IBM QRadar Network Insights

Detect threats in real-time with intelligent network traffic analysis

Highlights

- Uses in-depth packet inspection to identify advanced threats and malicious content
- Detects phishing attacks, malware intrusions, lateral movement and data exfiltration in real-time
- Records application activities, captures artifacts, and identifies assets, applications and users participating in network communications
- Applies Layer 7 content analysis for advanced security insights
- Adds extended network and file metadata to IBM QRadar SIEM

Today's advanced threats are more sophisticated and difficult to detect than ever. They hide in everyday network traffic. The very type of traffic from applications, web sites, e-mail, and file transfers that is commonplace and often expected. And once in, malicious actors can move laterally on your network undetected, collecting valuable data for exfiltration. Unfortunately, threat detection solutions often lack the necessary speed, depth and context needed to address cyber security challenges. Logs and network flows are important, but frequently do not provide sufficient visibility to threats throughout their lifecycle. And packet capture data is used mainly for post-incident forensics analysis instead of detecting threats in real-time. Finally, isolated network analytics deployments can have limited integration with large and often geographically installations of security solutions.

With IBM QRadar Network Insights (QNI), in-depth visibility into network communications on a real-time basis now becomes available to QRadar customers. Malicious activities cannot hide from the network, and threats can be hunted down so their impact can be avoided or minimized. Essential threat indicators can be gathered and activities relating to applications, assets, artifacts and users can be collected. With QNI, organizations can detect and analyze advanced threats, phishing e-mails, malware, data exfiltration, lateral movement, compliance gaps, and DNS and other application abuse before they can do their damage.

Seamless integration with QRadar also makes network analytics an important value-add to security operations staff. Threats can be identified by correlating network insights with log and event data, and hidden offenses can be revealed through analysis employing the latest threat intelligence information. QRadar Network insights can also reconstruct and analyze session content to provide a repository of forensics information, along with application level data to add context to metadata. Full analysis of suspect content can be automated, and targeted extraction can bring traditionally hidden threats and malicious activity to the surface. Network insights can also establish normal usage patterns to help detect anomalies that could be signs of an insider threat.

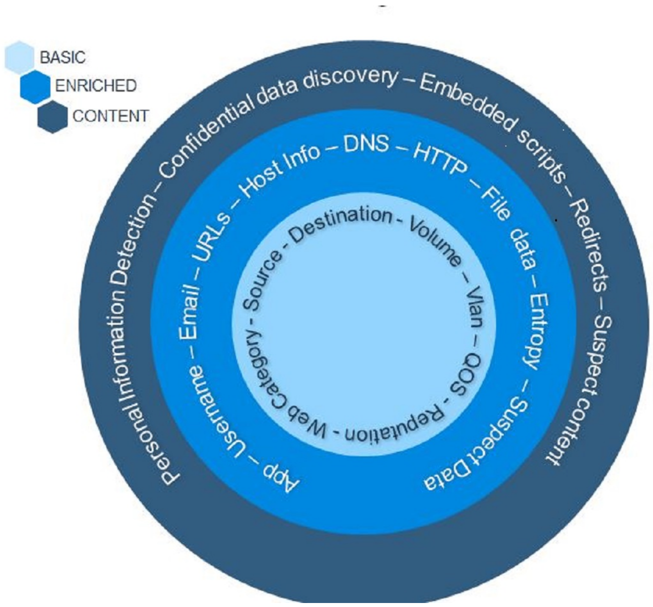
QRadar Network Insights uses deep packet inspection to analyze the data that flows into or within your network, and looks for known threats and malicious activities in real-time. When it identifies a threat, malware or potential data loss, it generates an offense in QRadar for rapid follow-up action.

Uses cases supported by QRadar Network Insights

Challenges faced by organizations today	
Lateral movement attack detection	Trace anomalous communications - recon, data transfers, rogue and malicious actors
Malware detection and analysis	Observe and analyze artifacts – names, properties, movement, suspect content
Phishing e-mail and campaign identification	Pre-empt and react - to malicious emails by analyzing sources, targets, subject, and content
Insider threats	Recognize high-risk users – targets for phishing, negative sentiment, suspicious behaviors
Identification of compliance gaps	Continuous monitoring - of enterprise, industry and regulatory policy compliance
Data exfiltration detection	Identify and track files – DNS anomalies, sensitive content, aberrant connections, aliases

The level of content analysis provided by QRadar Network Insights can be configured and customized to include the following:

- Basic Flow Insights - Contains source and destination information, network protocol, byte / packet counts, time of first / last packets, QoS, VLAN information, web categories, and IP Reputation.
- Enriched Flow Insights - Application identification, user names, e-mail and chat IDs, URLs, search arguments, host information, HTTP analysis, DNS queries / responses, file information (name, type, size, hash, entropy), configurable suspect content
- Content Flow Insight - Personal Information detection, confidential data detection, embedded scripts, redirects, suspect content


BASIC
ENRICHED
CONTENT
Personal Information Detection – Confidential data discovery – Embedded scripts – Redirects – Suspect content
App – Username – Email – URLs – Host Info – DNS – HTTP – File data – Entropy – Suspect Data
Source - Destination - Volume – Vlan – QOS - Reputation - Web Category

QRadar Network Insights uses deep packet inspection to analyze dataflows, port use, file types and transmission content to detect known threats. And because QNI uses real-time deep packet inspection instead of packet captures, it pulls and stores only the relevant payload information. This data, along with predefined signatures, is used to detect malware and phishing attacks, and the information collected (such as user ID's, messages and files) is leveraged to construct a pool of metadata that can be rapidly searched and examined to support rapid response to malicious activities.

QRadar Network Insights contains intelligence features out-of-the-box that provide rapid time-to-value by immediately and automatically finding malicious content. QNI gives security teams the user-identification credentials, recent communications information, and activity details for suspect traffic entering and exiting the network. This allows QNI to determine the kind of attack that has occurred, determine what systems or data have been affected, and support quick investigation and corrective action.

For more information

To learn more about this offering contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

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

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2016

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 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.

♻ Please Recycle