile devices; the staff to patch devices if the end point solution does not have that feature; and security operations center staff to monitor and manage the events that occur. The smaller the organization, the fewer staff you have to share the workload and the more divided the effort. The amount of staff time required to research, investigate and apply recommended changes and updates must be balanced against the time required to keep the rest of the cybersecurity defense measures functioning.

If prevention can be automated, staff levels could be reduced with work hours salvaged based on pre-implementation response time requirements. One CISO has improved services without expanding the cybersecurity team based on process time and savings resulting from automated endpoint security tools.

One public sector CISO found that incident response was a 70/30 ratio of firefighting and implementing value-added projects. Implementing a next generation endpoint solution would allow teams to move away from firefighting over time and allow security leaders to reallocate resources to other projects, such as threat hunting, insider threat concerns, or work on programs designed to either move the organization up in maturity level or drive value to the business.

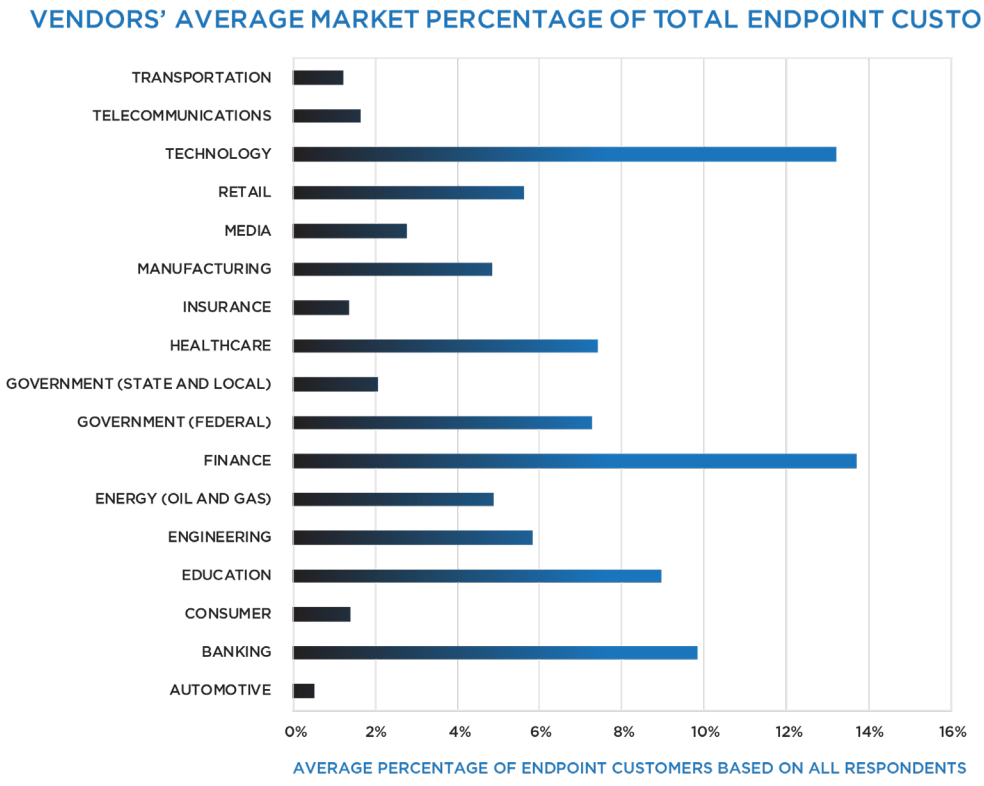
Maintaining Compliance Through Endpoint Security

Businesses and organizations that fall under the regulatory umbrella of federal laws and standards or industry regulations need to ensure they apply sound security principles to all endpoints, including servers, workstations, laptops, and virtual servers through any access vector such as network shares, USB, e-mail, instant messaging, and so on..

With many industry sectors initiating their own security standards and government regulations interlocking at federal, state and local levels, the endpoint protection vendors need to have a broad range of legal and regulatory experts and deeper experience in those "hard to secure" sectors like finance, banking, healthcare and education. An endpoint security solution could help a company meet its compliance needs, and reduce the risk of fines and other penalties. The Gramm-Leach-Bliley Act, for example, while it does not dictate specific endpoint security measures, it does require businesses to implement reasonable administrative, technical and physical safeguards that take into account the sensitivity of data and risk of loss.

In the health services sector, the Health Insurance Portability and Accountability Act (HIPAA) focuses on flexibility, scalability and technology neutrality, so no specific requirements for types of technology to implement are specified. It allows a covered entity to use any security measures that allow it reasonably and appropriately to implement the standards and implementation specifications. However, a covered entity needs to determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization.

In the retail sector, the Payment Card Industry Data Security Standards (PCI DSS) define security controls for accepting payment cards.



In regard to endpoint security in particular, network endpoints must be secured via a centralized policy, to ensure that security threats are mitigated. That includes the use of antivirus software. There is also an evolving need for advanced anti-malware programs that detect anomalous activities or indicators of compromise. If these anti-malware solutions also provide adequate antivirus capability they can be used in place of antivirus. Otherwise, the two technologies should be utilized in conjunction with each other.

While many believe that next generation endpoint security products are poised to replace traditional antivirus, what's clear is that next generation endpoint security is a technology whose time has come. The question to ask is: What's the right solution for my business?

Mike Davis, CISO at American Bureau of Shipping

In the government sector, the Federal Information Security Management Act (FISMA) is designed to maintain the confidentiality and integrity of federal agencies' information systems. Most organizations that fall under these regulations defer to the NIST 800-53 security controls that require endpoints to be protected against malicious code. These protection measures must include periodic scans of the information system and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy. In addition, the protection technology also must block and quarantine malicious code and send alerts to administrators in response to malicious code detection.

A challenge for any CISO is to ensure the endpoints in their security environment or individual information system security boundary are covered appropriate to the security level or data classification of the information processed on that endpoint. Having more than one solution in your enterprise may make sense depending on complexity.

Beyond Security: Other Business Cases

Inattentive users and unsecured devices are part of this world. Businesses and organizations face major threats to their information infrastructure and see impact to business processes daily. Beyond the obvious security issues like malware and data leaks, loss of availability of information systems, corruption of databases, and the potential corporate security and reputational impacts from seemingly innocent embedded devices like onboard cameras can have damaging effects on a business's market position, intellectual property, and profits.

Managing the endpoint goes well beyond anomaly detection and antivirus tools. Endpoints are complex computing environments that require management approaches to ensure operations are efficient, network resources are maximized, costs are controlled and services are integrated efficiently and effectively. Managing the ever increasing variety of endpoints, mobile devices and Internet of Things objects is more than just a security issue.

The ability to employ features like single sign-on authentication, perform network and device health checks, deliver new or updated applications, manage resources using operating metrics, and performing endpoint maintenance can be effected using those tools created for security management.

C-Suite leaders understand the modern information enterprise is as diverse as it is dynamic. "We want bigger, better and faster …" is the cry of the users. Quick access to diverse data, the ability to create and disseminate larger and more content rich documents, and the accompanying need for more resources are all conditions that should be managed – and what you manage should be measured to ensure success. Endpoint security tools should be able to return metrics that help.

When drafting that Request for Proposal, ensure you consider the efficiencies that can be gained by requiring integration between network device and endpoint management tools that are enhanced by also performing endpoint security functions.

To Deploy or Not to Deploy

In the case of the University of Wisconsin-Madison, we used to have only one endpoint solution. That was until the Fall of 2016, when we received two additional packages, each with its own unique features that greatly enhance our endpoint protection game. Our information enterprise is highly diverse with, in round numbers, 700 networks deployed on our 100-gigabit backbone. With our environments changing daily – and sometimes hourly – having an exact count of endpoints is near impossible, so we use a round estimate of over 70,000 endpoints.

To enable efficiencies in the two new solutions, we are using the advanced threat protection components to bolster our detection and prevention architectures and are feeding our analytics solution with valuable endpoint information. The value of having a better view through the endpoint solution suites is tremendous, so the decision to deploy was almost a no-brainer. In order to decide whether a particular solution or solutions will work and the benefits outweigh the costs, CISOs need to get answers to the following questions:

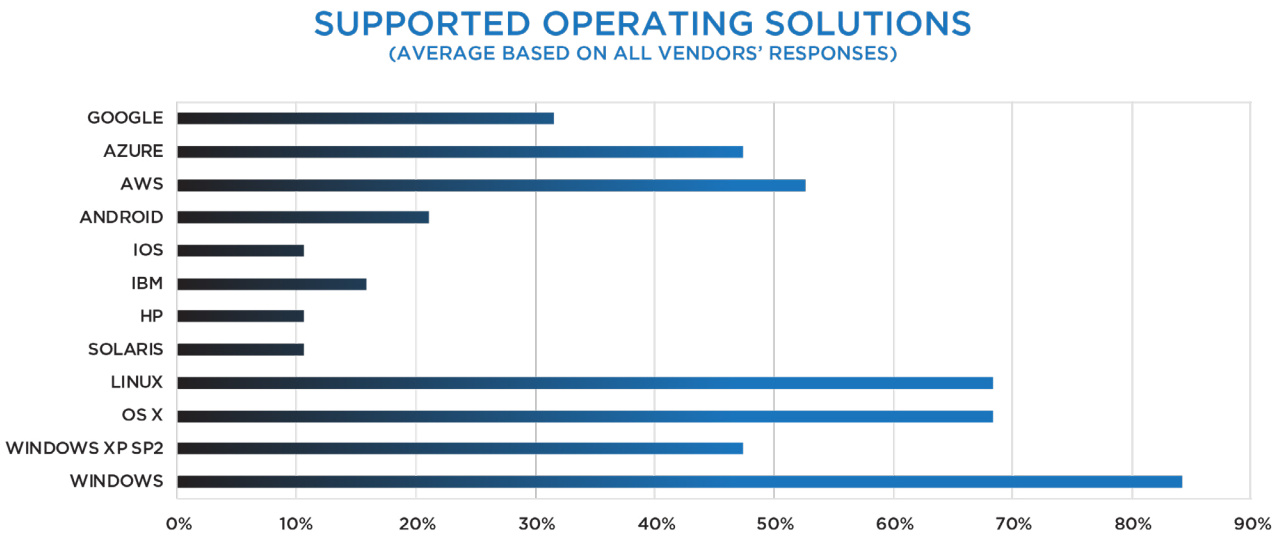
Deployment and Management

- How easy is the endpoint solution to deploy, configure, and manage?
- How do I upgrade the solution, how often are revisions and patches deployed, and what is the transition path for integrating with major tools in my security stack? Are updates provided through a cloud-based resource?
- What is the "tax" on the endpoint?
- Is the management console cloud based, on premise, or are both options available?
- What functions or roles are available in the console (e.g. what granularity of permissions do you have to allow segregation of duties in relation to the product management)?

Integration

- Is the solution part of a larger security platform or an independent "point product"?
- How does the solution integrate with my security infrastructure?
- Does the solution need a special data feed from a threat intelligence database?
- What platforms does you product support (e.g. Linux, Windows, Mac)?
- Does your product include support for mobile devices and mobile operating systems such as Android and iOS?
- What is the installed size of your agent?
- How is the data extracted from the endpoint and stored for later use in metrics analysis within my security program?

- What SIEM solutions does your product integrate with?
- What data points are available to the SIEM from your product?
- How do you protect the communication from the agent to logging servers or SIEM solutions?
- How does your product integrate with firewall or other solutions to incorporate network connection information and identify command and control traffic?



Security Features

- Is your product focused on prevention, detection, or both?
- What threat actor tactics, techniques and procedures are considered in the endpoint solutions design and operating program or processes?
- What heuristic, behavioral analysis, or machine learning features are incorporated into the solution?
- Does your product depend on signatures as part of its identification of malware?
- How frequently are these signatures updated, and what's the average size of an update?
- If your product relies on algorithms or analytics, how frequently are updates made?
- Does it require Internet access to provide advanced malware protection on an endpoint?
- Does your product depend on sandbox analysis as part of its identification of malware? If so, how does it compensate for sandbox avoidance techniques?
- Does your product address memory exploits?
- Does your product address malicious scripts or macros?
- Does your product integrate with Active Directory or other asset inventories to assist in managing the agent?
- Does your product automatically remove assets from the console when they are removed from AD or other asset inventory tools?

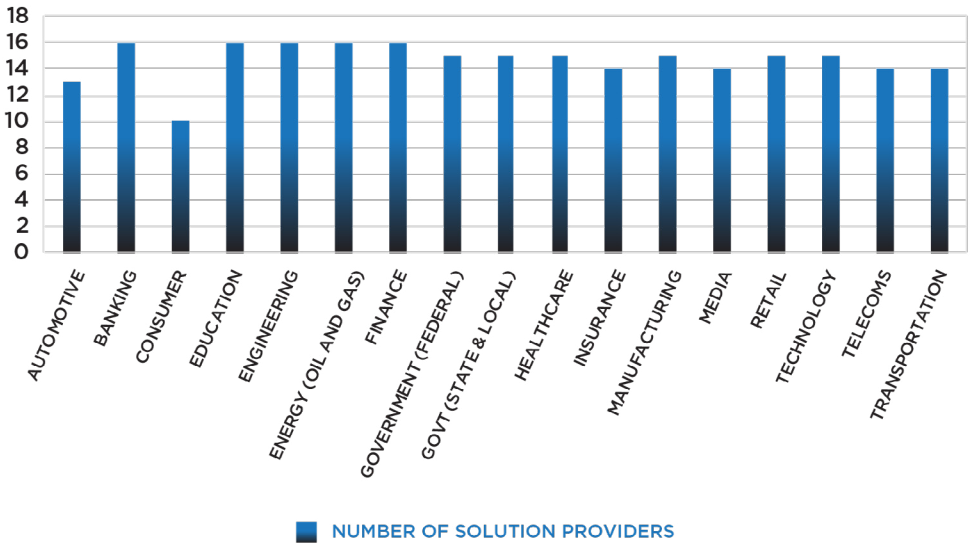
Market Assessment

The days when endpoint protection simply consisted of running an antivirus program are on their way out. Mobility and cloud services are causing endpoint devices to become the critical front lines of defense in a rapidly evolving threat environment, and the market is exploding.

The number of vendors in this space is growing quickly, new security technologies are emerging, and enterprises are pouring more and more money into this area. Choosing a vendor with a track record for success should be high on a CISO's list of requirements. Those endpoint security projects with significant deployments may be favored – or, they may be pushing a more generic solution at lower costs. In either case, the CISO and the procurement teams need to do their homework.

