IBM Security
Thought Leadership White Paper

July 2015

Combating advanced threats with endpoint security intelligence

IBM BigFix and IBM Security QRadar solutions enable real-time, closed-loop proactive risk management

Contents

Introduction

From custom malware to zero-day exploits, advanced security threats are exploding worldwide—and the sophistication of these attacks is higher than ever. Today's cybercriminals are adept at finding victims to target via email or web-based threats, 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 threats? Maintaining a high level of security by consistently enforcing security policies and patch levels on endpoints and servers is a good start. But when networks can have up to 30 vulnerabilities per IP address at scan time,[1] 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. In addition to being able to find vulnerabilities, organizations need to be able to understand the network context of those vulnerabilities so they can direct their remediation efforts at 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 speed detection of attacks across thousands of heterogeneous endpoints—even employee-owned mobile devices—and correlate the vulnerabilities with other malicious network activity to proactively remediate high-priority risks. The key is in the integration of IBM® BigFix® with IBM QRadar® Security Intelligence Platform. This paper will look at the strategic value of using these solutions together to fight the latest modes of attack.

Closing the gaps in vulnerability management

Today's complex IT environments are more challenging than ever to secure—and thus, more attractive than ever to financially motivated attackers and politically motivated "hacktivists." In fact, IBM X-Force® researchers have found that security incidents are on an upward trend.[1] Efforts to identify potential victims, deploy a range of attacks and exploit vulnerabilities are increasingly organized. What's more, exploit kits are now made publicly available for use by other attackers within hours of a vulnerability disclosure, spawning a phenomenon known as "zero-day" attacks.

To defend against security threats, organizations need an integrated way to identify and mitigate high-priority risks across an ever-changing IT environment. They need to:

- Understand the up-to-the-minute status of diverse endpoints
- View this endpoint information within the context of other vulnerability data
- Prioritize which vulnerabilities should be addressed first
- Take action quickly to remediate or mitigate endpoint vulnerabilities that have been prioritized as urgent
- Confirm that the corrective action has been successfully completed

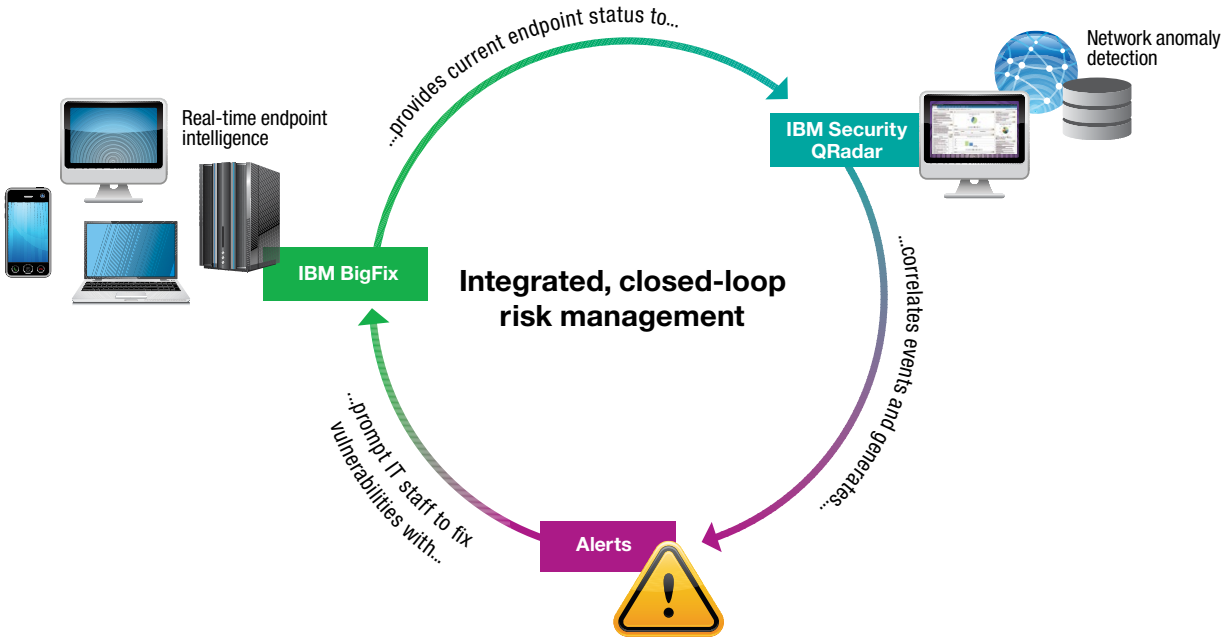
IBM can help organizations bring endpoint intelligence into the "big picture" of security information and event management (SIEM). By combining BigFix with QRadar Security Intelligence Platform, organizations can be proactive about vulnerability management. They can identify weaknesses in systems, software or the network that attackers can exploit—and then remediate those vulnerabilities to prevent an attack or minimize the impact to the organization.

