IBM Security
Thought Leadership White Paper

October 2016

Combating security threats with endpoint security intelligence and control

Prioritize vulnerabilities and expedite remediation with IBM QRadar and IBM BigFix

IBM

Contents

Introduction

From custom malware to zero-day exploits, advanced security threats are exploding worldwide—and the sophistication of these attacks is greater than ever. Today's cybercriminals are adept at finding victims to target via email or web-based attacks, as well as exploiting vulnerabilities in the endpoints themselves. Large, coordinated, operationally sophisticated attacks are now executed across broad swaths of the Internet, bypassing traditional security mechanisms. And the number of malware strains just keeps growing.

How can an organization stay ahead of these advanced security threats? Maintaining a high level of baseline security by consistently enforcing security policies and patch levels on endpoints and servers is definitely required and important. But when networks can have multiple vulnerabilities per IP address at scan time, the slow process of mitigating and patching these weaknesses can result in dangerous security gaps. Today's IT personnel have to make difficult, risk-based decisions on where to focus their efforts—often without having a complete picture of the security environment. This is even more critical when the number of vulnerabilities across the organization is increasing while the organization has limited resources and skills to fix the vulnerabilities. In addition to being able to detect vulnerabilities efficiently, organizations also need to take into consideration the broader context of those vulnerabilities, and associate the vulnerabilities with risk levels, so they can focus their remediation efforts on the areas of greatest risk.

This white paper discusses how to combat advanced security threats by adopting an integrated, intelligent and automated approach to endpoint security. It will explain how to broaden the context and capabilities of IBM® QRadar® Security Intelligence Platform with endpoint security intelligence and control of IBM BigFix® to identify, prioritize and remediate security risks. This paper will look at the strategic value of using these solutions together to fight the latest modes of attack.

IBM QRadar Security Intelligence Platform

QRadar Security Intelligence Platform is an anchor solution to help organizations effectively combat increasingly sophisticated attacks to safeguard their network environments, protect their intellectual property and avoid business disruptions. It does more than just monitor logs and network flow data; it collects data and activities from a wide variety of data sources and performs real-time correlation with rules and threat intelligence to quickly identify security offenses that may require immediate action.

IBM QRadar Risk Manager, built on QRadar Security Intelligence Platform, enables organizations to proactively manage network device configurations and correlate them with the network topology to analyze and identify security risks and possible attack paths.

IBM QRadar Vulnerability Manager, also built on QRadar Security Intelligence Platform, provides an efficient way to detect vulnerabilities across devices on the network. It can also collect and consolidate scanning results from various vulnerability scanners. By leveraging QRadar Security Intelligence Platform and QRadar Risk Manager data, QRadar Vulnerability Manager can serve as a centralized control point for vulnerability reporting and prioritization for an entire organization.

IBM BigFix for endpoint security

The best protection against threats to endpoints is to discover software or configuration vulnerabilities and secure the endpoints before an exploit can inflict damage across the network. BigFix provides an endpoint management and security solution to help customers continuously monitor endpoints' configuration, installed software, operating system or application patches, and report policy compliance across all the devices—based on either out-of-the-box or custom policies. BigFix can also fix non-compliance promptly by using IBM Fixlet® messages to change an endpoint's configuration state, apply appropriate patches, remove malware files or stop suspicious processes. This continuous monitor-report-fix cycle can effectively eliminate the windows of opportunity for attacks.

According to a 2015 data breach investigation report, almost half of newly reported vulnerabilities were exploited in the first four weeks after they were reported because hackers know many organizations cannot effectively patch new vulnerabilities.[1] Efficient patching is still the best approach to mitigating the risk of malware exploiting new vulnerabilities. BigFix provides an automated, simplified and efficient patching process across all endpoints, on or off the corporate network, for various operating systems and applications. Patching using BigFix can significantly reduce patch-cycle times and can considerably reduce operational costs.

For vulnerabilities that do not have patches available yet (zero-day vulnerabilities), BigFix provides organizations with a remote quarantine capability to isolate the affected endpoints from the network so they can be protected against attacks and prevented from infecting other endpoints until a patch or other remediation is available.

Closing the gaps in vulnerability management

To defend against security threats, organizations need a comprehensive approach to identify and mitigate high-priority risks across an ever-changing IT environment. This approach should consist of the following tasks:

- Understand the up-to-the-minute status of diverse endpoints
- Identify the vulnerabilities of each endpoint