With malware mutating too quickly for traditional antivirus to keep up, advanced endpoint protection methods include sandboxes, behavior-based malware detection, dynamic whitelisting, endpoint isolation and virtual desktops, and machine learning systems that spot new malware as soon as it emerges. In addition to improving detection, advanced endpoint protection vendors are also offering a variety of remediation and forensic analysis tools as well as integration with other enterprise security platforms such as advanced firewalls and security information and event management systems.

MARKET PRESENCE FOR DEPLOYED ENDPOINT SOLUTIONS



Traditional antivirus vendors are not sitting by idle, but have been rapidly adding new endpoint protection tools to their product suites. Network security vendors are also getting into this space. Vendors also are tailoring solutions to multiple technologies or targeting their sales and support to multiple markets. Many of those who responded to the RFI have customers that cover more than 90 percent of the available market verticals.

All this results in a complex and rapidly-changing vendor landscape. According to IDC, enterprises will spend $10.2 billion on endpoint security technology in 2017. The fastest growing part of this market is endpoint response and detection, which more than doubled in size in just one year, from $238 million in 2015 revenue to about $500 million in 2016, according to Gartner.

However, Gartner[1] also predicts that the market will likely converge around the traditional endpoint protection market. That means, for many enterprises, sticking with their existing vendors and simply adding the new security features as they become available makes sense.

[1] http://www.businesswire.com/news/home/20170329005220/en/Worldwide-Spending-Security-Technology-Forecast-Reach-81.7

Key Takeaways

Making key endpoint security procurement decisions is not easy. Doing so in a vacuum can lead to significant resource drain with minimal impact on detection and mitigation of risk. The CISOs who contributed to this investigation offer the following pointers as very important time savers, angst reducers and valuable takeaways:

Keep in mind that endpoint protection doesn't replace basic hygiene. Before you start enhancing your endpoint security, ensure that your environment is being patched and properly maintained.

When thinking about implementing endpoint security, consider not just whether it will work, but whether it will work in your environment. For example, endpoint solutions have the capacity to generate a great deal of data on how endpoints are functioning. Make certain that you have the right infrastructure – in this case, a data analytics platform – to properly leverage the information; otherwise it could just be overwhelming.

Also, when evaluating solutions, keep in mind that your particular infrastructure will help guide you on which vendor to select. You may be tempted to want the high end "Cadillac" version of a solution, but without the infrastructure and processes to support it, and experienced staff to run it, the solution will ultimately fail to deliver on expectations.

Another key point to consider is the impact of advanced endpoint protection on the overall functionality of the endpoint itself. Many products have an agent that runs on the endpoint, and this could potentially impact performance or affect whether a person can continue to work seamlessly.

In terms of specific features and functionality, there are several approaches. Some of my peers highly recommend considering solutions that include the ability to run unknown or unconfirmed processes in micro-virtualized containers.

When it comes to visibility and reporting, it is important that the product dashboard allow security staff to focus on important functions related to the endpoint and its impact on the organization. For instance, whether the endpoint health is at the standard the organization requires, and whether the logs are being processed appropriately. Moreover, the dashboard should make it readily apparent what decisions need to be made based on the information that is displayed.

Of course, cost is an issue for CISOs when selecting an endpoint protection solution. Weigh your choices by considering the following factors:

- What are your requirements?
- What are the alternatives?
- What technology will be replaced?
- What costs will be eliminated?
- What new functionality will be obtained?

By factoring in all of the aforementioned variables, the cost per client may turn out to be little more than a wash.

Buying the solution is one thing, but it also must be cost effective over the long term. Consider the overall total cost of ownership, including the resources that are required to properly integrate, engineer and maintain the solution.

And finally, don't forget the Internet of Things, which will only become increasingly important as time goes by. Your solution should provide visibility into building access controls systems, security cameras, HVAC and other key components which are just as important to security goals as understanding where the next large data leak is coming from.

Advanced endpoint security solutions have a lot to offer to enterprise organizations, and as the CISOs who contributed to this report concluded, such solutions are or will be a key component to a comprehensive security program. Decide what would work best in your environment, narrow the field, do a PoC or two and determine the best fit for your environment.

IS NEXT GENERATION ENDPOINT SECURITY REALLY NECESSARY?

Max Babler, ***Director, Security, Infrastructure and Operations (CISO Equivilant), Madison Gas and Electric***

Every research paper should entertain the contrarian opinion. It's good when CISOs ponder an alternate viewpoint to those they hear from the masses. Through this point of view, we learn and possibly gain insight that may lead to a more refined understanding of our own particular approach. I asked one of my close colleagues, Max Babler, to provide that contrary argument. Max is the CISO at Madison Gas and Electric, an energy provider in the capitol city of Madison, Wisconsin.

Depending on your requirements, you may not need endpoint security/antivirus tools at all. Devices that don't see many changes and don't need to have interactive access to the web, for example, are less likely to need antivirus or next generation endpoint protection. Creating firewall zones that limit the device's access to other systems and simplify monitoring network transactions might be all you need. Provide strict access requirements for the device, mandatory vetting when a device needs updates or requires new data, or "sneaker net" restrictions such as blocked USB ports.

Endpoint security may not the "be all end all" of security. In some cases, it is not even ideal. More advanced functions can cause instability, corrupt data and prevent systems from doing the job they were meant to do. While every vendor tries to limit the impact of such things, when control really counts, having a constantly changing definition of "bad" sitting on the machine waiting to decide something looks suspicious can lead to some really unfortunate problems of stability and other issues that we should look at more closely.

Let us decompose the considerations involved in running without local endpoint security software.

Web Surfing

Most security professionals will tell you that purpose-built servers and systems rarely need full access to the Internet. In fact, the notion of open Internet on most devices in a data center is ridiculous and tantamount to security malpractice.

Deny those bad actors millions of attack vectors by limiting access to the Internet or deny a network role to the device. Secure the endpoints by locking down the browsers to only what is needed, or run transactions through a proxy and close the risk off entirely. Ensure that the web access has a full forward proxy to provide increased security by scanning downloads.

Network Controls

If your system can be isolated in its own network zone, with only approved traffic, controlled protocols, approved MAC filters, and so on, then the device has very little network or Internet traffic risk, especially if paired with one or more of the other techniques listed in this section. In most cases, a network security strategy can use anomaly and intrusion detection and protection systems to further defend your asset in its network zone, further lowering the risk to the asset itself.

Stability Risk

It might seem like a far-fetched notion that the tool to prevent harm can cause major pain but this is reality. Properly configured antivirus and smart intrusion software can be effective and not inhibit stability.

Systems with a high data volume shift can constantly be in scan mode if the engine does not understand and accept certain changes as safe. Complex architectures such as Microsoft clustering can also be a major problem since cluster resources share certain transactions between systems. Without alignment of software drivers for disk and IO, the system can blue screen and crash when an intense scan kicks off.

The answer is simple – isolate, secure and don't run traditional antivirus locally; especially where the system uptime is a safety issue. It's better to over engineer and control the environment than risk the system stability of a carefully designed application.

Access Controls

One of the biggest threats a system has is its user base. Well meaning people from every background and occupation can perform actions that put systems at risk, whether intending to or not.

Skeptics beware! See the latest research on spear phishing and ransomware success rates. Even when people are trained and tested, social engineering is a powerful weapon that all hackers have and it can lead to user related breach or disclosure.

Strict access requirements are key to protect systems. If you can limit user access, there is simply far less risk of intended or unintended infection, breach or disclosure.

Couple this with advanced directory-based anomaly detection to help discover unusual account access and you stand a good chance of finding potential risk vectors before the platform becomes affected.

White Listing

Does the system have a high volume of change? This question is aimed at determining if the system is a candidate for application whitelisting. Whitelisting is a way to inventory a computer's software programs and specify that only certain specific programs may install and run on this device. If you have a verified "known good" of each file on the machine and can enforce it, you greatly reduce the risk and attack surface.

Software Updates

Another likely risk vector is the updates you receive from your software providers. Whether it's operating system updates or application changes, some payloads are simply not vetted properly or flow through not so secure channels. The result is you receive an update to your system that is pre-infected.

Now, you do need to scan these things, but you don't necessarily have to do the scan on the device. If you have a process that has at least one scanning engine to look for infections – but two or more is better – then you can greatly reduce risk.

It would also not hurt to think about the chain of custody of your updates. Do you know where they have been before they got to you? Is there a more direct source? If there is, change to that.

Device Hardening

Most systems have USB or other mass storage ports in addition to video ports. Those ports interface with the hardware layer and have direct access to the operating system.

Turn off the ports you do not need. Lock down ports to accept only certain devices – white listing a specific mouse and keyboard, for example. Filter the connection through a "dumb" circuit, an assured connection translation that filters off risky transactions. (A dumb circuit is simply an assured connection translation that filters off risky transactions. A good example of this approach is to run HDMI through a DVI converter and back to HDMI. This effectively strips off the Ethernet signal and does not allow that smart TV to be an attack vector for your laptop,)

In the End…

We are not saying that antivirus tool suites are all bad or completely unnecessary, but we are saying it can be bad and unnecessary if you fail to do the prep work to create a safe place for your critical computing workload.

Balancing the environmental controls around your critical devices and access to your critical devices can go a long way to minimize risks without the need for localized antivirus software suites.

Summary

The point of this paper is not to tell you what the best endpoint security solution is, or is not. No CISO will tell you their next generation endpoint security solution is the best there is. Keeping up with the CISO next door is also not the best strategy; providing a tool in the toolbox to help your security teams is. Sun Tzu, the fabled Chinese Warrior, tells us that we must know our enemy's strengths and weaknesses as well as we know our own. If this paper tells you anything, it is that you need to know your technology and business operating environment; understand your users, your C-Suite and Board of Directors; and to continually research the landscape of vendors and their services and tools that will help the CISO stay ahead of the enemy.

These days it seems like there are as many endpoint security tools and vendors as there are organizations that analyze and rate them. CISOs spend a significant portion of their time reading technical articles, taking time to review JAWP (just another white paper), or poring through emails from the hundreds of vendors that claim their product or approach will save you time, money, and manpower while they simultaneously solve world hunger (for the vendors at least). Hopefully this paper puts the thoughts of a variety of CISOs and the capability of a cross section of vendors in your view – with our intent to help you understand the most important point:

Ultimately the best endpoint security solution and vendor is the one you just selected.

CISO CONTRIBUTIONS

ADP

V.Jay LaRosa
Vice President, Global Security Architecture

COMPANY OVERVIEW

ADP is the one of the world's largest and most experienced providers of human resource services. The company employees more than 56,000 associates and serves over 650,000 clients in over 110 countries. More than 70 percent of the Fortune 500 use at least one of ADP's services, which include HR, payroll, talent, time, tax, and benefits administration, and the company is a leader in business outsourcing services analytics and compliance expertise.

The company is headquartered in Roseland, New Jersey and was established in 1949. It had more than $12 billion in revenues in 2016. ADP has led the way in defining the future of business outsourcing solutions and remains one of the world's most innovative companies. Our unmatched experience, deep insights and cutting-edge technology have transformed human resources from a back-office administrative function to a strategic business advantage.

BUSINESS USE CASES

The threat landscape has changed significantly. Across industries, you see breaches occurring at an alarming rate. In the old days, you looked for a frontal assault on your Internet pipes and servers. Today, most attacks originate from endpoints and the majority of large breaches start with phishing attacks.

Threats today are squarely focused on our end users through phishing scams and on browsing habits with drive-by attacks. They're successful because the endpoint runs so many different variations of software, which creates the potential for exploits in Java, Flash, PDF, Microsoft Word, PowerPoint, and Excel. Managing all of those software combinations and being able to enforce technology hygiene is tough for even sophisticated organizations, especially when you consider how long it takes for zero-days, target specific malware, and vulnerability exploitation to be discovered. This means that criminals have the potential of a huge lead time to work to take over endpoints in an organization.

Legacy detection-based defenses are not stopping modern cyber attacks. The traditional methodology of detect-to-prevent has long been defeated. Anti-malware and antivirus signatures are ineffective. Add to this the fact that attackers are being sponsored and supported by nation-states, well funded organized crime, and even ideological terroristic organizations, and that zero-day breaches are leveraging customers' own technology. You have to have a better approach. Endpoint protection – especially endpoint protection with micro-virtualization – is a better way.

TECHNOLOGY ENVIRONMENT

ADP has transitioned into a centrally-supported organization with distributed global support functions. All Information Technology rolls up to one global CIO, which ensures that all of our Windows, Mac, Android and iOS devices are managed in the same manner. From a server perspective (including hosted client operations), we are well distributed globally. Added to that, we also have a strong global organization for enterprise architecture and sharing of information across organizations, staff and technology delivery teams.

Our advanced endpoint security solution uses micro-virtualization to isolate dangerous threads running on our endpoints. If someone opens up a phishing email, it opens up in a hardware-enforced isolated and virtualized container that will prevent it from ever accessing the underlying file system and the network stack. This has proven to be very effective for us. It's virtually seamless to our users and has minimal overhead on our workstations. Our users have no idea it's even there.

In the underlying operating system, we still anticipate and expect old-school attacks in our cyber defensive planning and operational response protocols – things like buffer overflows and other service based exploits. Next generation endpoint solutions can use agents and machine learning to see how process execution is unfolding on the workstations and detect and prevent nefarious activity there.

Finally, our focus goes way beyond developed malware attack scenarios and we are now preparing for malware-less attacks such as those that leverage PowerShell or other system functions like Atom tables, which are used to compromise workstations or servers and move multi-directionally inside the network in a way that would be otherwise undetected by traditional antivirus or anti-malware. This is where we leverage a complementary solution to micro-virtualization that uses machine learning and advanced EDR capabilities to give us complete visibility and advanced analytics in our environment.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

First and foremost, our main goals are to protect our clients' data and to protect our clients' funds. Clearly this is critical for clients as well as ADP. We've seen and heard from our peers in other large enterprise organizations that an average of 50 to 100+ compromised workstations a month is not unusual. With ransomware and other sophisticated types of attacks on the rise, having to rebuild this many workstations at that pace is a massive waste of time, productivity, and resources just trying to recover from attacks.

Several years back, before we considered next generation endpoint solutions, we spent a lot of time, money, energy and resources baselining all of the activity that was going on in our complex and multinational environment. It was important to know exactly what we were doing, on which networks and network segments. We instrumented our global technology environments and platforms with automated detection, sandboxing and visibility in place so we could understand when or where bad things might be happening. This visibility gave us a new operational context around incident response and a new level of detail into host infection management. This new opportunity gave way to changing from a response strategy to a new focus on prevention.

We looked to advanced endpoint security to help us prevent attacks from happening or spreading laterally, so we could move from a detect and respond model, to a prevention first model to get out from behind continuous remediation.

