Security

February 2017

Transforming endpoint security: Going far beyond attack detection

Close the loop by integrating prevention, detection, investigation and response

Introduction

As cyber attacks seem to succeed at will, endpoints remain the most vulnerable and most favored attack vector, providing the lowest barrier of entry for cybercriminals. Endpoints require a continuous, multifaceted approach to securing them, both proactively to reduce their attack surface, and reactively to contain and remediate detected attacks.

The security industry has responded by providing solutions intended to spot and react to malware and malicious behavior. However, no matter how good these tools are, they suffer a number of crucial weaknesses. Approaches that focus largely on detection typically address only part of the larger problem faced by any enterprise. Deeper security requires an organization not only to detect threats, but also to go beyond detection to understanding the company's total security posture—and then to acting decisively to undo damage of an attack and prevent similar attacks from occurring, enterprise-wide.

The zero-day myth

While many organizations are focused on preparing for a zero-day attack, according to a recent report by the National Security Administration (NSA), not a single zero-day attack was involved in a high-profile cybersecurity breach in the 24-month period ending in September 2016.[1] As Curtis Dukes, deputy national manager of security systems at the NSA, explained, "The fundamental problem we faced in every one of those incidents was poor cyber hygiene."[1]

Most incidents were instead the result of relatively simple attack techniques—garden-variety methods such as spear-phishing, water-holing and USB drive delivery. They simply leveraged well known vulnerabilities, which very often were still present due to poor patching, monitoring and management of endpoints. Why are zero-day attacks so rarely employed? They are very difficult to develop, making them relatively expensive to use, especially as a zero-day exploit's window of opportunity is short and, once discovered, cannot be re-used without alteration.

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

When solutions are inadequate, organizations not only let attackers in, they fail to detect attacks in context and fail to respond effectively.

In other words, if easier methods work, criminals will use them. It's up to security and IT organizations to block those easier methods, forcing criminals to use zero-day attacks instead—and being ready to detect and respond when they do.

The challenges of endpoint security

Few enterprises have the budget, personnel and expertise necessary to protect every square inch of the organization—including every endpoint—around the clock, but that is exactly what their security teams are charged with doing. In the process of attempting the seemingly impossible, many organizations with a security-only approach face important challenges:

- **Insufficient visibility:** When solutions generally focus on detection and containment, they often lack sufficient context regarding the current state of the endpoints they protect. They can have limited visibility into how the endpoints are configured, what software is installed and how it is being used. Even organizations with better visibility into endpoints from other tools may be overwhelmed by the data they are collecting—leaving them unable to correlate their data with detected, potentially malicious activity to form a basis for the investigation phase that is critical to developing a response plan.
- **Complexity of investigations:** Because detection is just the beginning of the response process, it is critical to have as clear a historical picture as possible into the environment and the activity taking place in it. The investigation then needs to determine the veracity and scope of the attack, asking questions such as: Is this actually an attack? What is the root cause? How many devices are affected? How many devices could be affected? On the basis of the answers the investigation returns, it is then possible to decide upon the steps required to contain and then remediate the problem. With an overwhelmed, often short-staffed security operations team; limited visibility into the environment; and insufficient time to absorb all the latest threat intelligence information, organizations can have considerable difficulty in arriving at appropriate conclusions.
- **Ineffective remediation:** As security teams and their tool sets have grown organically over time, they have not necessarily grown in ways that complement each other. The result has been silos of teams and tools. By adding new roles and new tools to address specific needs as they arise, organizations can find themselves paying for, installing, configuring, managing, patching and upgrading dozens of non-integrated solutions that provide limited views of the environment. One IBM client was employing 85 different security tools from 45 different vendors. Not only are these patchwork infrastructures costly, in the face of complex investigations, they make accurate incident investigations and conclusions difficult. Any given tool in the patchwork provides only a small slice of the larger picture.

  As the NSA found, poor endpoint hygiene—not the all-feared zero-day attack—was the leading cause of all high-profile attacks in the recent two-year period it studied. In many cases, the organization had essentially left the doors and windows open—neglecting to patch vulnerabilities, for example—inviting the simplest method of intrusion. Once inside a network, attackers can linger for months. In fact, malicious and criminal attacks typically take as much as 229 days to identify.[2]

  And a recent survey of data breaches revealed that more than 99.9 percent of exploited vulnerabilities had been compromised more than a year after the associated Common Vulnerability and Exposure (CVE) was published.[3] With disparate tools, it's difficult to proactively harden endpoints for potential threats, or sweep the entire enterprise for lingering malware. That takes comprehensive endpoint hygiene, which includes activity monitoring, patch and configuration management, security controls enforcement, and advanced malware detection.

All of these challenges lead to a fragmented defense strategy—one that is unable to provide the visibility and coordination needed to prevent, detect and effectively respond to today's targeted attacks.