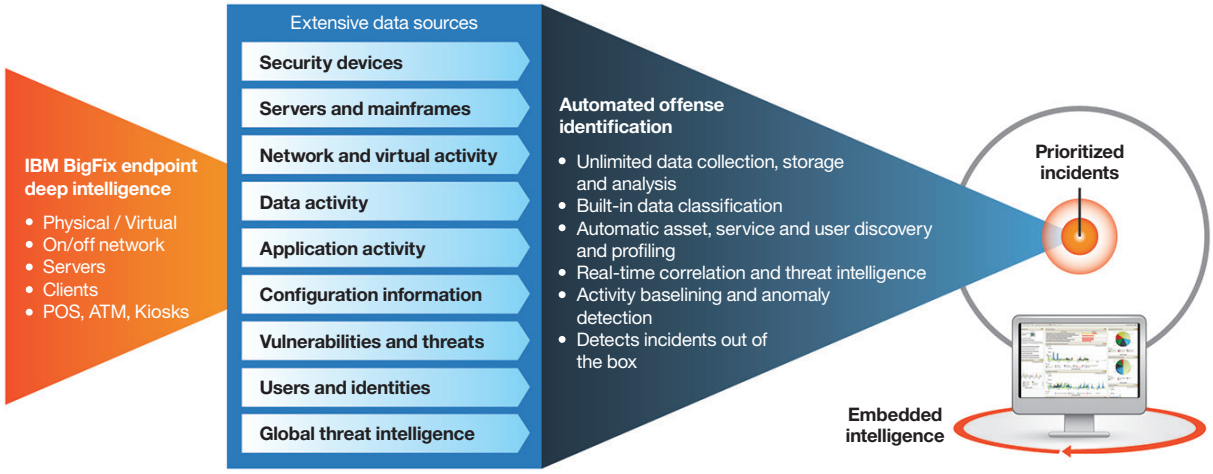
- Prioritize vulnerabilities
- Take action quickly to remediate or mitigate high-priority endpoint vulnerabilities or quarantine the devices
- Confirm that the corrective action has successfully returned the endpoint to a more secure state

Many vulnerability management solutions focus on identifying or prioritizing vulnerabilities, but lack intelligence and capabilities to remediate the prioritized vulnerabilities efficiently. IBM can help organizations close this vulnerability-management gap by combining BigFix with QRadar Security Intelligence Platform. With this integrated solution, an organization can identify and prioritize vulnerabilities in operating systems or application software that attackers can exploit, and then remediate those vulnerabilities to prevent an attack or minimize the impact to the organization.

Establishing closed-loop risk management with endpoint intelligence

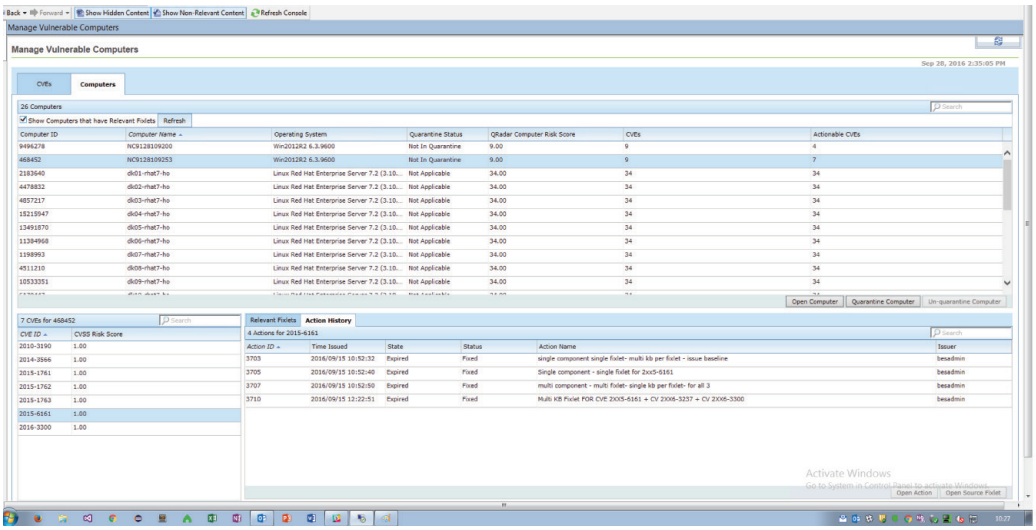
With today's advanced threats growing stealthier, more dynamic and more damaging, the need for integrated, intelligent, automated resources has never been greater. Employing an integrated solution that combines both QRadar Security Intelligence Platform and BixFix can empower IT operations and security teams to work together to protect assets from increasingly sophisticated attacks.

BigFix can provide deep, near-real-time endpoint status information, reporting applied patches, recent configuration changes and more to QRadar Security Intelligence Platform in order to improve the system's risk analytics accuracy. More specifically, the BigFix agent running on an endpoint, on or off the organization's network, continually assesses configuration and patch policy compliance, and feeds the latest status to QRadar, so QRadar can correlate the endpoint status with other security events or network activities to pinpoint suspicious incidents.