KEY FACTORS TO CONSIDER

For advanced endpoint protection, the most important factor to consider is whether it is truly advanced. In the past with our environment, we have detected and caught advanced attacks from sophisticated actors, who were able to circumvent legacy preventative defenses like antivirus and sandboxing but, required manual intervention to stop.

In selecting an advanced endpoint solution, you want to ensure that, to the greatest extent possible, you are future-proofing your defenses. This means that looking at how the advanced endpoint solution minimizes the amount of human activity required, and how it can isolate and prevent, rather than just detect malicious processes or activity, is crucial. How it reports them back to you for you to gain operational intel is also fundamental to your program. If you prevent but can't investigate to respond, you can't validate effectiveness or produce TCO metrics to show the value of your investments. Other considerations include training to operate, cost of the load on the network, and costs associated with responding to false positives and fine tuning the system.

Finally, you have to remember that endpoint protection is iterative, not static. Any advanced endpoint solution you adopt has to be flexible enough to protect you today and in the future against an adversary that is actively trying to circumvent it.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

Almost every endpoint protection vendor out there leverages the same methodology to detect and prevent bad things from happening on endpoints: instrumenting the kernel. The problem is that the criminals know how to defeat kernel-based technologies, they know how to kill antivirus technology and shut down security software with kernel-level exploits. So, if you are going to invest in endpoint protection, you want to make sure that the vendor is able to provide various alternate mechanisms for security to prevent criminals from disabling the technology.

That includes using hardware-based capabilities in the Intel chip set to be able to detect and prevent process execution from ever even making its way into the core processor. That helps prevent more advanced threats and helps to identify threats sooner.

One of the other things we looked for is the ability to run unknown or unconfirmed processes in micro-virtualized containers. When malicious code is isolated and contained, you can then examine it to determine whether it was a genuine process that should be allowed to run or an exploit attempt.

Of course, you want visibility into your network, to have detailed information about your endpoints, but at the end of the day, you want your advanced endpoint solution to not just identify threats, but to prevent them and isolate them.

OUTCOME AFTER IMPLEMENTING AN ENDPOINT SECURITY SOLUTION

One of great things about the advanced endpoint protection technology we leverage is that we can show exactly how many endpoint breaches we avoided every month. While it is difficult to assign a dollar value to each prevented breach, you can look at the systems and data on those systems as well as what the associated user had access to, in order to figure out what the value of prevention was.

The same thing is true on the server side as well. If you can show, for example, that a particular server had access to a significant number of personal identities or that a large volume of currency flows through the server, the value of preventing or disrupting an attack on that server allows you to quantify the investment of that advanced endpoint protection very quickly.

Another advantage we can quantify is the fact that we don't have to rebuild significant amounts of machines each year. That is a hard, quantifiable fact that we can rely on. Productivity loss at the business unit levels is not something many people measure today, and this is something that is relatively easy to quantify.

IMPACT ON STAFFING LEVELS

If you believe that deploying this technology will allow you to reduce staff, that is incorrect—at least in our experience.. We don't look at our endpoint security rollout as a staff reduction strategy. We view advanced endpoint solutions as an amplifier of productivity. These advanced endpoint solutions can help make the responders more capable, which is really the goal with these tools.

We were definitely able to refocus our staff and make them much more efficient and effective with these toolsets.

PEER RECOMMENDATIONS AND ADVICE

If you're not thinking about advanced endpoint protection, you should be. This is the most important investment that you can make in protecting your organization.

Criminals have some of the most advanced weapons that you can imagine, and they're targeting our endpoints every single day. The end user workstation has, on any given day, a hundred-plus pieces of software installed, plus hundreds of services that are running. Every day, we see billions of email messages with things like polymorphic malware and ransomware with worm-like capabilities. You're never going to be able to defeat them with traditional antivirus-based defenses, particularly those that are signature based. If you're not thinking about a new approach to be able to defend your end users, you're a sitting duck.

SUMMARY

Just about every enterprise needs to be looking at advanced endpoint solutions because they need to understand that they are a target for every malicious actor – from nation-states, to identity thieves and data thieves. The reality is that every one of us is a target, not just large enterprises like ADP. Companies need to look not only at the threats as they exist today, but also the future threats, and prepare for them. So, whether you're a small, medium sized or large enterprise, you are at risk. We all are.

AMERICAN BUREAU OF SHIPPING

Mike Davis
Chief Information Security Officer

COMPANY OVERVIEW

Since its founding in 1862, the American Bureau of Shipping (ABS), a not-for-profit corporation, has been committed to setting standards for safety and excellence as one of the world's leading ship classification societies. ABS has been at the forefront of marine and offshore energy innovation for more than 150 years. In a constantly evolving industry, ABS works alongside its partners tackling the most pressing technical, operational and regulatory challenges so the marine and offshore industries can operate safely, securely and responsibly. The surveyors, engineers, researchers and regulatory specialists who form the ABS team work in more than 150 offices in 70 countries around the world providing traditional classification services as well as on-the-ground technical services in asset performance, energy efficiency, environmental performance and life cycle management.

BUSINESS USE CASES

Safety and protection are fundamental to the American Bureau of Shipping. Just as the organization is committed to empowering marine and offshore industries to operate safely, securely and responsibly, so are we committed to protecting our valuable data assets from cyberattacks.

With a business operations environment that includes a network of clients and contractors and a diverse employee base of around 5,000 people in 150 locations, the organization presents a large, attractive attack surface to would-be attackers. On any given day, ABS, like most other companies, is at risk of phishing campaigns, zero-day exploits and advanced targeted attacks.

The ability to prevent data breaches, ransomware and other malware on endpoint devices is a primary business imperative for ABS. Although our traditional antivirus and firewalls were able to stop known, signature-based malware, we were finding it challenging to block new malware variants, such as memory-resident malware. Needing to block threats in real time before they cause real harm, we turned to next generation endpoint protection as a solution.

TECHNOLOGY ENVIRONMENT

We have a multifaceted, distributed infrastructure that includes our IT operations headquarters, which are co-located with a data center, and six data center hubs located across the globe to support business operations in 70 countries. Each of the hubs supports remote operations, servicing a diverse end user base of employees, third-party vendors and partners who use a wide variety of devices to transact and connect.

When it comes to having influence and control over users, we must contend with the fact that although we perform risk assessments on our vendors, we ultimately lack control over the external parties that connect to our network. So, when deciding to adopt a next generation endpoint strategy we determined that we'd continue with an integrated layered security approach, integrating a next generation firewall solution as well.

We also operate a security operations center (SOC) with a managed service provider in the cloud, which includes an advanced threat analytics service that incorporates security information and event management (SIEM). And we run web packet and capture tools with the SIEM and the SOC. Everything is integrated and working in tandem and though there may be a slight overlap for the most part everything is complementary. However, we do look for redundancies and always are trying to increase efficiency, which was a key factor in deciding to replace our traditional antivirus product with a next generation endpoint security solution. The solution we selected integrated easily with the existing security infrastructure and leverages artificial intelligence to detect and prevent the execution of harmful code on the endpoint.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

Our primary business goal was to efficiently detect and prevent malware from executing on endpoints in real time, while minimizing exceptions. Beyond detecting 100 percent of all known, signature-based malware, this requirement included detecting malware using advanced techniques such as scripts and macros, 'execution-less malware,' zero-day attacks, bots and unknown future variants. In combination with this need was the requirement to protect against memory exploitation from memory-resident malware. With a next generation endpoint security solution that uses artificial intelligence, behavioral analytics and vendor threat intelligence, we had a high level of confidence that we were ahead of the malware curve.

All CISOs know that two tenets in information security are that capable security talent skilled in handling complex threats is scarce and no solution is ever 'fire and forget.' Because the security team was already stretched thin and multitasking, a second business goal for us when implementing a next generation endpoint security solution was that that the solution would be easy to operate with a low level of support and minimized security skillsets.

It is important to remember that each device connecting to the network represents a possible entry point for attackers to gain access to data and launch their assaults. All it takes is one click from a user for their endpoint machine to be compromised. Once that happens, attackers are in. To provide complete coverage of all endpoints on the network, a third business goal was that the solution be scalable, support a wide range of device types, including BYOD, and support multiple operating systems (e.g. Windows, MAC, Linux).

Another business goal was that given the parameters of replacing existing products, the solution be cost-effective and quickly deliver business value.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

The most important technological issue for ABS was how well the product detected threats on the endpoints. We also looked at ease of integration and use, transparency, impact on our network and network operations as well as how many staff it would potentially take to run and maintain it. We wanted a solution that could be tailored to our environment and that would minimize the problem of false positives, which would require our attention. While we wanted a solution that would work out of the box, eventually we contracted for additional professional consulting services that helped tune the endpoint protection for our specific environment. We started with zero baselines of known good processes and we added to that.

KEY FACTORS TO CONSIDER

When considering a next generation endpoint product, it is easy to become overwhelmed by all the choices. Important factors I recommend considering when deciding on a next generation endpoint solution include cost, extent of remediation capabilities, ability to leverage threat intelligence and timeframe to experience results.

If you conduct a proof-of-concept evaluation, which I would recommend, and the list of contenders is narrowed down to the top two or three best products in your environment, cost usually becomes the independent driver. It is important to evaluate the functionality and cost trade-offs when selecting one product over another, including expenditures associated with addressing any residual risk that occurs once the new system is implemented.

During evaluation of next generation endpoint solutions, we found that there is no single product that suits all situations. For example, a product may excel in detection at the expense of remediation capabilities. As a result, it is important to be mindful of any functionality gaps that will require additional products, supporting tools or manual activities. This becomes especially important when functionality may be lost due to replacing existing antivirus tools.

One thing I recommend doing is customizing the threat intelligence features in a couple of different areas. For example, we are putting together a cyber threat intelligence program, which involves understanding what we get from our existing tools and what monitoring gaps are left that we need to fill in.

IMPACT ON STAFFING LEVELS

Alerts from even a well-tuned system can quickly burden the IT security team with more work and overwhelm their ability to respond effectively. With our security team already covering multiple security tools, we needed a solution that would act as a force multiplier to make the team more productive and efficient.

Implementing technology that detects and blocks malware from executing and minimizes false positives has allowed us to minimize our false positive efforts and redirect our attention to act on true indicators of compromise as well as focus on more strategic projects. That said, in terms of pure numbers, adding a next generation security solution could potentially allow security teams to better prioritize tasks, especially if using a risk based security strategy.

PEER RECOMMENDATIONS AND ADVICE

I recommend if a CISO isn't using an advanced endpoint protection solution that they consider one and when you do consider one, ensure that it easily integrates with your architecture, is easy to use and is transparent to the user.

Be sure to consider all factors when making a determination. What are your requirements? What are the alternatives? What technology will be replaced? What costs will be eliminated? What new functionality will be obtained? By factoring in all of the variables, the cost per client may turn out to be little more than a wash when replacing the older technologies.

Next generation endpoint solutions that are replacing a traditional antivirus system will likely require customization and tuning in order to get back to the organization's true zero baseline. This typically requires engaging a professional services team to initially help configure the system with policies tailored to the environment and network configuration.

SUMMARY

Faced with a threat landscape that is constantly evolving, as CISOs we can't help but come to the conclusion that we need better prevention. To this end, we are continuously evaluating products to either augment or replace our current protections. While many believe that next generation endpoint security products are poised to replace traditional antivirus, what's clear is that next generation endpoint security is a technology whose time has come. The question to ask is: "What's the right solution for my business?" Answering that requires an understanding of how all aspects of the product—features, usability, integration and value—fit into your overall security strategy. What I can tell you is that we're stopping a lot of malware, and have not had any related incidents yet – though as we all know there is no "100%" endpoint solution; thus a defense in-depth approach is still required.

ASRC FEDERAL

Darren Death
Chief Information Security Officer

COMPANY OVERVIEW

ASRC Federal is a $1 billion defense contractor based in Washington D.C. It is part of the Alaska-based Arctic Slope Regional Corp., which is a $3.5 to $4 billion holding corporation. The parent company is involved in construction, oil and gas, refining and distribution, finance, hotels and convenience stores, a travel company, and more. ASRC is the largest private employer in Alaska.

From a system perspective, I have a lot of interaction with the parent company. I am responsible for securing the endpoints, not only for all ASRC Federal employees, but for all employees at the holding company as well.

BUSINESS USE CASES

ASRC Federal is a geographically distributed company, with employees across the United States. The same is true for our parent company, Arctic Slope Regional Corporations (ASRC). We want to be able to protect our endpoints wherever they are, and whether they are on our network, or connected to a public Wi-Fi network such as at Starbucks.

We're also making a march towards the cloud, so a lot of our data will no longer be sitting in an internally-owned data center.

From a networking perspective, we need to establish trust within a model that is inherently untrusted. That means we need to ensure that we're establishing secure connections between the endpoints – on or off our network – and wherever the data is located.

We're in the process of extending the protection levels we have today. We are evaluating the advanced capabilities offered by our current vendor, as well as looking at the solutions provided by other advanced endpoint protection vendors.

TECHNOLOGY ENVIRONMENT

Presently, we're running an advanced protection suite on the endpoints, but we are moving beyond this capability with the addition of advanced analysis capabilities offered by next generation endpoint protection.

We also are implementing network segmentation this year so that users have access only to the resources that they need. We're also looking to implement information rights management, including a cloud-based productivity suite, with comprehensive data encryption. If you don't have permissions, you won't be able look at our data. We also will be implementing multi-factor authentication to move beyond simple passwords. Our goal is that everyone will use two-factor authentication on their client devices.

We have a great deal of depth in our defensive measures, and we're looking to build on them. For example, we have multiple layers of malware inspection as data is coming into the environment, and our addition of advanced endpoint protection will certainly enhance our capabilities.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

At ASRC Federal, we believe it's essential to operate a secure organization and to be able to demonstrate best practices to our customers. As a systems integrator, our credibility relies on walking the walk, not just talking the talk.

Given that we advise our customers to implement advanced endpoint protection, we need to do the same for ourselves. We must practice what we preach and demonstrate that we're doing an effective job with the measures and tools we recommend to others. We must ensure that our customer data is protected at all times.

This information is going to come through our endpoints and end up on our servers and in our cloud. To fully protect our customers' data, we must protect our total environment.

KEY FACTORS TO CONSIDER

Endpoint security vendors make a lot of claims about the effectiveness of their algorithms, about their ability to detect and block zero-day attacks, and so on. I take the position that a product can't be 100% effective 100% of the time, so I layer my coverage and buy more than one solution. It really doesn't affect performance but it certainly increases the efficacy of our total solution.

Nothing works perfectly on its own, but if you have more than one tool you are in a better position.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

I'm very interested in advanced endpoint solutions that can safely do detonations. I want to know what malicious code is intending to do. This kind of knowledge helps us boost our defenses against that activity in the future.