A new approach to endpoint security

As organizations' reliance on IT to generate business value grows, so do the threats to the IT infrastructure. In fact, 387 new malware threats are identified every minute.[4] To stay ahead of these threats requires a new approach to endpoint security—an integrated, adaptive solution that closes the endpoint security loop with key best practices and solution capabilities.

An effective approach to endpoint security supports clear visibility into the infrastructure and activities, complete understanding of attacks and the necessary response, and precise actions for containing and remediating attacks. It enables the organization to:

- Continuously patch and remediate vulnerabilities that can be used to establish a foothold in your environment, reducing the effective attack surface
- Continuously analyze and record endpoint activity to help detect activity related to any type of attack (including known vulnerability exploitation, zero-day attacks or non-malware-related intrusion)
- Reduce both the time it takes to detect a breach and the "dwell time" an attacker can remain in the infrastructure after gaining access
- Augment signature-based endpoint detection tools with behavioral-based systems that use heuristics to correlate multiple events that are indicative of evasive behavior
- Employ a kernel-mode agent to provide complete visibility into endpoint activity, rather than a user-mode agent that can miss more sophisticated and evasive malware
- Support intelligent investigation and response capabilities, with tools to evaluate the scope of an attack, prioritize the threat and provide the ability to remediate immediately
- Improve and automate compliance efforts by mapping the continuous enforcement of endpoint policies and controls directly to a wide range of industry standards and regulations, facilitating audit preparation as part of an overall security environment
- Provide continuous and complete visibility across all endpoints that can be shared by multiple teams, facilitating collaboration between IT operations and security operations
- Enable fast deployment and provide tangible value within hours or days, not weeks or months

Intelligent endpoint protection

IBM® BigFix® represents a new category of intelligent endpoint protection by enabling a comprehensive endpoint security strategy that implements both direct responses and proactive security measures from the same platform.

The addition of the IBM BigFix Detect module is an answer to the reality of today's threat landscape, where intruders may gain access to virtually any enterprise, whether through an attack from a malicious outsider or the innocent mistake of an authorized user. To the established proactive capabilities of the BigFix platform, with its visibility into endpoint configuration and activities that helps the organization manage readiness before an attack occurs, BigFix Detect adds capabilities for response—the ability to deal with attacks and malware after they occur.

BigFix Detect provides three key capabilities designed to close the loop on endpoint security. Continuous protection, intelligent detection and guided response are combined with real-time visibility into endpoint activity and security status, so companies can see clearly, understand completely, and act precisely to meet threats.

Continuous protection

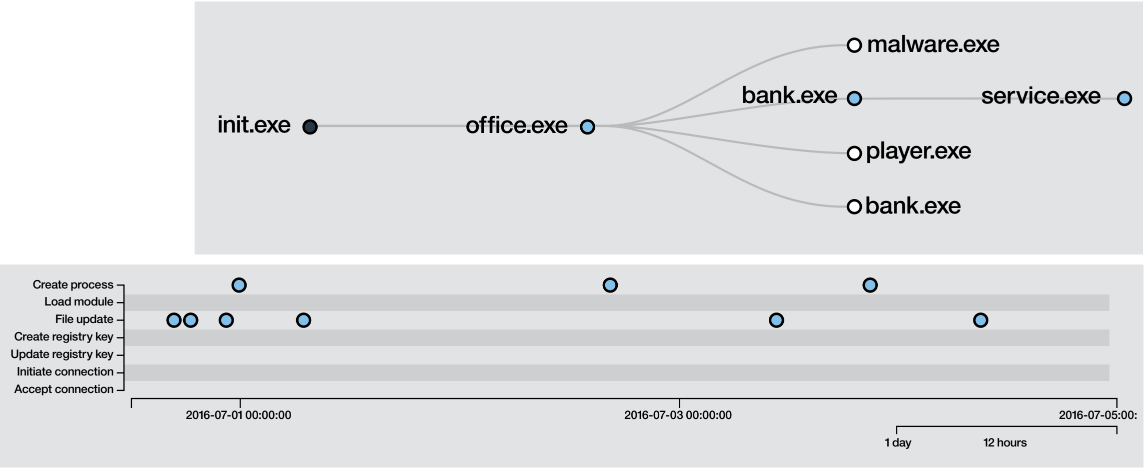
Continuous protection allows organizations to sidestep both known and emerging threats. Continuous protection, starting with anomaly detection, is equivalent to keeping doors and windows locked, forcing attackers to work harder to gain entry, such as by using more complicated and expensive zero-day attacks. Continuous protection lets enterprises:

- Monitor security controls continuously
- Maintain standardized baselines relevant to security, compliance, configuration and patching
- Roll out pre-verified operating system application updates in minutes or hours versus days or weeks
- Deploy, monitor and enforce third-party security agents
- Facilitate collaboration on patch and configuration management between IT operations and security operations

Intelligent detection

Intelligent detection employs a kernel-mode agent that enables all critical endpoint activity to be collected—unlike less effective user-mode agents. It then applies threat intelligence and behavioral patterns, rather than ineffective signature-based malware detection methods, to detect attacks. Intelligent detection leverages the intelligence gathered from millions of active endpoints on the BigFix platform to correlate events, recognize malicious behavior and analyze root cause, helping to accelerate remediation.