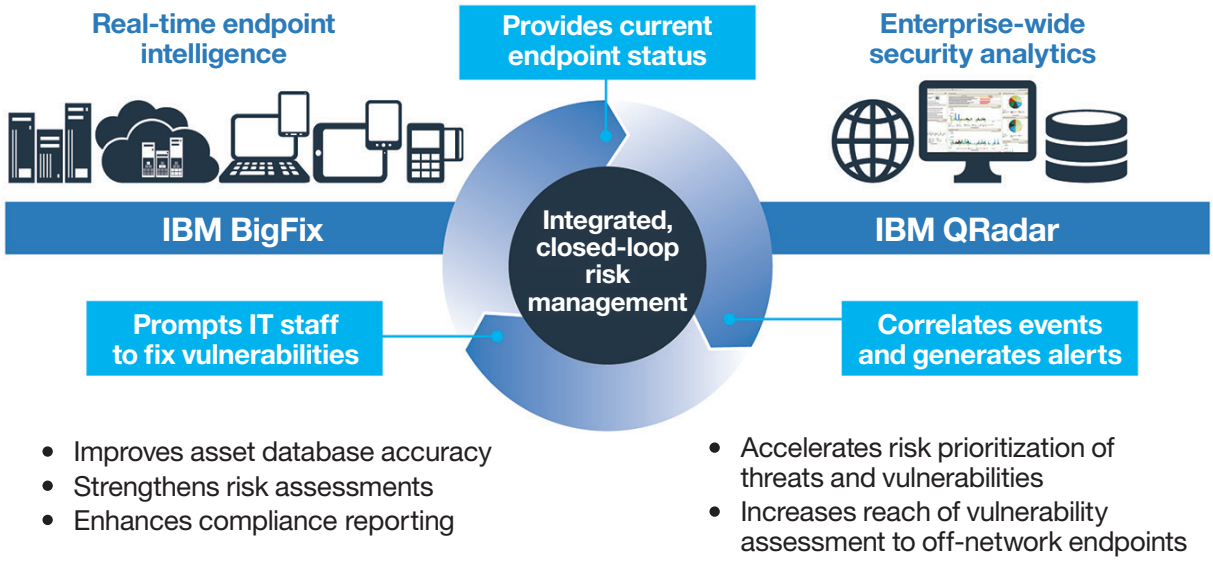
IBM BigFix feeds the latest endpoint status to IBM QRadar, which correlates that status with other security events to pinpoint and prioritize suspicious incidents.

QRadar Vulnerability Manager can be used to scan vulnerabilities or collect vulnerabilities from BigFix and other endpoint vulnerability scanners, assign a risk score to each asset based on correlation with a broader context provided by QRadar Risk Manager that includes network topology and communication activities, and then send the vulnerabilities and asset risk scores to BigFix. For each vulnerability detected by QRadar, BigFix can identify the appropriate remediation actions (patching or quarantine) for the IT staff to take. Furthermore, the IT staff can use the asset risk score, the number of vulnerabilities on each endpoint, or the available remediation to prioritize their remediation efforts, so the most critical vulnerabilities can be remediated sooner.



IBM BigFix can effectively remediate vulnerabilities identified by QRadar Vulnerability Manager and provides various metrics to help customers prioritize their remediation efforts.

After the remediation action is taken, the latest endpoint status is reported back to QRadar, which again is correlated with other security events or network activities, and may update the previously reported suspicious incidents. By combining BigFix endpoint intelligence and control with a QRadar enterprise-wide security intelligence posture, an organization can establish a continuously running, closed-loop risk-management program to effectively combat security threats.



IBM BigFix and IBM QRadar together form an integrated, closed-loop risk management system with real-time endpoint intelligence and enterprise-wide security analytics.

Conclusion

To make vulnerability management more effective, organizations need an integrated approach that incorporates both endpoint intelligence and network context. IT staff need to know which vulnerabilities are scheduled to be patched by an endpoint management system and which ones are not, to help ensure that remediation efforts are efficiently prioritized. In addition, IT staff must be able to quickly take action on security intelligence and make necessary updates across all endpoints within an organization.

QRadar and BigFix solutions can work together to help organizations stay ahead of advanced threats. This intelligent, automated and integrated approach can deliver strategic value by enabling consolidated management and efficient use of security resources. Incident response times, including the delays between vulnerability exposure and detection, can be streamlined by combining the near-real-time endpoint status details from BigFix with the security intelligence of QRadar solutions—reducing millions of security events to a manageable, prioritized list of weaknesses. This way, organizations can take a proactive approach to strengthening their IT resources against the most persistent threats, significantly reducing their risk.

National security requires real-time endpoint compliance

Federal agencies are faced with a multitude of security threats, which have prompted regulatory mandates for the deployment of solutions that can continuously monitor, manage and mitigate vulnerabilities. The integration of QRadar and BigFix solutions provides outstanding value for federal agencies.

An enterprise cybersecurity solution can help government agencies combat threats and eliminate vulnerabilities. As one example, more than 50 US federal agencies have standardized on BigFix to manage and secure over three million workstations, servers (both physical and virtual), and other endpoints across a vast array of operating systems. Such solutions deliver real-time, continuous endpoint security and compliance by leveraging a library of many thousands of checks.

For more information

To learn more about IBM QRadar Security Intelligence Platform, IBM BigFix or other IBM Security solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
October 2016

[1] "2015 Data Breach Investigations Report," *Verizon*, April 2015. https://msisac.cisecurity.org/whitepaper/documents/1.pdf

Please Recycle

WGW03051-USEN-02