Malware writers have upped their game and they have included the ability for the code to see if it's running in a virtual machine, which could be an indication of a sandbox. The writers have included a virtual machine bypass feature in their malware. Some of the endpoint protection vendors know this tactic and they've come up with their own tricks to fool the malware to increase the chances that it gets detected. I like this kind of innovative approach that stays a step ahead of the malware.

I'm also very much interested in forensics capability. I would like my chosen tools to have all the data to be able to rebuild an event and present it to our security analysts in a succinct way. I don't want to have to hire a staff to do forensics; I'd prefer to have that data just be part of the suite.

Out-of-the-box integrations and APIs also are important to ensure that endpoints are communicating with the things I want them to communicate with, while still providing the seamless end user experience that everyone expects.

IMPACT ON STAFFING LEVELS

I don't expect to see any impact to our staffing level. However, it should be a help to the SOC operator because there is a certain amount of data gathering and hunting their analysts won't have to do because the software is doing it for them and presenting it to the team.

I don't anticipate there will be any changes in our staffing needs post production of a new or upgraded solution.

IMPACT ON STANDARDS AND REGULATIONS

Given that ASRC Federal is a government contractor, we have considerable regulatory requirements to observe. We fall under NIST 800-171, which covers security of unclassified information under the Federal Acquisition Regulation. That regulation requires that we have anti-malware protection in place.

I consider an anti-malware solution to be a bare minimum security measure for our endpoints. Regulatory compliance is the driver that got management attention, but I am steering ASRC towards security maturity that is far beyond compliance. My decision to implement an advanced endpoint protection technology is based on improving our cybersecurity program maturity.

At ASRC, we have a very savvy senior leadership team that understands there's a difference between compliance and maturity. They fully support the decision to exceed NIST's minimum specifications.

PEER RECOMMENDATIONS AND ADVICE

I would say that every CISO should be looking at implementing an advanced endpoint protection solution. In my opinion, antivirus is almost dead. AV still catches bad stuff, so it's still somewhat useful, but it's clearly not enough.

Endpoint protection doesn't replace basic hygiene. Before you start trying to enhance your endpoint protection, you need to ensure that your environment is being patched and properly maintained.

I'm in favor of having vendor bake-offs because there are a lot of great tools out there right now, but I don't see anyone that is a shining light. Each one has its special niche, but I don't think any of them have really proven themselves. If there were one outstanding vendor to go to, everybody would be going to that one vendor.

So, if you've got a relationship with a vendor and you feel that you're going to be getting comparable service from them versus switching to someone else, then go with your existing vendor. Perhaps if you mention you're looking at other vendors, they might give you a rate discount on your license.

But if your current vendor isn't meeting all your needs, and you can get the same or better service from another provider at a lower cost then that's a great reason to switch.

SUMMARY

Advanced endpoint protection is more than just the evolution of antivirus. It's something bigger. It's a way to take that endpoint and prove that I know what it is, that it's still protected, that it hasn't been compromised, that the user is a trusted user, and that they're accessing the data they need and no other data. Our employees are working from many different locations, and we are moving towards cloud-based applications and systems. We have to have a solution that can protect our systems regardless of where they are, and what network connection they are on. We need to move in that direction to keep our information and our customers' information secure.

FREEPORT-MCMORAN INC.

Vaughn Hazen
Chief Information Security Officer

COMPANY OVERVIEW

Freeport-McMoRan Inc. (FCX) is a global natural resources company with headquarters in Phoenix, Arizona. FCX is the world's largest publicly traded copper producer, the world's largest producer of molybdenum, and a significant gold producer. Our portfolio of metal assets includes the Grasberg minerals district in Indonesia, one of the world's largest copper and gold deposits; with significant mining operations in the Americas, including the large-scale Morenci minerals district in North America and the Cerro Verde operation in South America. The FCX global workforce includes over 50,000 employees and contractors.

With such a large and diverse workforce, distributed all around the world, managing the IT assets and protecting information is a challenge. With a team of 11 full time employees and 25 contractors, Vaughn Hazen is responsible for all aspects of information security at the enterprise, including intrusion detection and prevention, data security and incident response.

BUSINESS USE CASES

Being a highly distributed enterprise with operations around the world, we face a number of challenges from bad actors. At FCX, we value information security and invest accordingly to combat threats. As such, we were an early adopter of a next generation endpoint security solution. The main reason we implemented the technology in 2015 was to protect our intellectual property, and ensure the proper operations of IT infrastructure.

One of the challenges that we have is our global footprint. We have active nation-state activity in some of our locations that we identified as credible threats. In addition to nation-state actors, we saw poor user behavior allowing computer infections into the environment. Rather than simply respond to all of these incidents and reimage infected machines, we wanted to be more proactive, and adopting a next generation endpoint security solution grew out of that desire. At the same time that we were investigating solutions for new malware techniques, ransomware was becoming more prevalent. Rather than having to respond and either pay the ransom or rebuild entire systems, we wanted a solution that would prevent the attacks from being successful in the first place. Our next generation endpoint security solution held the promise for stopping these attacks. And so far, it has been successful.

TECHNOLOGY ENVIRONMENT

Before deploying a next generation endpoint security solution, we used a mix of solutions, including antivirus or anti malware, file reputation, threat intelligence for active blocking, and sandboxing. The goal was to mix endpoint detection with other technologies to provide a more comprehensive solution. Though it was superior to traditional antivirus, it wasn't enough to protect our endpoints so we moved on a purpose-built endpoint solution that is both proactive and reactive. Today, even with our next generation endpoint security, we still take a layered security approach to protecting FCX.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

We needed a solution that would allow the business to run smoothly and stop the need to regularly reimage machines. We needed to make sense of all of the threat data without requiring a great deal of human interaction. At the outset, there was a lot of tweaking to address false positives, and a lot of interaction with the solution provider. We knew the endpoint security solution used new technology, including machine learning, and would have kinks. Because of this we would have to have calls regularly with them. Early on, we encouraged them to create a knowledge base so that we didn't have to find the only tech support person familiar with a particular issue and now it is part of their standard offering. Because of the nature of the work that FCX does, there was a need to create solutions that would work with our SCADA solutions, but which did not rely on those SCADA-based services to be connected to the cloud or the Internet generally.

As well, when we selected a solution to deploy to meet our business mandates, we required a solution that would be deployed without having to get into our process control network as a cloud-based solution. So, there were numerous interactions with various endpoint providers to ensure that either an on-premise management console or a proxy was an option. Finally, the endpoint security solution needed to address rogue or infected USBs and other devices, and to be able to identify and isolate the harm that might occur from that attack vector.

KEY FACTORS TO CONSIDER

There is an ongoing debate in the security industry over what is more important – advanced detection or advanced prevention. Next generation endpoint security products are starting to converge between the detection and response, as well as the prevention, so advanced capabilities are developing in both of those areas. I don't think that it is advisable to simply take one or the other capability; considering a solution that has both is the preferred approach. Any endpoint security solution must also have the capability to address executables and scripts as well as memory exploits. Solutions that don't address all of those will have protection gaps. Signature-based antivirus solutions are no longer sufficient, and with the newer options, signature-based solutions are no longer necessary.

Regarding return on investment (ROI), one important question to address is the cost of not having a next generation endpoint security solution. We are operating in some interesting places and we see interesting malware. Before we implemented our current solution, we were spending time and energy mitigating, responding and rebuilding after malware events. Our focus had to be on response. All we could do in some cases was to reimage, which was costly, required a significant allocation of employee time, and had a negative impact on our users. It was a bad solution that was not sustainable, and we had to find something better.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

One important factor for FCX was the ability to work with a diverse IT environment with extensive custom code, applications and executables. When we first rolled out our solution, we set it in "listen" mode which identified many of our custom executables as false positives. It is important to know the environment and how the solution will impact it. We needed to test how the solution worked in a real environment and then work with the vendor to white list our custom applications before we went live.

While dashboards are nice, what is important is whether or not the solution is preventing the attacks. Something that is cutting edge containing advanced protection capabilities will not have all of the mature capabilities built in from the beginning. They don't exist, so when leveraging a new capability, it is going to be immature. It is not going to have the same level of dashboards or the same level of management capabilities that you would expect in a more mature product. However, with the improvements we have made in the two-plus years since we implemented our next generation endpoint security solution, it is much more mature.

OUTCOME AFTER IMPLEMENTING AN ENDPOINT SECURITY SOLUTIONS

Rolling out a next generation endpoint security solution has been challenging, but it has been well worth it. It significantly enhanced our ability to effectively detect and respond to threats, for both known and unknown attacks. As well, our solution has so far protected us against ransomware, which has become a prolific threat.

But it is not just about blocking things that are known or suspected to be harmful. It is also about being able to conduct business. Recently, our endpoint security solution identified something as a Trojan that should be blocked. It was, however, just really bad programming for an industry-specific solution. It was our registration executable for our software that required a dongle. We were able to whitelist this executable and keep the business running. Any advanced endpoint security solution has to be able to work in your environment with your specific needs, and be adaptable.

IMPACT ON STAFFING LEVELS

Implementing a next generation endpoint security solution has made a positive impact on our staffing. The initial implementation was intense, having to white list so our business process was not affected, but in the long run it has allowed us to refocus our staff. Historically, our incident response team had to continuously react to those malware incidents. With a next generation endpoint security solution, we are proactive. Our team is now able to perform more advanced work than just chasing malware.

IMPACT ON STANDARDS AND REGULATIONS

Some regulations that don't recognize next generation endpoint security solutions require entities to have antivirus products. These traditional solutions often mean having some kind of agent on your network. However, running multiple agents does not equate to more security; in actuality, it means less security since each agent represents a potential attack vector. The more agents that you have on an endpoint, the broader the footprint is on that endpoint, increasing the likelihood that you are going to be exploited due to the additional vulnerabilities.

Therefore, running multiple endpoint solutions may provide compliance with a standard, but may actually lower security posture. However, some of the standards are starting to get smarter, recognizing the capabilities with the newer solutions. Additionally, the newer solutions are earning more certifications which allows them to meet compliance requirements in lieu of traditional antivirus.

RECOMMENDATIONS

I recommend investigating a next generation endpoint security solution to replace a reactive solution, but ensure that it converges detection with prevention. It is important to recognize, however, that there will be a lot of pain when adopting new technologies. Though the currently-available products are maturing, next generation endpoint security solutions are still relatively new with capabilities being added continuously, so you will need to plan for that pain.

SUMMARY

FCX has found significant value in its next generation endpoint security solution. Adopting a next generation endpoint solution has made a positive impact on several levels for FCX. We no longer need to constantly reimage machines, improving business processes while saving time and money, and we have been able to refocus staff members.

Each organization will have different needs with varying levels of technological maturity and readiness. In our case, the relative uniqueness of our business required an extensive effort to roll out an advanced endpoint solution. Those with a more homogeneous environment may have an easier time with the implementation. Focusing on the behavior of the solution and artificial intelligence rather than the standard signature-based approach can lead to false positives. It is important to test it in your environment to determine what is most effective in your situation.

NATIONAL LIFE GROUP

Andrew Speirs
Chief Information Security Officer

COMPANY OVERVIEW

National Life Group is one of the top 20 life insurance providers[1] in the United States – and is also the fastest growing[2], passing the $100 billion mark in 2016. To support this growth, National Life Group has been investing in technology and plans to increase its spending on technology infrastructure to improve services for the business, for customers, and for employees. The company also has been bringing more of its technology back in-house.

Based in Montpelier, Vermont, National Life Insurance Company, the flagship of National Life Group, was chartered in 1848 and now has more than 1,200 employees divided among campuses in Montpelier and Dallas, Texas. The company also has about 400 contractors and 15,000 agents that sell products and services. In addition to life insurance, National Life Group's family of financial services companies offer annuity and investment products[3].

National Life Group is a high-touch operation, and our servant-leadership mindset has really taken off with our distribution force. Peace of mind is very important to us, as that is what life insurance products deliver to customers.

BUSINESS USE CASES

Our main business objective for implementing a next generation endpoint security solution is to ensure that our data is secure and our brand is protected. This type of solution supports our "defense-in-depth" strategy while enhancing the productivity of our employees and associates.

We want to ensure that our staff has the latest protection and detection technology. Moreover, it's important that patching and security management are done in a way that is seamless to our internal customers.

National Life Group has been in business for more than 160 years. From a reputational standpoint, it's of utmost importance that we protect our brand and guarantee that we are here for another 160-plus years.

TECHNOLOGY ENVIRONMENT

Until recently, as CISO I was the primary in-house security professional. We changed that dynamic in 2015.

Today, while we still leverage many outsourced services, our security resources are approximately 60 percent outsourced and 40 percent insourced. We built our new security team to coincide with our company's vision, which sees security as a strategic investment.

From a technology environment standpoint, we straddle mainframe, open systems and the cloud. An outside vendor runs the infrastructure services, and another does most of the .Net application development.

We have adopted a cloud-first strategy. Various applications are already in the cloud and we are looking to expand our usage. We are using various platform-as-a-service providers.

We rely heavily on a virtualized environment to provide our employees and our associates access to data and resources. It is critical for us to provide our clients a great user experience on any device. For that reason, we need an endpoint solution that protects our data on disparate endpoints.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

We look at endpoint protection to safeguard our brand and enhance our employee productivity. We invest our focus and energy to ensure our associates have a productive endpoint experience. With our next generation endpoint solution, our employees can continue to do their jobs unimpeded, while from a security standpoint, we have visibility all the way to the endpoint.

We can quickly identify a potential problem and then isolate an endpoint and mitigate any harm. Because of our virtualized environment, we also want to ensure that our users are minimally disrupted in the event of a problem, and that we can get them up and running again very quickly.

KEY FACTORS TO CONSIDER

It is important that CISOs continuously assess their security posture. When looking at a next generation endpoint solution or any burgeoning technology, they need to ensure that it works in their environment and is in line with their corporate objectives. From a technology perspective, CISOs should ask themselves if integrating next generation endpoint security would provide them visibility and the ability to proactively stop attacks while potentially simplifying their security stack.

The solution also must be cost effective over the long term. When determining this, it is important to consider the overall total cost of ownership, including the resources that are required to properly integrate, engineer and maintain the solution. CISOs also should consider whether specific subject matter experts are needed and readily available to implement, manage and support the solution in their particular environment.

The endpoint protection space and associated technology are constantly changing. It is essential to have a meaningful relationship with the chosen vendor and that the vendor functions as a partner. Regardless of the size of the client organization or contract, the vendor must be responsive to the organization's needs. As CISOs, we don't have cycles to push vendors on how to think through helping us be more productive. Many of us have to do a lot with a small amount of resources.