Leveraging real-time endpoint intelligence for closed-loop risk management

With today's advanced threats growing stealthier, more dynamic and more damaging, the need for integrated, intelligent, automated resources has never been greater. BigFix and QRadar Security Intelligence Platform can help meet this need. They empower IT operations and security teams to work together to protect assets from increasingly sophisticated attacks.

BigFix can provide the real-time endpoint status and rapid response needed to fight the latest advanced threats—especially unexpected zero-day attacks. The BigFix intelligent agent continually assesses compliance with policies, which provides critical input needed for security information and event management.

Using QRadar Security Intelligence Platform, organizations can apply a broader vulnerability context to their endpoint security. From the QRadar console, IT staff can incorporate real-time endpoint status information from BigFix with other security-related data from hundreds of sources. This helps IT staff intelligently prioritize which vulnerabilities to correct first. When a required update has been identified to help address a vulnerability, organizations can use BigFix to take the corrective action—and to confirm that the corrective action has successfully completed on all affected endpoints.



Deploying IBM BigFix and IBM Security QRadar solutions, IT teams can use a central console to analyze vulnerability data, correlate events and prioritize risks for automatic remediation.

The following examples show how BigFix and IBM Security QRadar solutions can be used together to strengthen security.

Advanced threat detection

Cybercriminals are continuously using new tactics to attack endpoints, and these advanced threats can often go unnoticed by traditional security approaches such as anti-virus and anti-spyware solutions. But with granular visibility into endpoint properties, BigFix enables organizations to see "stealthy" configuration changes and automate remedial action. Similarly, BigFix can discover suspicious applications. When a piece of malicious code attempts to install unauthorized applications, BigFix has the ability to identify that behavior in real time and automatically remediate it.

QRadar users can leverage this endpoint intelligence to help IT staff focus on the vulnerabilities that do *not* have an automated fix. In fact, IBM Security QRadar Vulnerability Manager helps minimize false positives and filters out vulnerabilities that have already been classified as non-threatening. For example, applications may be installed on a server, but they may be inactive, and therefore not a security risk; devices that appear exposed may actually be protected by a firewall; or endpoints that have vulnerabilities may already be scheduled for patching.

BigFix continuously assesses the status of endpoints, automatically initiating updates and configuration changes via IBM Fixlet® messages. By understanding which vulnerabilities have a Fixlet available, QRadar users can drastically reduce the total number of vulnerabilities that need to be analyzed—improving the response and remediation time for unpatched vulnerabilities. What's more, IT staff can use ad-hoc queries to help identify offenses and suspected incidents.

Malicious activity identification

When unusual activities are taking place anywhere on the network, QRadar users can correlate that suspicious behavior with other threat data and assign the high-risk vulnerabilities to BigFix for remediation. This way, IT personnel can not only know which updates, changes or patches are considered high priority, but can also take action on them—helping reduce the risk of the initial exploit, lowering exploit propagation and improving productivity. Closed-loop verification helps ensure that changes are completed and the status is reported to the management console.

