Business challenge

US Foods needed an automated, centralized endpoint management solution to replace cumbersome software compliance monitoring and application deployment processes across 15,000 endpoints.

Transformation

The company selected the IBM® BigFix® solution for lifecycle management, software usage analysis, power management, and security and compliance.

Business benefits

Needed
automated centralized endpoint management solution.

Replace
cumbersome software compliance monitoring

Deploy
processes across 15,000 endpoints

US Foods

IBM BigFix solution reduces company's software spend, increases compliance

US Foods needed an automated, centralized endpoint management solution to replace cumbersome software compliance monitoring and application deployment processes across 15,000 endpoints.

"By auditing ourselves with IBM BigFix, we reduced what could have been over a million dollars in penalties to less than USD7,000."

—Dan Corcoran, Director of Client Technology, US Foods

Share this

Seeking to streamline cumbersome endpoint management processes

US Foods is a leading distributor of more than 350,000 products to over 250,000 customers, including independent and multiunit restaurants, healthcare and hospitality entities, and government and educational institutions.

Software vendors are increasingly vigilant about protecting their licensing revenue and enforcing their agreements, meaning their customers face the ongoing prospect of potentially costly software audits. Before finding itself in that situation, US Foods conducted an internal audit, analyzing software license compliance for its top-five applications.

For six months, Dan Corcoran, the company's director of client technology, spent nearly 10 hours a week collecting and assimilating software installation and licensing data from 15,000 laptops and desktops at 67 distribution centers.

"The process was very labor intensive with our endpoint management software at the time and it was difficult for us to wrap our arms around exactly what software we had," he recalls. "Our previous tool didn't help us distinguish between different applications from the same vendor or between different versions of the same software."

Lacking confidence and control

Less than confident in the endpoint data he had, Corcoran asked personnel at each distribution center to track down and confirm his findings. This was another cumbersome task requiring an hour or more per week throughout the internal audit period.

Even though the endpoint management tool supported centralized lifecycle management and deployment capabilities, bandwidth inconsistency from one distribution center to another forced Corcoran to decentralize some of those activities, at the cost of time and control. "It would take us 7 to 10 business days to do a Microsoft patch, because we had to rely on somebody else to take action. Nothing was systematized; we needed to institute a standard across the entire organization."

Centralizing management of 15,000 endpoints

Significant inefficiencies in the internal software audit process, along with a power management initiative launch, led US Foods to replace its previous endpoint management software, Symantec Altiris, with the IBM BigFix solution.

The company deployed the BigFix solution to help ensure software license compliance across all of its 15,000 endpoints as well as to reduce its device-related electricity costs and compress its patch and application deployment cycles.

"Out of the box, IBM BigFix dramatically streamlined our patch deployment processes, reducing deployment times by 80 percent. It also greatly increased confidence in our software usage data and enhanced our lifecycle management processes significantly," says Corcoran, who points out that two years into full production with the IBM solution, the company's central office now manages all of these endpoint-related activities, thus reducing time and effort spent in the company's remote offices and locations.

As an example of how he uses the BigFix solution for asset management, Corcoran points to a recent analysis of Microsoft Office Suite application usage. Sampling 500 endpoints, he discovered that all endpoints had the Microsoft Office Professional software suite with Microsoft Access software, but less than half ever opened Access software and the majority rarely used it. The company thus stopped providing the Professional version of the software, saving an estimated USD500,000.

Reducing audit vulnerability and optimizing custom Fixlets

Perhaps nowhere is the BigFix solution more critical than in audits. "Prior to acquiring the IBM solution, our software compliance vulnerabilities were over six figures," recalls Corcoran. "But in just one instance, by using IBM BigFix to audit ourselves, we reduced what could have been over a million dollars in penalties for a particular vendor to less than USD7,000."

In addition to out-of-the-box functionality, US Foods uses several custom "Fixlets" (policies) to extend granular visibility and control into any endpoint. For instance, Corcoran's team developed a Fixlet allowing any device to interface with the BigFix solution through a virtual private network to install a printer. Using the outward facing relays the team captured accurate hardware and software inventory information from a recently acquired company.

"Typically, we'd be in the dark regarding their software and hardware configurations, but we now capture that information, even if they're not on our network," says Corcoran. Armed with that insight, Corcoran determined in one case that US Foods could retain a significant portion of the acquired company's hardware and software inventory, which saved US Foods USD70,000 in capital expenditures.

Corcoran sees an expanded role for the BigFix solution in the future, by supporting more Apple Mac endpoints and potentially supporting driver handheld mobile devices. "I never had that same comfort level with the previous toolset. I see us getting more engaged with BigFix so that we have a single source of the truth for our entire environment."

Solution components

- IBM® BigFix®

Connect with us

Take the next step

To learn more about the IBM BigFix solution, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security/bigfix

© Copyright IBM Corporation 2017. IBM Security, Route 100, Somers, NY 10589

Produced in the United States of America, July 2017. IBM, the IBM logo, ibm.com, and BigFix are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml. Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both. This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. **Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle

WGC12421-USEN-01