1. LIMRA Sales Rankings, 4Q2016, for individual life insurance sales
2. LIMRA Sales Rankings, 4Q2016, among reporting life insurance companies with individual life sales of at least $50 million in 2006.
3. National Life Group® is a trade name of National Life Insurance Company, founded in Montpelier, VT in 1848, Life Insurance Company of the Southwest, Addison, TX, chartered in 1955, and their affiliates. Each company of National Life Group is solely responsible for its own financial condition and contractual obligations. Life Insurance Company of the Southwest is not an authorized insurer in New York and does not conduct insurance business in New York. Equity Services, Inc., Member FINRA/SIPC, is a Broker/Dealer and Registered Investment Adviser affiliate of National Life Insurance Company. One National Life Drive, Montpelier, VT 05604. (800) 344-7437. TC96388(0717)1

For National Life, we had to consider if the solution was cost effective, and whether it easily integrated into our security operations center (SOC), patch management and incident response systems, and other processes.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

We had several important criteria that drove our selection of a security solution, including the following:

- Lightweight agent – The agent that observes and helps detect malicious activity has to have a small footprint and be non-intrusive to end users.
- Increased visibility – We need to know what, if any, malicious behavior is happening across all our endpoints.
- Seamless integration – The solution has to fit right into our existing environment with minimal integration efforts and minimal impact on current infrastructure and operations.
- Forensic data – We want to get deep forensic data at the endpoint level to aid our investigations and support mitigations.
- Ability to quickly stop the "badness" from occuring – Detection is not enough; we want to quickly stop bad things from running in our environment.
- Regulatory impact – The solution has to support and advance our regulatory compliance efforts to include robust reporting.
- Signal-to-noise ratio – We want the solution to raise meaningful alerts without overwhelming our security operations center.
- Total cost of ownership – The total cost of the solution must be within our budget resources.

We particularly value the ability to leverage the data the next generation endpoint solution collects through integrated feeds, which allows us to detect and alert on threats. It's also important that we can quickly and effectively isolate infected hosts. As well, we want a solution that is proactive and prevents incidents, like ransomware, regardless of our patch level.

A goal for our security team is to continuously strive to move closer to having a single pane of glass, which allows us to onboard security associates more quickly and leverage our solutions more effectively. This lets us simplify our technology stack and enables our team members to be more productive in their use of these tools.

OUTCOME AFTER IMPLEMENTING AN ENDPOINT SECURITY SOLUTION

We began looking in 2013 for an endpoint solution to bolster our security operations center. We knew things were occurring in the environment, but we didn't have a clear picture.

Through our technology vendors, we have a security operations center, have a handle on the Dark Web, and are able to spot indicators of compromise. But when the first pieces of ransomware were coming out, like most companies, we were worried about being vulnerable.

It wasn't until we started deploying advanced endpoint security agents in our environment that we actually had full visibility. It was a night and day difference. Now we can see the processes that are running, and, if we need to, we can isolate a machine and stop the "badness" from happening.

IMPACT ON STAFFING LEVELS

With our new focus on security as a strategic investment, we have moved from around 93 percent outsourced to 60 percent. We're standing up our capabilities and getting new people on board.

In terms of staffing levels, I wouldn't say that our endpoint solution has resulted in any sort of direct impact or cost savings related to human resources. However, we have seen success in that the endpoint technology has enabled our team to focus not only on preventing catastrophic events but also on cyber protection and resilience.

IMPACT ON STANDARDS AND REGULATIONS

When we look at endpoint solutions from a standards and regulations standpoint, compliance is always important. At National Life, we think about protecting our data and our brand while providing cyber resiliency. We think about what the right solution is. It's not about checking a compliance box.
When we invest in a product we focus on the capabilities of a defense in-depth strategy, a respect for our budgets, and a productivity gain when we can get it because we're not chasing our tails with noise in the system.

THE OHIO STATE UNIVERSITY

Helen Patton
Chief Information Security Officer

COMPANY OVERVIEW

The Ohio State University (OSU) is a top-ranked research university with 66,000 students and 45,000 employees. OSU has operations in multiple countries with campuses around the world. The university operates teaching hospitals and clinics, and even has a nuclear reactor on the main campus. In addition to providing a world-class education to our students, the university conducts, funds and supervises research valued at $847 million.

The Information Security team is comprised of 50 people who, along with others that are embedded in each of the colleges and various business units, are charged with protecting the privacy, confidentiality and security of the information entrusted to and generated by the university.

BUSINESS USE CASES

OSU has many drivers for information security. Regulations like PCI, HIPAA and FERPA all require stringent information security management. As a research university, OSU has funding agencies, sponsors and business partners that demand information security and privacy protection. The university has a duty to protect the confidentiality and security of the financial, healthcare and educational records of its students, faculty and administrators.

In addition, universities like OSU that generate and exchange vast amounts of valuable research information are frequently the target of attacks by malicious actors attempting to acquire the proprietary intellectual property for the purpose of economic or other espionage activities.

Add to that the need to provide students and guests a safe, secure and reliable infrastructure so they can do what they need to do – all within the setting of an open and distributed environment – and it all results in significant business drivers with substantial challenges.

Technology is changing so rapidly, to the point where people are carrying large amounts of data on mobile phones, accessing university information from across the globe, and sharing critical information on large scales. Standard network security is no longer enough to be able to protect the information, as traditional networks are being replaced by user-based borders.

We have to protect all of this without impacting the privacy and academic integrity of the people whose endpoints we are managing. It's a very delicate balance, and this is why we are investigating advanced endpoint protection tools.

TECHNOLOGY ENVIRONMENT

In higher education, it's typical to have a highly decentralized environment with each department or college being responsible for its own IT operations. As a result, there's a great deal of heterogeneity in our environment, which can make it a challenge to manage.

As we look at endpoint protection, we are prioritizing the need for a solution that works in both a centralized and a highly distributed environment, and one that works well across a range of devices and various operating systems and programming languages.

We are looking for a tool that will give us as much visibility into the endpoint as possible, regardless of where the endpoint is, or the condition it's in. Because of our diverse environment, we want to ensure that our preferred endpoint solution has a small footprint.

The user experience is another important criterion. We don't ever want a security tool to get in anyone's way. For example, if a researcher thinks that a tool is limiting their ability to process data, they are going to disable or uninstall it. So, it's important to us to have a next generation endpoint tool that, as much as possible, is transparent to the end user.

Most endpoint analytical tools that look for threats do this by learning to identify typical user behaviors, and then identify anomalies that stand out from common behaviors. OSU has a wide variety of users, from college students, to researchers, to faculty, to administrators.

What is considered to be "normal behavior" is going to vary greatly from person to person, and department to department. Role-based behavioral monitoring is critical, but it's also complicated by the fact that we do a lot of job sharing. From a next-generation, behavior-based analytics perspective, this might present certain challenges—particularly the difficulty in getting a common behavioral baseline from which the tool can identify meaningful anomalies.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

I think of information security in terms of three lenses. First, can my team identify and remediate issues as quickly as possible? Second, do we have awareness and a culture of security within the organization? And third, do we have the right technology hygiene that's going to be able to do the basic blocking and tackling that needs to be done to keep the environment as good as it can be?

Endpoint analytics can help identify risky configurations or behavior in our environment, which we can then ameliorate with additional training and support. That allows us to target our governance, training and awareness programs to the areas and people where it will have the greatest impact.

There's a lot of basic technology operations work that needs to be done in order to allow the next generation of tools to do the advanced analytics that they promise. For instance, we have to make sure we have things like asset and inventory management; configuration and patch management capacity; and intrusion detection, isolation and prevention. That's all basic hygiene. Once we get those ducks in a row, we can build on that foundation with more advanced solutions.

From a business perspective, next generation endpoint protection has the ability to be more efficient and effective, largely by replacing multiple tools. But we can't remove all the legacy tools at one time, and there's a good deal of cost and pain associated with the transition.

KEY FACTORS TO CONSIDER

Before you transition to any advanced endpoint solution, you have to consider whether your organization has the maturity to be ready for such tools, and whether you will get value from them. Endpoint solutions have the capacity to generate a great deal of data about how the endpoints are functioning, but if you don't have the right data analytics platform, you're going to be overwhelmed. The same thing is true with visibility. If you gain visibility into what's really happening with the endpoints, what are you going to do with that information? How are you going to decide what's important and what's not, what you have to pay attention to, and what you don't?

For example, being able to examine, at a granular level, exactly what files are coming into and out of the enterprise is a very powerful capability, particularly if you are a bank or a brokerage house. But as an open university dedicated to free expression, we also have to consider the privacy impact that using such a tool might have on students, faculty and researchers. It's not enough to have the capability. You have to ensure that you have policies and a culture that will support the use of these capabilities and, for us at least, to be as transparent as possible in the deployment.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

A critical factor in selecting an advanced endpoint solution is to examine the ease of operations for the people who are going to be running it on a day-to-day basis. The goal is to help find true threats and true attacks—to find a particular needle in a haystack of needles. You want to ensure that the solution is not generating a lot of false positives, and can integrate with your other security and IT operations tools already in your portfolio.

For the most part, the endpoint security vendors are offering similar solutions, so I look at things like what kind of customer service I can expect to get from the vendor. This includes not just the tool itself, but whether the vendor will partner with the university to provide student scholarships, in-depth training for technology support staff, and even training for university executives.

OUTCOME AFTER IMPLEMENTING AN ENDPOINT SECURITY SOLUTION

The most significant thing for us is not only the number of vulnerabilities or incidents that the advanced endpoint solution is able to find over and above our existing toolset, but the speed at which these threats can be found. When it comes to being able to detect and respond to threats, speed is critical. Also, the advanced endpoint solutions can be much more efficient, particularly in terms of their processing footprint and impact on our organization.

IMPACT ON STANDARDS AND REGULATIONS

The university is subject to a wide variety of federal, state and international security and privacy regulations, including HIPAA, PCI, FERPA, and Ohio state regulations as well. This presents a challenge, as sometimes the regulations conflict with each other or with what we believe we need to do. For example, we have a certain regulatory requirement that says, at least on paper, that we must have traditional signature-based antivirus in place. If we follow the letter of the law, it's hard to get rid of our existing tools and replace them with advanced endpoint protection because our regulators are not yet comfortable with the next generation of tools that, in reality, offer better protection than traditional AV products.

PEER RECOMMENDATIONS AND ADVICE

Only implement an endpoint security tool if you can use it to achieve a better security posture, not just compliance with regulations. Your enterprise must be mature enough to deal with the information generated from these platforms, and you must have the capacity to respond effectively to what the endpoint data reveals.

SUMMARY

Information Security is about enabling people at the university to fulfill their mission without putting sensitive or critical information at risk. At The Ohio State University, we have an extraordinarily large number of people with disparate jobs and missions, and they need to achieve their goals over a wide variety of devices and network segments. To the extent that advanced endpoint solutions can help manage the chaos, with minimal impact on throughput and the ability to function, it's a great asset. We believe that being well prepared to deal with the data an endpoint tool generates will be key to our mission's success.

OPPENHEIMER & CO.

Henry Jiang
Chief Information Security Officer

COMPANY OVERVIEW

Oppenheimer & Co. Inc. is a leading investment bank and full-service investment firm that provides financial services and advice to high net worth investors, individuals, businesses, and institutions. For over 130 years, Oppenheimer has provided investors with the necessary expertise and insight to meet the challenge of achieving their financial goals. Oppenheimer's commitment is to clients' investment needs, with experienced and dedicated professionals, and a proud tradition to deliver effective and innovative solutions to clients.

Reported results for 2015 include client assets under administration totaling approximately $78.7 billion, while client assets under management that were fee-based totaled approximately $24.1 billion. Oppenheimer employs roughly 3,200 employees.

BUSINESS USE CASES

For financial services companies, the priority of cybersecurity controls primarily resides with prevention and detection controls. And some would argue that the prevention carries more weight than the detection.

For some organizations, isolation technology can be too resource intensive as it does require substantial memory and processing powers on the endpoints. But in organizations where the endpoint environment is standardized and tightly controlled, there's an opportunity to use advanced endpoint protection technologies like micro-isolation. That allows for quicker remediation of infected machines with lower staffing requirements.

TECHNOLOGY ENVIRONMENT

The financial services industry is one of the few sectors where users work in a heavily controlled environment, so that every endpoint that would deploy the endpoint protection technology would be a firm-managed asset.

That means that a computer's image is standardized. Only certain programs are allowed, and only certain browser behaviors are allowed. It's very much a purposely-built environment that's deployed to all the machines.

That allows financial services companies to look at vendors that operate well in these kinds of tightly-managed environments that wouldn't work in, say, a media company that has Macs and other types of machines.

A lot of firms in other industries aren't in the same position, and won't be able to roll out the same kind of isolation technology to the same degree.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

Many financial services companies are facing a situation where employee machines are infected with malware and need to be reimaged. That is a time consuming and expensive process. In addition, if the infection isn't noticed instantly it has the potential to spread quickly to other machines, such as what happened with the WannaCry ransomware in the spring of 2017.

The ideal solution would not interfere with the way the employees do their jobs, eliminate the need to reimage infected machines, and prevent infections from getting into the environment in the first place – all without requiring a large number of new employees to manage the technology.

KEY FACTORS TO CONSIDER

Even in a strictly controlled environment like a financial services company, you still have some variety – legacy software, cloud-based applications and also home-grown applications running in your environment. The endpoint protection solution needs to be able to work with all application types.

In fact, the endpoint solution protection should be application agnostic. It should work with all application types.

Having said that, a common initial infection vector of malware is via Microsoft Office applications such as Microsoft Word or Excel with macros enabled, or PDF reader, or, in some cases, the direct file access to executables or scripts that load on your endpoint. These attack vectors are primarily coming from the Internet, email and Web browsing activities.

These email attachments or browser activities represents the majority of endpoint infections, and therefore deserve an effective, automated prevention control in this space.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

A common mistake when selecting a vendor is to take the vendor's words at the face value. Instead, companies should perform their own due diligence by using real life examples to test and validate the vendor's claim in an environment that closely resembles their operating conditions. The vendor will probably provide their own examples, but they might not be the most relevant test. Instead, use the latest examples of malware that are actually hitting your company, which is specific to your industry and risk profile. There should be plenty of them. That is a better way to gauge the effectiveness of the security solution. Security teams should take their time with the testing, so that they can see what really works, and what doesn't work. It doesn't take a computer science genius to do that. However, to be effective it is important to develop a plan on what to test.

OUTCOME AFTER IMPLEMENTING AN ENDPOINT SECURITY SOLUTION

One way to secure endpoints is to run downloaded executables in an isolated container. That means that for a hacker who gained a foothold on an endpoint via initial exploitation, when the commands are being executed, this adversary is not going to be infect or discover other parts of the system, nor network resources.

It's literally multiple virtual machines that are created on the fly on the computer. Everything is containerized within its own bubble.