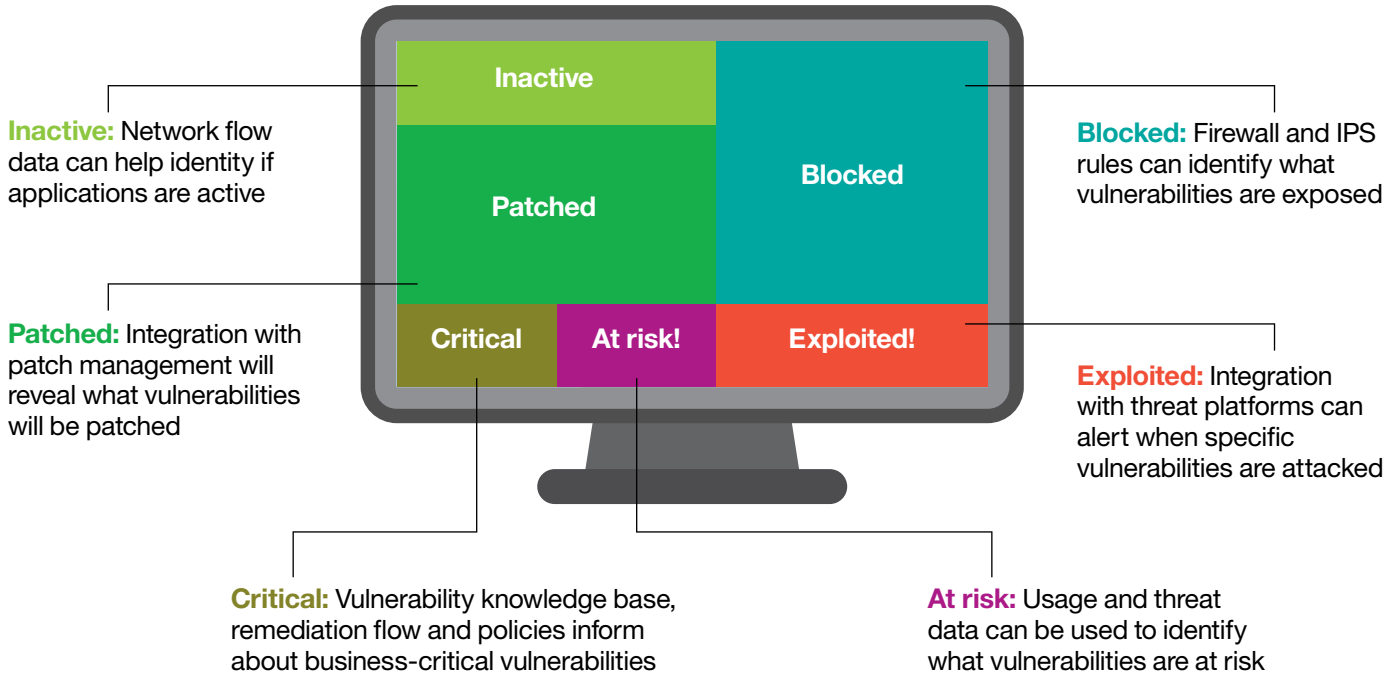
Whether applying a patch to repair a newly discovered vulnerability on hundreds of thousands of endpoints or assessing the configuration status of employee-owned devices, BigFix can affect organization-wide change in minutes. With BigFix, assessment and analysis are conducted on the endpoint itself—which increases the speed of discovery, software delivery and validation. Less communication is required between the management server and endpoint, increasing speed and reducing the amount of network bandwidth consumed.

User activity monitoring

BigFix can accurately interrogate any aspect of an endpoint and provide a real-time view into problems that exist in the environment. For example, BigFix can detect when users are using modified "jail-broken" devices or have installed suspicious applications, and can then quarantine the device from the network. This enables organizations to discover issues quickly, and it provides an additional layer of defense when traditional security defenses either fail or provide fixes too late to prevent an incident.

In addition, QRadar users can easily combine mobile events from BigFix with network activity for offense identification, forensics investigations and compliance reporting. With more accurate asset information, IT staff can rapidly identify rogue or unmanaged endpoints, improving detection and response time. QRadar also maintains a current network view of all discovered vulnerabilities, including which vulnerabilities are currently blocked from exploitation by firewall and intrusion prevention system (IPS) rules, and which are still at risk of being exploited.

