Transform government endpoint security and management with IBM BigFix

Advanced attack detection, investigation and enterprise-wide remediation in a single platform

Endpoints are perhaps the most frequently exploited weaknesses in any organization’s defenses, whether a commercial or government enterprise. From mobile devices to mainframes, endpoints hold the data that cyber attackers seek, and their variety means that those attackers have a wide range of weaknesses to probe. An attacker may compromise the computer on an employee's desk, or a server holding crucial customer data, using known vulnerabilities or zero-day attacks, or by commandeering them from within the firewall with lateral movement from an already-compromised machine.

To detect and block these endpoint attacks, enterprise security teams have rapidly adopted endpoint detection and response solutions to scan endpoints for malware or intrusion attempts. These tools, with varying degrees of sophistication, focus on detecting and containing problems rather than on proactively defending against them, or fully remediating the damage they can cause across the agency or enterprise.

An effective endpoint security solution must provide continuous visibility into your endpoints, and enforcement of compliance to your security, configuration, usage and patching policies. IBM® BigFix® does precisely that, with support for continuous policy compliance, rapid investigation and analysis, and precise action. BigFix goes beyond point solutions to help IT and security personnel understand and protect the entire range of endpoints. By discovering all endpoints, continuously monitoring installed and running software, and enabling efficient patch and configuration management, BigFix helps establish a solid enterprise-wide baseline.

Highlights

- Discover and audit virtually all endpoints on or off the network
- Detect evasive attacks with behavioral analytics
- Leverage guided investigations to define the scope of detected attacks
- Define exactly what actions you need to take
- Immediately contain and remediate attacks enterprise wide
- Continuously and proactively reduce your attack surface
Where conventional solutions fall short

Lack of visibility

Incomplete visibility of endpoint status provides poor context for detection

Complexity of investigations

Limited data and skills inhibit accurate investigation and decision making

Ineffective remediation

Disparate tools and teams reduce your ability to effectively defend and respond

Figure 1: Reactive endpoint protection, focused on detection alone, presents organizations with three main challenges.

Security demands visibility, understanding and action

Cybercrime doesn’t happen in a vacuum, and responding to it takes not just visibility into individual affected endpoints, but understanding and focused action. It’s critical that security and IT operations teams collaborate to not only detect ongoing active attacks, and prioritize newly discovered vulnerabilities, but to understand the status of the endpoints throughout their environment. Only then can they analyze each detected threat to understand its full impact on the enterprise, and precisely focus associated remediation actions to choke off current attacks and prevent them from spreading.

Even when attacks get through your defenses, knowing their scope and impact is crucial. With a baseline of known endpoints and configurations, a security team can see, understand and act in response to attempted breaches.

See clearly

BigFix facilitates the discovery and audit of endpoints, however they are connected, to provide a complete picture of their configuration, security posture, installed software and usage. This complete picture provides a broad context, enabling the advanced behavioral analytics to detect malicious activity.

Capabilities required for effective security

SEE

Clearly

UNDERSTAND

Completely

ACT

Precisely

Figure 2: An effective endpoint security solution must see, understand and act in response to attempted breaches.
Understand completely
The first critical step after malicious activity is detected is to investigate its veracity and scope and answer such questions as: Is this a real attack? What is the root cause? Which device is “patient zero”? How many devices have been affected? How exactly do I contain and then remediate the attack across my entire enterprise? Using the integrated “trusted advisor,” your security team is guided through an investigation to answer all these questions.

BigFix is also integrated with IBM QRadar®, an industry-leading security analytics platform. The integrations include targeted vulnerability prioritization, as well as the ability to feed endpoint activity data into IBM Watson®, resulting in increasingly thorough analysis and investigation of potential threats and detected attacks.

Act precisely
Only after clear conclusions have been reached can an effective response be implemented. Once the root cause of a security breach has been established, information that can help remediate the problem is fed back to BigFix in numerous ways, including automatic creation of a precise IBM Fixlet® for an operator to execute enterprise wide, as well as the population of a dashboard listing applications and devices potentially impacted by the attack, giving security personnel a continuously updated overview of their security environment.

The immediate first response to an attack of any kind is containment—removing from a cyberattacker’s reach any resources and facilities being used directly in the attack. These steps involve, for example, quarantining affected devices or files, killing processes and fixing registry entries on affected machines.

Then the remediation phrase should be initiated as soon as possible to prevent other endpoints from being compromised. BigFix can help you go far beyond containment by leveraging a massive library of prevalidated software, application and operating system versions. With this library of ready-to-deploy software, administrators can roll out remediation packages quickly, on a massive scale.

But mopping up after an attack is the last thing a security team wants to be doing. When it comes to security, prevention is far more valuable. Viewing your own systems from an attacker’s perspective can give you a leg up: Which of your endpoints are the most vulnerable? Which are unpatched, running an out-of-date operating system, or infected with exploitable malware? At a time like this is when a comprehensive solution and an enterprise-wide security perspective is invaluable.

BigFix can discover and disarm an in-progress attack, but should also be utilized proactively, to continuously reduce the attack surface of your endpoints, minimizing the chances that they’ll be compromised in the first place.

---

**Figure 3:** IBM BigFix provides an extensible platform for both proactive and reactive security.
For more information
To learn more about IBM Security and IBM BigFix, please contact your IBM representative or IBM Business Partner, or visit ibm.com/govcybersecurity.

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 effectively manage your agency or department. It provides full lifecycle management of IT products and services, from acquisition to disposition. For more information, contact your sales representative.

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

Produced in the United States of America
May 2017
IBM, the IBM logo, ibm.com, BigFix, Fixlet, IBM Watson, QRadar, and X-Force 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.

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. 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