So, think about this scenario. You have a zero-day. The virtual instance of the application gets infected. Guess what you need to do in order to contain that? Or eradicate it? Just close that browser. Simply close the affected applications, and the malware instance will dissolve automatically. What do you have to do with the machine? Nothing. You don't have to reimage the machine.

That means that a company that previously used to reimage infected machines no longer has to do that. There is no downtime for the user.

This isn't the same as sandboxing. With sandboxing, you run the analytics in a different area so that you can determine if an unknown application is good or bad. But the sandboxing is going to take time to go through the analysis, three minutes, five minutes, 10 minutes, or even longer. Meanwhile, if it's already in your environment, you're going to get infected. Firms do not want to take any chances and have a three or five minute window in which a machine can get contaminated while sandboxing is doing its job.

Take the WannaCry ransomware as an example. If one machine gets infected, it self-propagates quickly through your network. It only takes one.

IMPACT ON STAFFING LEVELS

Lots of advanced endpoint solutions emphasize the data they collect. But if you don't operate in an environment where you can have a dedicated team to play with the data and collect the analytics, then it isn't the ideal solution.

With large companies, you can have people dealing solely with the forensics and analytics. That's their full-time job. They can piece everything together. But if you don't operate in that type of environment, you've got to stop things first, and analyze later.

IMPACT ON STANDARDS AND REGULATIONS

There are regulations that require companies to have traditional antivirus protection in place. Some people are concerned and they say that antivirus is dead.

I don't believe that to be the case. Traditional antivirus products, even when it's free or very low cost per user, still works. It still has a huge value, and costs so little. Why not keep them in your security stack?

Advanced endpoint protection and antivirus complement each other, rather than replace each other. You need to have all those layers working.

PEER RECOMMENDATIONS AND ADVICE

If a firm is operating in a heavily sterilized environment, with sanctioned assets, centralized patch management, and a centralized image process, it should certainly consider an endpoint protection solution that offers micro-isolation or something similar. The focus should definitely be on endpoint for those organizations.

For organizations that cannot afford, either by policy or just by nature of the business, to put an emphasis on endpoint, certainly they need to move the protection layer to the edge, such as a cloud access security broker or a cloud-based web proxy, or an email gateway.

SUMMARY

For firms operating a centralized, controlled environment, like most financial services firms are – and I'm sure maybe other sectors as well – the endpoint really is the most effective area for security controls. That is where you should invest your resources. And if you have the staff and financial wherewithal, an advanced endpoint solution with micro-segmentation is definitely worth considering as it can be very effective in preventing the spread of malware.

PERDUE FARMS

Tunde Oni-Daniel
Head of Information Security

COMPANY OVERVIEW

The Perdue brand is the number-one brand of fresh chicken in the United States and Perdue AgriBusiness is an international products and services company. We were founded in 1920 and are based in Salisbury, Maryland. We have more than 22,000 employees and more than $2 billion in sales with more than 180 locations across the United States and South America.

Perdue Farms is the family-owned parent company of Perdue Foods and Perdue AgriBusiness. We are dedicated to enhancing the quality of life for everyone we touch through innovative food and agricultural products. We are committed to making Perdue the most trusted name in food and agricultural products through our Perdue, Harvestland and Coleman Natural food brands, through our agricultural products and services, and through our stewardship and corporate responsibility programs.

BUSINESS USE CASES

For Perdue, it's all about protecting the brand. We don't really collect a lot of private information from customers, so our security focus is really about protecting our brand and employees. We have to make sure that we are able to secure not just our manufacturing, but also our salespeople, our brokers and users as they connect through our systems.

The main business drivers for both security in general and for endpoint security in particular are to ensure that we are computing better, sharing smartly, and of course, that we are secure. We also are trying to minimize the risks associated with conducting business in an environment that is heavily dependent upon technology.

In addition, we are concerned about risk. Members of our Board of Directors read the media and see what is going on with respect to cyber threats and vulnerabilities and are understandably concerned. They are acutely aware of the nature of the risks in cyberspace, and are committed to protecting our brand, our people and our partners as well as the public at large.

From a manufacturing perspective, we are also part of the nation's critical infrastructure. We work with both the Food and Drug Administration and the Department of Homeland Security to ensure that our manufacturing and processing plants are secure. This also means securing the IT environment in which they operate.

Even though we were managing our endpoints, with the evolving threats we were seeing a proliferation of viruses and malware. We were particularly concerned about ransomware – one or two instances of ransomware can be a very humbling experience. We decided that we had to move more into the advanced endpoint protection space.

TECHNOLOGY ENVIRONMENT

The IT environment at Perdue is extremely diverse. At the corporate offices in Salisbury, we maintain a hyper-converged environment that has a mix of business-driven applications. Perdue uses a good deal of cloud-based applications and we use our IT environment for a broad range of things from logistics, to transportation, to communications.

We have a cross section of users that we have to protect – our partners, our customers, the public, and, of course, our people. In those different segments, we have to safeguard them in different shapes or forms based on what they have access to. Specifically talking about the endpoint, we started to see a lot of problems where the endpoints were getting compromised, and as a result infected laptops would have to be shipped back to us to be rebuilt.

We needed something more than simple antivirus and anti-malware. We wanted to meld our InfoSec capability around endpoint management and provide true incident response.

We adopted a solution that uses sensor-based intrusion detection and protection to examine connections to the cloud and monitor for unusual activity.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

Aside from our primary goal of protecting our brand and reputation, and just minimizing risk, we also wanted a solution that would allow us to work with our vendors and suppliers, employees, brokers, sales staff and others. We wanted them to be able to connect to us securely from anywhere. A lot of our sales staff are true road warriors, and we need them to be able to work from Panera, Starbucks, their mobile devices – anywhere they can get a connection. So for us, it was about connectivity as well.

We decided we had to make some modifications around how we did endpoint protection. In order to truly meld the whole capability around endpoint management to true incident response, we needed to look at something that basically worked across the endpoint detection and response space as well as provided us with next generation antivirus capability.

As an added benefit, better endpoint protection means that we don't have to incur the cost of shipping devices back and forth. We reduced spend from a shipping perspective, while freeing up team members to do other key security-related tasks and reduced downtime for users.

KEY FACTORS TO CONSIDER

We were looking for an endpoint solution that baselines what the normal endpoint behavior is, how that normal behavior is supposed to really function, and then blocks or terminates anything that deviates from that. The solution also needed to send a notification to the incident response team and also send a notification to the user. My team could then understand how things occurred, what the user clicked on, and exactly what the application was trying to do on the endpoint.

A lot of the traditional antivirus-based solutions are basically dated at this point. They're searching for the low hanging fruit. Based on my team's analysis and research, only 10 percent of all the alerts would have been caught by traditional antivirus. Over 60 percent of the new types of malware that are coming in may not be detected by traditional antivirus and are trying to impersonate an actual user.

But there are things that a user should not do.

For example, if you find that something is trying to run privileged commands on the endpoint, you know that's not supposed to be there. Those are the kinds of things you are looking for advanced endpoint solutions to detect, based on what type of activity is known as normal, and what's known to be abnormal.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

There are a number of technological milestones we looked at when assessing an advanced endpoint solution. That included determining things like, how light is its footprint? What resource dependencies does it have? How well does it integrate? How well does it report? How well is it manageable? Does it have any dependencies from management perspectives?

For instance, if I have this particular solution, do I have any browser-based plugin dependencies to administer the solution, or do I have any other applet dependencies I need to use? Do I have to keep any historical material in the environment?

From a log retention perspective, I have to consider how long the provider actually forensically retains logs. I also ask whether the solution is able to work across platforms.

OUTCOME AFTER IMPLEMENTING AN ENDPOINT SECURITY SOLUTION

The biggest benefit Perdue experienced after implementing the advanced endpoint solution was our ability to really see where we stand across the enterprise. For us, this included the ability to see vulnerabilities and potential exploits on our shop floor, and to protect the manufacturing capabilities without having to worry about operational downtime. With all of our custom code and processes, this was a huge benefit, and something we were unable to achieve before. Part of that success is because we went through extensive testing before we deployed any solution.

Another highlight is the ability to have a centralized dashboard, where we can see across the enterprise. This allows us to prioritize staffing and other resources.

IMPACT ON STAFFING LEVELS

The new endpoint solutions didn't impact the number of our staff, but it did allow our existing security staff to focus on things that are more important. The folks that worked on the endpoint are now working on the dashboard to ensure that it's properly maintained and the logs are being properly processed, and they're making the decisions about what to do next.

IMPACT ON STANDARDS AND REGULATIONS

We generally look to the ISO 27001-2013 and the NIST cybersecurity framework for guidance on how to implement security processes. I think the NIST guidelines have more well-defined controls so we use that for our corporate controls. This is important because we are a part of the nation's critical infrastructure, so security and resilience is equally as important to us as is compliance. The ability of endpoint security technology to identify and help us mitigate risks is part of the overall philosophy of NIST and ISO.

PEER RECOMMENDATIONS AND ADVICE

The most important thing for CISOs to consider when thinking about implementing endpoint protection is not whether it will work, but whether it will work in their environment. For example, at Perdue, we took a long time to vet the solutions and to deploy them in a test environment to determine which one worked for us. CISOs need to make certain that they're working with vendors or partners who will allow them to truly assess direct feasibility within their environment and how well it works before they make a determination on what to do.

SUMMARY

At Perdue, our business operations demand a high degree of security and a light touch on the manufacturing floor, while not disrupting our manufacturing operations. Our next generation endpoint solution helps us do that in a way that really gives us visibility into our security status at any point in time. This all comes back to our mission to protect our brand, our people and our partners as well as the public at large.

Consider the different platforms and versions of platforms supported by the technology providers to understand what percentage of your environment would be covered.

RWJBARNABAS HEALTH

Hussein Syed
Chief Information Security Officer

COMPANY OVERVIEW

RWJBarnabas Health (RWJBH) is the most comprehensive health care delivery system in New Jersey, treating over 3 million patients a year. It is New Jersey's second largest employer – with more than 32,000 employees, 9,000 physicians and 1,000 residents and interns. The system includes eleven acute care hospitals, three acute care children's hospitals, a leading pediatric rehabilitation hospital (Children's Specialized Hospital), a freestanding 100-bed behavioral health center, ambulatory care centers, geriatric centers, the state's largest behavioral health network, comprehensive home care and hospice programs, fitness and wellness center.

BUSINESS USE CASES

As a CISO at a healthcare organization, my role is to ensure that systems responsible for patient care and treatment are up and running and accessible to practitioners, medical staff and other patient care providers 24/7.

Endpoint protection is paramount to achieving this goal. At RWJBarnabas, there are a number of different specialty care facilities. For example, within the acute care facility there are specialized facilities for cardiology, renal transplant, pancreatic transplant, heart transplant, and oncology services. In addition, physicians travel around the world promoting healthcare and healthy living, and fostering the goals and objectives of the Robert Wood Johnson foundation as well. It's all about furthering the mission of the hospitals and healthcare facilities. Antivirus and anti-malware programs are primary, but not exclusive, tools to protect the data and functioning of computers involved in healthcare operations.

Healthcare is a very complicated business model just by the way it's designed, and the way it has evolved over time. For example, we have applications that are hosted internally, while others are external, and they are accessed through PCs, laptops, or tablets. What is important is how information flows through the system – from the time a patient walks in and gets registered to the time they are discharged and treatment and billing ends. Understanding Electronic Health Records (EHR), telemetry, medical device security, infusion pumps, MRI-type machines, connected laboratory equipment and devices, clinical systems, and remote access is critical to meeting the mission of the hospital. Endpoint protection is paramount to achieving security of all of these devices.

CURRENT TECHNOLOGY ENVIRONMENT

RWJBarnabas currently relies on the proper functioning of thousands of connected mobile workstations for patient diagnosis and care, as well as cloud-based EHR systems for patient records. The primary endpoint protection strategy relies on antivirus and anti-malware products to secure these devices from malicious code, coupled with layers of compensating controls to monitor and respond to other potential threats. These controls include continuous monitoring solutions, encryption and authentication, and limiting what can run on individual devices. Data Loss Prevention (DLP) solutions also help stop the migration of sensitive information or PHI outside the controlled network.

The team is looking into more advanced endpoint protection systems, and a key consideration is balancing their costs and benefits. We know that we will eventually move to a more advanced solution – one that will permit a greater degree of monitoring of the endpoints and automate the process of threat analysis and response, but it's a tradeoff. What's important to RWJBarnabas is the ability to maintain control over the data and network, to be able to see what is going on, and to be able to respond effectively to current and new threats. We are looking at how best to leverage our existing IT resources and staff, and how best to outsource what can more effectively be outsourced. Like other healthcare providers, RWJBarnabas is cost sensitive, and we have a large investment in current solutions. We want to get the right mix between what we 'insource' and what we 'outsource,' what we purchase and own, and what we license and rent.

TOTAL COST OF OWNERSHIP

The total cost of ownership (TCO) for a desktop or a laptop usually turns out to be almost double what the organization has to pay for the physical hardware. For example, when you buy a PC for X hundred dollars, you have to buy antivirus software, asset management software, Windows licenses and the data leak prevention (DLP) controls on those machines. Once the device is totally configured, you're almost looking at double the cost of that unit by the time you acquire it and put it on somebody's desk to be used. That becomes a very touchy subject when you're looking at budgets and how you're going to secure the environment with the given amount of operating or capital expense you have. One of the primary goals of our endpoint protection strategy is to ensure that we get the most value from our assets. We continuously reassess our security needs and objectives. When the functionality of more advanced endpoint solutions is more comprehensive than our existing solutions, we will reexamine the potential benefits verses the cost.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

The main goal we are trying to achieve in terms of endpoint protection is to provide our clinicians and business users a computer that will let them do their job without interruptions and without unacceptable risks. They shouldn't experience any downtime because they were infected by malware. The same is true with respect to preventing and mitigating harm from phishing attempts. We try to lock down any data coming into and out of our enterprise, and minimize the risk of exfiltration.

KEY FACTORS TO CONSIDER

When evaluating endpoint solutions, we have to consider the harm we are trying to prevent. Having a centralized management and threat analytics console that provides visibility into our environment is critical. For us, the most important thing is ensuring availability of data, and to make sure that our clinicians and business users have access to data on workstations, tablets or other devices all the time. We also need flexibility, in particular the ability to integrate with our Security Information and Event Management (SIEM) system and our Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) engines, to provide alerting, and to give visibility into the current threat environment.