If users have installed a virus, BigFix can ensure that endpoints are disinfected and stay up to date. The solution's centralized management console provides a single, granular view for comprehensive visibility and control across distributed global networks. Operators can perform remedial actions in minutes—and receive immediate validation that the action has completed successfully.



With endpoint security intelligence, organizations can understand the severity of vulnerabilities, including which systems are scheduled for patches or have a critical vulnerability, so security personnel can focus remediation efforts on the highest priorities.

Compliance reporting and monitoring

QRadar solutions and BigFix can work together to provide continuous policy enforcement to help maintain compliance. In fact, BigFix provides organization-wide reports instantly—without having to poll systems to assess the overall security compliance posture. This data can then be included within out-of-the-box QRadar compliance reports, including historic views of daily, weekly and monthly trends, as well as long-term trending reports required by many security regulations.

With a single, integrated dashboard for viewing multiple vulnerability assessment feeds and threat intelligence sources, QRadar users can understand the overall context of network usage, security and threat posture. This helps facilitate compliance—including CyberScope reporting and continuous diagnostics and mitigation programs—by prioritizing security gaps for resolution. It's an integrated approach to addressing vulnerabilities and then reporting on the up-to-the-minute security status.

Fraud detection and data loss prevention

With the help of QRadar solutions and BigFix, IT operations and IT security teams can more easily collaborate on suspected offenses, initiating investigations and corrective actions from the same console. This can help speed the response to web-based malware and other types of advanced threats.

Operations staff can be overwhelmed by a sea of vulnerabilities—without the contextual data to help them focus their efforts on the weaknesses that are most likely to be exploited. It is not uncommon, as a result, for several weeks to pass between the discovery of a known vulnerability and the known patch being applied. At the same time, security teams can lack a comprehensive view of endpoint status, which limits their understanding of the threat landscape. And, if an endpoint vulnerability is identified, security teams can find it nearly impossible to quickly remediate or mitigate the risks.

BigFix can provide security for fixed, network-connected endpoints and roaming, Internet-connected endpoints faster than waiting for a vendor's mass-distribution of signature files. BigFix cross-references threat information against a large, continuously updated cloud-based database to assess the malicious potential of files and URLs in real time, and delivers anti-malware protection to endpoints as needed. A laptop used in an airport, for example, can receive anywhere, anytime, cloud-based protection from threats lurking on websites it visits or files it receives.

IBM security solutions: On the front lines at federal agencies

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 BigFix and QRadar solutions provides unique value for federal agencies.

In addition to the ability to manage up to 250,000 endpoints from a single management server, BigFix provides out-of-the-box CyberScope reporting. It also conforms to the Security Content Automation Protocol (SCAP) and other component standards. With BigFix, federal IT security teams can have a common operating picture for managing vulnerabilities. Plus, while BigFix can have more than a 98 percent first-pass patch success rate, agencies have closed-loop reporting within QRadar to know in real time when all endpoints are successfully patched.

Conclusion

To make vulnerability management more effective, organizations need an integrated approach that incorporates both endpoint control and network context into the remediation process. 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 prioritized and directed most efficiently. In addition, IT staff need to be able to quickly take action on security intelligence and make necessary updates across all endpoints within an organization.

IBM BigFix and IBM Security QRadar 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 more efficient use of resources devoted to security. Incident response times, including the delays between vulnerability exposure and detection, can be streamlined by combining the real-time endpoint status details from BigFix with the security intelligence of QRadar solutions—reducing millions of security events into a manageable list of prioritized weaknesses. This way, organizations can take a proactive approach to strengthening their IT resources against the most persistent threats, significantly reducing their risk.

For more information

To learn more about IBM BigFix, IBM QRadar Security Intelligence Platform 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 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 can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. For credit-qualified clients we can customize a financing solution to suit your business and development requirements, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 systems and products are immune from the malicious or illegal conduct of any party.

[1] IBM, "IBM X-Force 2013 Mid-Year Trend and Risk Report," September 2013. **ibm.com**/security/xforce/downloads.html

Please Recycle

WGW03051-USEN-01