Our decision to focus currently on antivirus and anti-malware as our primary endpoint solution is based principally on the current operating environment, cost, and the fact that we have a wide variety of compensating controls to help us protect the data we work with every day. In the future, we expect that our endpoint protection strategy will expand beyond the current antivirus, anti-malware model to more advanced behavioral-based detection, depending on our needs, the threat, the regulatory environment and our overall budget. Many of these advanced detection applications are subscription based, and would add significant cost. While they deliver value, we have to decide whether they fit our current needs and within our current budget.

We examine cost, but not in the traditional way. First, we look at needs. What problem does the proposed technology purport to solve? What is our exposure? What risks are we taking? After that, we look at how well the new technology solves our problems, and then finally its cost or value. We also look at our own compensating controls. For example, we do a lot to lock down the individual workstations and restrict access to certain data. When evaluating an endpoint solution or any other solution, we look at our overall security posture.

When we view costs, we look at multiple factors. What will be our total cost of running the product or service, including training, maintenance, upgrades, and integration? Will the proposed solution increase or decrease our overall headcount? We also have to consider how to prioritize our human capital – how we want to use our resources and what we want to focus on. Should we run the product or service ourselves, run it through the cloud, or outsource it completely? And if we outsource, do we outsource management, monitoring, remediation, or everything? We are taking it cautiously.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

In selecting a vendor, both visibility and flexibility, as well as the ability of the endpoint security technology to provide an automated method of notification, are the kinds of things important to our decision-making process. We prefer to have a dashboard that will let us know on a daily or even hourly basis what our overall security posture is, and which prioritizes potential threats accordingly. In the future, we will be looking at solutions that support advanced threat analytics, but right now we are getting focused on protecting the data we know is at risk.

IMPACT ON STANDARDS AND REGULATIONS

Of course, any solution has to "check the box" for compliance. In our current environment, this primarily means compliance with HIPAA privacy and data security requirements, as well as the NIST Guidelines, and in the future, will likely include and expand PCI-DSS requirements. Our current mix of antivirus and anti-malware solutions, together with DLP solutions, checks these boxes. However, we also will have more sophisticated PCI compliance requirements and general security needs. We want to ensure that we are doing more than just checking boxes. That's why we continue to evaluate products that go beyond compliance to ensure visibility and resilience.

PEER RECOMMENDATIONS AND ADVICE

No single solution fits all of the needs. Our primary goal is to maintain uptime, and our current solution meets our current need. But as the threat environment evolves, so will our needs, and we expect to be evaluating more endpoint vendors in the near future. We meet regularly with other CISO's, both in the healthcare and non-healthcare fields, to share experiences.

RWJBarnabas is in the process of evaluating advanced endpoint solutions based on their experiences with respect to functionality, flexibility, visibility and total cost (including personnel costs), and we are deciding what mix of solutions will fit our specific needs. Compensating controls will always be necessary, but in the current threat environment – especially with the increase of successful ransomware attacks at healthcare institutions – they may not be enough. Advanced endpoint solutions may provide more "bang" for more "buck." CISOs know they will ultimately implement advanced endpoint solutions – but will do so thoughtfully. It must be done as part of a comprehensive security program, rolled out in a thoughtful and intelligent manner. We must consider the impact on network performance and service delivery, as well as cost, control and security value. The solution has to fit within our environment. At RWJBarnabas, we know we will be moving to advanced endpoint eventually. It's all about how, when and which mix of solutions.

PEER RECOMMENDATIONS AND ADVICE

CISOs should consider the signal-to-noise ratio of endpoint protection. You want to ensure that whatever solution you select provides useful information in your environment without generating too much noise, either to your security team or to your end users.

A next generation endpoint solution should identify and block malicious activity before it reaches the end user. The solution needs to do this regardless of your patch level. For that, we looked beyond signature-based identification to behavioral-based next generation endpoint solutions.

Experienced security professionals know to “assume compromise;” that is, that malicious activity is already inside the environment despite a robust set of perimeter defenses. Thus, we sought a solution that would be looking for abnormal behavior. A good next generation endpoint solution will have already patterned that information and tell you, "that's bad behavior," and it will stop it regardless of patch level. This doesn’t mean you shouldn’t patch, but rather provides an extra layer of protection.

SUMMARY

Endpoint solutions have allowed us to provide additional layers of security while simplifying our stack to meet our overall business and technology objectives – to protect our brand and protect our data. It gives our associates greater confidence and reduces our downtime, while allowing our IT security staff to focus on building a more resilient network to guarantee that we will continue our growth and be servicing clients 160 years from now.

WESTERN DIGITAL CORPORATION

Geoffrey Aranoff
Vice President, Information Security

COMPANY OVERVIEW

Western Digital is an industry-leading provider of data storage technologies and solutions that enable people to create, leverage, experience and preserve data. The company addresses ever-changing market needs by providing a full portfolio of compelling, high quality storage solutions with customer-focused innovation, high efficiency, flexibility and speed. Our products are marketed under the HGST, SanDisk and WD brands to OEMs, distributors, resellers, cloud infrastructure providers and consumers.

BUSINESS USE CASES

Endpoint protection can help large enterprises in various ways. First, it successfully stops threats from delivering malware or executing an exploit, thereby moving the ability to detect and protect higher in the cyber kill chain. This helps drive towards a goal of minimizing the incidents that require an immediate response by adding a layer of advanced protection that recognizes and blocks more potential threats than typical antivirus solutions do.

Another major concern at large technology and manufacturing companies is protecting proprietary information and manufacturing processes from theft or other attack. It is important to safeguard against unauthorized data migration or worse, theft. To the extent that advanced endpoint protection can prevent attacks aimed at proprietary information, such endpoint protection in conjunction with other controls provides a high degree of protection for sensitive data.

It is important to evaluate the performance of any endpoints going into your environment. At a manufacturing company where it is imperative to protect manufacturing processes, it is also important to weigh endpoint solutions against the possible negative performance impact on processes and adopt solutions that will add the necessary protection with minimal disruption.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

A goal that can be considered when deciding whether to implement advanced endpoint protection is whether it will block more effectively against commodity threats on the endpoints when compared to normal antivirus. While many companies do employ other cyber controls, due to continuous phishing and global cyber campaigns such as the recent WannaCry and Petya outbreaks, it is important to consider a solution that allows companies to quickly add blocks to PCs and have a greater assurance that many advanced threats would be detected and stopped even without additional intelligence added to the solution; for instance, signatures.

By adding this layer of protection, it enables operational security resources to more quickly respond to and analyze ongoing threats, spending less time on threats that are identified by the advanced cyber tool.

Additionally, it adds an ability to quickly quarantine objects on systems that have been identified as advanced malware or exhibiting suspicious behavior, allowing time to further investigate.

KEY FACTORS TO CONSIDER

There are many factors to consider when evaluating advanced endpoint protection technologies. First, do they really detect a much higher percentage of non-commodity malware than normal antivirus? Many antivirus vendors have added features such as heuristics to increase their ability to detect malware. Second, can they block or contain the threats they identify or threats that users digest from other intelligence sources (other indicators of compromise that they have not yet been exposed to)? Finally, do they have other value such as fast scanning of the environment for identified threats or additional cyber forensic analysis capability for systems that have contracted malware?

One of the keys of a successful cyber defense strategy is to increase the ability to identify and contain an increased number of threats while decreasing the time to detect and remediate. Although I am not ready to call advanced endpoint solutions true full protection, they certainly move the needle in the right direction. Where a traditional signature-based antivirus solution may identify 30 to 40 percent of the malicious processes, and even fewer of the advanced ones, advanced endpoint solutions at least have the capability of detecting a much higher percentage of these malicious programs and include the ability to either sandbox or block a good deal of them.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

When selecting a vendor, it is key to determine the impact of advanced endpoint protection on our overall functionality of the endpoint. While endpoint providers will tell you about the benefits of the solution, they don't always readily identify the performance impact it may have on networks and applications, or may not know in specific environments.

It is important to understand your environment and the different performance thresholds vital to your company. It is also essential to consider the different platforms and versions of platforms supported by the technology providers to understand what percentage of your environment would be covered.

OUTCOME AFTER IMPLEMENTING AN ENDPOINT SECURITY SOLUTION

There is a variety of different theories on how to measure the effectiveness of cyber security programs. I am not a big believer in ROI studies prior to a technology purchase or solution adoption unless it can be based on real incidents where you can measure the difference in effectiveness if you would have had a different or additional technology or solution, and then apply real resource, technology, impact, and remediation costs. However, once technologies and solutions have been implemented, a CISO must be able to quantify success. In assessing the impact of deploying advanced endpoint solutions, you should see that detection and remediation times have decreased and be able to associate real costs with that decrease in time and the increase in bandwidth for the operational team.

IMPACT ON STAFFING LEVELS

Deploying advanced endpoint protection solutions doesn't really reduce the overall number of people in information security, but it can change the required skill levels and work required. The idea is that if a security program is successful (as defined in the above section) in detecting and mitigating advanced threats, then the program is spending less time and resources on detection and response, and therefore able to focus the personnel on other areas of security, such as protection and enabling more secure solutions. This change in focus will result in higher costs for resources due to the increased skillsets required, but the team will be adding more value and saving costs from potential security incidents going forward. Therefore, theoretically it does return a positive ROI over time.

SUMMARY

To the extent that advanced endpoint protection solutions are able to shorten the time from attack to detection and remediation, as well as providing automation for segregating and mitigating threats, they represent a substantial improvement over traditional signature based antivirus and anti-malware.

WISCONSIN DEPARTMENT OF HEALTH SERVICES (DHS)

Shane Dwyer
Chief Information Security Officer

COMPANY OVERVIEW

The Wisconsin Department of Health Services (DHS) is one of the largest and most diverse agencies in the State of Wisconsin. DHS is committed to supporting economic prosperity and quality of life by protecting and promoting the health and safety of the people of Wisconsin. DHS has an annual budget of roughly $11.5 billion and more than 6,100 employees. DHS oversees Medicaid, the single largest program in the state budget, and other health and social service programs.

DHS ensures that the services provided to Wisconsin residents are of high quality and provided in accordance with state and federal law; ensures that Wisconsin taxpayer dollars are being utilized effectively and efficiently by preventing and detecting waste, fraud and abuse; and works to continue Wisconsin's long tradition of strong health outcomes and innovation.

WHY SECURITY LEADERS SHOULD CONSIDER NEXT GENERATION ENDPOINT SECURITY

Attackers have their sights set on the healthcare industry. Health records contain protected health information, which also may include insurance and payment data. This type of information can be leveraged by attackers, which could have a more significant impact on identity theft and national security than other forms of data. Whereas the theft of a credit card can be remediated fairly quickly, it may take months for a compromise of health records to be discovered and remediated.

The valuable and varied amount of information we handle as a government agency makes DHS an attractive target, and defending against internal and external attackers is a constant battle. Complicating the situation is the fact that attackers know that state government generally has less funding (and potentially more vulnerabilities) than other often well funded Federal or private sector organizations. To complicate matters, organizations like DHS also outsource and engage with multiple third-party vendors, agencies, and partners – all of which potentially expose the organization to additional attack vectors.

From a business perspective, our primary goal is protecting and promoting the health and safety of the people of Wisconsin. To do that, we have to ensure that the data we collect, store or use is not compromised by either internal or external attackers. Traditional antivirus solutions are unable to provide the visibility into the spread of attacks within the network, or to allow us to stop the compromise of credentials which attackers use to pivot from attacks on the endpoint to other system resources. Advanced endpoint protection helps protect the entire network, provides visibility into the network, and allows for faster response to potential threats, all while improving compliance with privacy and data security regulations.

Ultimately, we report not only to legislative bodies, but to the people of Wisconsin. It is the people's expectation that DHS will implement appropriate measures to secure their data. The other business driver is to maintain the trust of the citizens of Wisconsin and instill confidence in our business partners.

THE TECHNOLOGY ENVIRONMENT WITH ENDPOINT SECURITY

When considering an endpoint solution, it's important to view the solution from the perspective of the entire technology environment. Not only are organizations faced with the issue of mobility and multiple, varied endpoints, but they operate with complex infrastructures that include multiple operating systems and hybrid environments that comprise cloud, on-premises, and off-premises components.

DHS is no exception. We have a complex, distributed, multi-layered infrastructure that includes cloud, on-premises, and outsourced components, multiple operating systems and a myriad of technologies. DHS endpoints range from traditional laptops and desktops to mobile devices to medical equipment and industrial controls—each of which is an attack vector in and of itself.

Traditional layers of defense in depth that many security leaders consider may be a combination of signature-based antivirus, removal of administration rights, network segmentation, secure configurations, or even least privileged accounts to protect the endpoints. Because of the interconnectedness, we need to take into account all the different layers and consider the damage that can occur should an attacker get into the infrastructure. The challenge that we wrestle with is: How do we stop them from going further? We believe that one of those layers is with evolving endpoint security solutions.

BUSINESS GOAL IMPLEMENTING ENDPOINT SECURITY

Recognizing that attacks will continue and attackers will eventually find their way into the network, a goal to consider would be implementing a next generation endpoint security solution.

A realistic goal of any government organization should be to shut down attacks in real time. The theft of system administrator credentials and subsequent running of commands off the endpoint is a major concern as it expands the attack surface and further opens the door to a data breach and theft of medical records. Intelligent endpoint security can play a vital role in disrupting the attacker's mission and limiting the damage by blocking their

efforts at one of the critical points of entry.

Like many organizations, DHS is subject to various regulations and legal requirements that specify response requirements. For example, if DHS suspects that an attacker has compromised one of its federal connections, it has one hour to report the suspected breach to respective regulators. A second goal would be to reduce response time. Here, next generation endpoint security plays a valuable role in allowing the defenders to be able to evaluate an attack, understand the scope, focus their efforts, and be agile in their response actions.

When attackers infiltrate a network, the remediation effort often involves bringing in expensive incident response teams. Many security leaders are unable to afford or justify the resources to maintain this skillset internally at their organizations. Engaging third-party support is not cost effective; a third goal would be to reduce the response costs associated with a breach.

IMPACT ON STAFFING LEVELS

Without the right tools and processes in place incident response can be a time consuming and labor intensive process, especially because the necessary data is not always readily available to the defender. Security Operations Center analysts may need to contact data custodians and owners of systems to share information and drive real-time decisions—all of which takes valuable time when seconds count. Next generation endpoint security can make this data readily available and help to streamline the triage processes. Such a solution would provide accurate data with more control over false positives and even take action to stop threats in real-time.

For example, incident response can be as much as 70 percent firefighting and 30 percent implementing value-added projects. You want to be able to flip those percentages. Implementing a next generation endpoint solution would allow teams to move away from firefighting over time and allow security leaders to reallocate resources to other projects, such as threat hunting, insider threat concerns or work on programs designed to either move the organization up in maturity level or drive value to the business. Like many government agencies, our staffing levels are set by the state. While using endpoint security solutions may have an impact on overall staffing levels, it does permit us to reallocate resources from responding to day-to-day security incidents to working on value-added projects that help our security in the long run.

KEY CRITERIA TO REQUIRE WHEN CHOOSING AN ENDPOINT SECURITY VENDOR

For DHS, a next generation endpoint solution is a strategic investment. As security leaders our challenge is building the business case. The overriding criterion for an organization should always be the ability to show return on investment or the business value that a new technology will bring to the organization.

In looking at next generation endpoint security solutions, we have asked: Can it save incident response time? Can it stop an attack as it's occurring? How does the cost balance with the financial and reputational losses associated with a breach? In conjunction with providing business value, what is our timeframe for and return on investment (ROI). Even though it's more like insurance than direct ROI, we look to see a return within three years. With potential administrative changes every four years in State government three to four years is a realistic timeframe to measure value.

As a CISO, a preventive approach tops the list of key criteria for my choosing a next generation endpoint security solution; for example blocking attacks in real time and stopping the attacker from pivoting from an endpoint to another resource deeper within the network. The ability to stop attackers in their tracks is highly valuable. Even though the system was compromised, it would allow us to prevent any further damage, such as the loss of records or the dropping of ransomware.

In addition to stopping attacks, we also want to reduce response times. Because we are subject to various regulations and legal requirements that specify response requirements, the team needs to be able to quickly evaluate the situation, understand the scope of the event, and do it cost effectively. The two elements that come into play here are continuous monitoring and threat intelligence.

Continuous monitoring should be high on the list of requirements because it will give a complete picture of what is happening on the network. With full visibility, an organization will be able to be more effective and can more efficiently respond to attacks as they are happening. Because continuous monitoring combined with threat intelligence provides the ability to see trends, organizations could leverage the information to identify security processes or controls that, when implemented, will reduce future incidents.

SUMMARY

Compensating controls are often more expensive than an actual control; and single-use endpoint products often create more issues than they solve. Next generation endpoint security brings tremendous value in detecting and preventing attacks; but, it is more than simply fixing a security problem. It is about maturing security controls and practices and bringing business value to the organization. Next generation endpoint security serves as a force multiplier to make security teams more productive and effective – empowering them to operate at a higher level and with more agility. Ultimately, it is about winning the battle of the day in the war against cyber threats.

CISOs seeking to implement next generation endpoint security should first examine the complexity of the environment. When a broad spectrum of endpoints and clients are to be included in an implementation, the scope of the project can broaden quickly. In addition, CISOs also must consider the maturity of both the environment and the staff. While implementing the Cadillac version of a solution may be attractive, without the infrastructure and processes to support it and experienced staff to run it, the solution will ultimately fail to deliver on expectations. Because no one solution fits all environments, it's vital that CISOs ask pointed questions and scale the solution appropriately based on complexity and maturity.

COMPANY

IBM
1 New Orchard Road
Armonk, NY
10504-1722
USA

WEBSITE

www.ibm.com/security
www.bigfix.com

CONTACT

Teresa Worth
Worldwide Product Marketing Manager - BigFix
Teresa.worth@ibm.com

INVESTMENT INFORMATION

Founded in 1911

Publicly Held - IBM

OFFICE LOCATIONS

Headquarters 1 New Orchard Road Armonk, NY 10504-1722 USA	75 Binney St. Cambridge, MA 02142 USA IBM Security HQ	1480 64th Street Emeryville, CA 94608 USA BigFix Development	

MANAGEMENT TEAM

Marc Van Zadelhoff GM, IBM Security	Jim Brennan VP Product Mgmt.	Mary O'Brien VP Development	Tom Mulvehill Director, Product Mgmt.	Kristin Hazlewood Director, Development	Mark Phinick Global Sales - Endpoint Security	

EMPLOYEES

Total Number: **387,000**	**Total Technical:** N/A	**Total Support:** N/A				

CUSTOMER BACKGROUND

Total Customers: > 1000	**Total Endpoint Customers:** > 1000	**Total Endpoint POCs:** 100M+				
Markets: Automotive Banking Consumer Education Engineering	Energy (oil and gas) Finance Government (federal) Government (state and local) Healthcare	Insurance Manufacturing Media Retail Technology Telecom Transport				

CUSTOMER ENDPOINT INFORMATION				
Average End-user Revenue: N/A	**End-user Endpoints:** Varied	**Regulations:** PCI-DSS CIS DISA-STIG USGCB FDCC		

PRODUCT INFORMATION
IBM BigFix
Launched on: 2002

PRODUCT OVERVIEW		
IBM BigFix Patch	Automated patch management to help reduce patch cycle times from days and weeks to hours or minutes	General Availability Date: 2002
IBM BigFix Lifecycle	Reduce cost, risk, and complexity of managing endpoints with integrated software patching, distribution and provisioning	General Availability Date: 2002
IBM BigFix Compliance	Enforce continuous compliance across security, regulatory and operational standards	General Availability Date: 2002
IBM BigFix Inventory	Maintain audit readiness and mitigate security risks with software compliance and usage	General Availability Date: 2002

Application Development Process

PRODUCT DESCRIPTION
IBM BigFix The market leading, collaborative endpoint management and security platform for IT infrastructure and security professionals, IBM BigFix minimizes the cost, time and effort required to discover, manage and secure endpoints in real-time. Use IBM BigFix to: • **DISCOVER QUICKLY** - First identifies, then provides accurate, real-time information about endpoints • **MANAGE EASILY** - Deploys and patches operating systems and 3rd party software, assesses application usage, monitors compliance, and inventories endpoints across multiple operating systems to reduce the cost, time and effort of managing endpoints • **SECURE CONTINUOUSLY** - Provides continuous monitoring, patching and compliance enforcement across endpoints

PRODUCT ACQUISITION	
IBM BigFix	Acquired in 2010

ENDPOINT PRODUCT ROADMAP & DEVELOPMENT

The BigFix portfolio is comprehensive and provides a unified platform for both Endpoint Security and Management. As previously mentioned, we deliver truly agile development providing 25-45 updates, feature, functions, new capability and content a month. See our release notes https://forum.bigfix.com/c/release-announcements. For 2017 we will be focusing on following themes

Ensure continuous security and compliance
Continued checklist enhancements, additional certifications Expanded PCI DSS checks, enhanced integrations with QRadar. BigFix App for QRadar to provide security posture of Endpoints and the enterprise from QRadar.

End user and server lifecycle management
Integration with Mass360 for enhanced Win 10 and Mac OSx management via MDM API's and app catalog, Drive endpoint management with increased automation, complex patch management. Improve customer value with enhanced Integrations and drive new ecosystem with BigFix.me and App Exchange. Enhance BigFix Query for conversation based threat hunting

Maintain software audit compliance
Enable legacy customers to migrate and adopt BigFix Inventory. Drive ISO adoption and enable expanded license support with new usage metrics, catalog and bundling. Improve performance to cater to emerging security use cases.

ENDPOINT SECURITY PRODUCT SYSTEM ATTRIBUTES

Covers

Cloud
On premises/in-house

Supports

Windows
Windows XP SP2
OS X
Linux
Solaris
HP
IBM

iOS
Android
AWS
Azure
Google
Other (90+ OS supported)

Centralized policy console for controlling anti-malware, anti-spyware, IPS, firewall, application control, web security, email security and endpoint patch management
Integrate with Active Directory or other asset inventories
The solution automatically remove assets from the console when they are removed from Active Directory and other asset inventory tools
SIEM Integration with IBM X-Force Threat Intelligence
Threat Solution Integration with CVE, QRadar
Post-event remediation tools
Forensic capabilities
Vulnerability detection and patch management

REPORTS

Administrators

BigFix Web UI provides a single pane of glass view into impacted endpoints and applicable patches along with the ability to apply patch immediately or set a schedule across endpoints.

Security Executives

Executive Dashboard provides a real-time endpoint security posture view at across customizable tiles that displays metrics, charts and analysis of real-time endpoint data.

DASHBOARD INTEGRATION

Through a single pane of glass, the IBM BigFix App for QRadar brings together multiple powerful sources of information, security events collected and analyzed by QRadar, endpoint activity, and endpoint security posture, such as the vulnerability/patch status and antivirus deployment health measured and managed by the BigFix platform. With this broad visibility into both activity and security posture, direct connections can be made between a detected attack and endpoint exposure, providing clarity into exactly what remedial actions should be taken.

FEATURES IN THE DAY-TO-DAY MANAGEMENT DASHBOARD

- Device summary
- Patches to be applied
- Vulnerabilities discovered
- Antivirus deployment status
- Software installed, processes running, and files with cryptohashes

QUESTIONS

Direct questions to info@securitycurrent.com

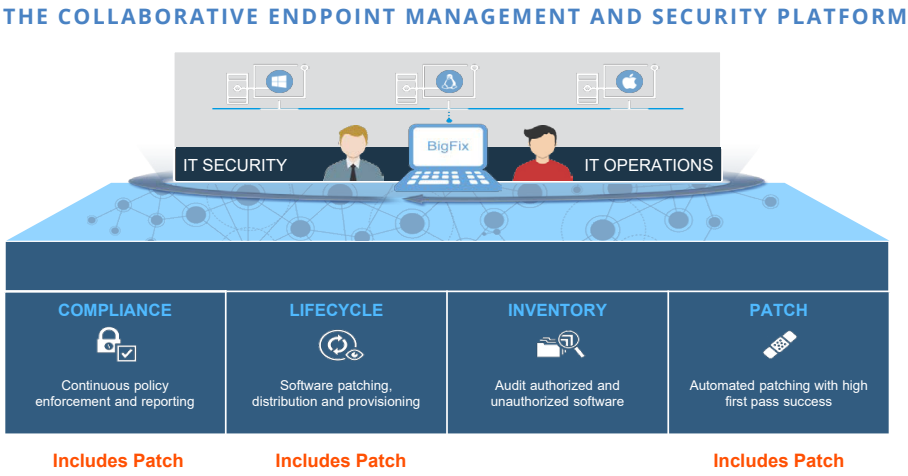
IBM BigFix

Discover, Manage and Secure Endpoints – *FAST!*

The endpoint landscape changes constantly. IT infrastructure and security specialists struggle to discover real-time information on operating systems, software versions, application usage and compliance drift on every PC, laptop, server, ATM and POS etc. across the enterprise. There isn't enough time or budget to continuously and effectively deploy software, apply patches, discover new assets, assess endpoint usage or monitor and enforce compliance on multiple versions of Windows, Mac and variants of Unix operating systems, hundreds of applications, and thousands of endpoint devices (including those in remote locations with low bandwidth or occasional access to corporate networks). This increases the likelihood of a successful endpoint attack. If you can't see it, you can't fix it.

The IBM BigFix family

IBM BigFix is a collaborative endpoint management and security platform for IT infrastructure and security professionals. Unlike other tools that only provide slow, partial views of dated endpoint information on limited numbers of operating systems, applications and devices, IBM BigFix provides the accurate, real-time endpoint data that organizations need to discover, manage, and secure their endpoints. Only with IBM BigFix, can IT operations and security teams can use a single tool to re-image remote devices, distribute and patch software, discover and inventory new assets, assess application usage, and monitor and enforce compliance polices across many types of devices using multiple versions of Windows, Mac and variants of Unix operating systems and applications – regardless of bandwidth and connectivity. Comprised of four tightly integrated modules, IBM BigFix reduces your endpoint attack surface while minimizing the cost, time and effort required to discover, manage and secure endpoints across the extended enterprise.



With IBM BigFix, you can:

- Keep remote servers and internet-facing PCs, ATMs, and POS' updated, secure and always properly configured - regardless of OS, location, or connectivity
- Patch systems faster with a higher, 99% success rate
- Query endpoints and get answers in seconds
- Ensure continuous compliance with security and regulatory policies (i.e. CIS, PCI DSS, etc.)
- Accelerate Windows 10 migrations at the lowest cost possible
- Reduce annual software spend by reclaiming under-used licenses and eliminating software license compliance fines
- Reduce cost and complexity with a single console, skill set and platform that spans IT Ops and Security
- Reduce the number of tools, agents, and vendors for lower costs and better manageability

Why IBM?

IBM BigFix is part of a comprehensive IBM portfolio that helps organizations address management of the full range of IT operations across the enterprise. Supporting the instrumented, interconnected and intelligent IT operations of a smarter planet, IBM solutions help ensure real-time visibility, centralized control and enhanced productivity for the entire IT infrastructure, including globally distributed endpoints.

To learn more about IBM BigFix, contact your IBM representative or IBM Business Partner.
Visit: www.ibm.com/security/bigfix

Appendix C – Supplemental Information & Resources

Works Cited

1. Deloitte. (2016). *2016 NASCIO Cybersecurity Study: State governments at risk: Turning strategy and awareness into progress.* Online: Deloitte University Press. Retrieved from https://dupress.deloitte.com/dup-us-en/industry/public-sector/nascio-survey-government-cybersecurity-strategies.html
2. Embedded Microprocessor Benchmark Consortium. (2017, March 6). IoT-Secure; and EEMBC Benchmark. Retrieved from EEMBC Corporate: http://www.eembc.org/iot-secure/about.php
3. Freund, J. A. (2015). *Measuring and Managing Information Risk; a FAIR approach.* Waltham, MA: Elsevier.
4. Griffith, S.B. (1963). *Sun Tzu - The Art of War.* London, UK, Oxford University Press.
5. Oullette, E. M. (2017). *Magic Quadrant for Endpoint Protection Platforms.* Online: Gartner. Retrieved from https://sentinelone.com/gartner-report-bing/
6. Ponemon Institute. (2016, June). *2016 Cost of Data Breach Study: Global Analysis.* Retrieved from IBM Offering Information: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias

Lead Writer

Bob Turner

Bob Turner is the Chief Information Security Officer at the University of Wisconsin-Madison where he leads the development and delivery of a comprehensive information security and privacy program. His previous experience includes managing consultants focused on cybersecurity policy and compliance with assessment of information systems and cyber security inspection as principal strengths. Bob also served in the U.S. Navy as a Communications Officer with a 23 year career in telecommunications and information systems management. He earned BS and MS degrees in Management and Information Security and is a Certified Information Systems Security Professional and with National Information Assurance Training Standard certificates as a Senior Systems Manager and Systems Certifier issued from the Naval Post Graduate School.

CISO Editors:

Nikolay Chernavsky

Senior Vice President and Chief Information Security Officer

Financial services sector

Anil Varghese

Chief Information Security Officer

Service King Collision Repair Centers

SECURITY CURRENT

Security Current improves the way security, privacy and risk executives share information and collaborate to protect their organizations and their data. Its CISO-authored and peer driven proprietary content and events provide insight, actionable advice and analysis giving executives the latest information to make knowledgeable decisions.