Intelligent detection



Intelligent detection correlates events, recognizes malicious behavior, and analyzes root cause, helping to accelerate remediation.

Guided response

Context-based guided response from a software-based trusted advisor tool helps jumpstart the investigation of an attack based on the detected activity—including defining the veracity, exposure and scope of the incident—then provides remediation suggestions. Guided response leverages a massive library of pre-validated multivendor operating system and application content installation packages to provide relevant remediation options within minutes, whether for an individual endpoint, a group of endpoints or the entire enterprise.

Guided response then allows for rapid remediation by creating IBM Fixlet® messages, the BigFix messages that provide instructions to agents to perform an action. Fixlet messages can be rolled out immediately once the appropriate remedial action has been determined. Their actions include patching, reconfiguring or quarantining affected endpoints, or even remotely reimaging them.

Real-time visibility

The BigFix platform provides continuous real-time visibility throughout the endpoint security cycle, enabling discovery and audit of all endpoints, gathering inventory of all software usage and licensing, and continuously assessing configuration, security, compliance and patch posture.

Thousands of attributes are continuously collected from endpoints and sent to a single management server by a single multi-purpose agent. The agent can be used on all types of endpoints, from PCs and servers to ATMs and point-of-sale (POS) devices, including those running Microsoft Windows, Microsoft Windows Mobile, UNIX, different flavors of Linux, and Apple Mac OS, whether those endpoints are physical or virtual, fixed or mobile. The agent uses minimal memory, compute resources and bandwidth.

While the solution provides extensive configuration and compliance reports, an ad hoc query tool also allows administrators to query endpoints and retrieve precise results within seconds.

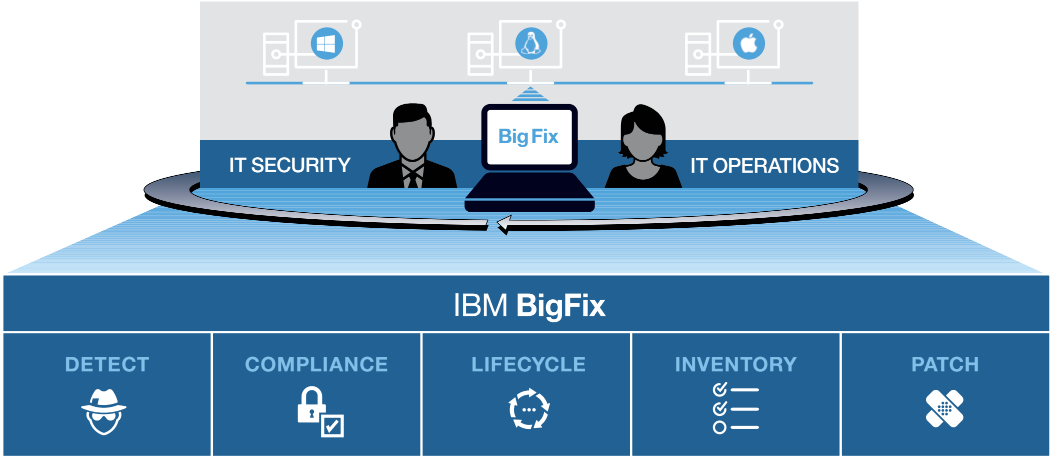
A collaborative endpoint security and management platform

For an industry accustomed to multiple, fragmented technologies and point solutions, BigFix offers a compelling alternative: a single-console, single-agent platform that addresses operations, security and compliance initiatives in real time and at a global scale. One BigFix server can support more than 200,000 endpoints, enabling organizations to make the most of their investments in security and systems management.

The BigFix platform is made up of multiple integrated components:

- **IBM BigFix Detect:** Detection, context-based investigation and precisely focused remediation of active threats made possible by the newest module of the BigFix platform
- **IBM BigFix Compliance:** Continuous compliance of security, operational and regulatory policies
- **IBM BigFix Lifecycle:** Software patching, provisioning, distribution and remote control of endpoints
- **IBM BigFix Inventory:** Visibility into what software is installed and how it is used, helping reduce costs and increase compliance
- **IBM BigFix Patch:** Capabilities that compress patch cycles into minutes or hours versus days or weeks, with a first-pass success rate of more than 98 percent

Collaborative endpoint security and management platform



The BigFix platform brings comprehensive endpoint security capabilities under a single umbrella.

Why IBM?

In the ever-evolving world of IT security, it can be difficult to trust that your organization is doing all that is required to adequately prevent, detect and respond quickly to threats. To help organizations reach this point, IBM BigFix provides an integrated platform that uniquely combines proactive endpoint security with intelligent detection mechanisms and context-based guided responses.

This comprehensive collection of capabilities allows organizations to improve their security posture at every stage of the endpoint security cycle, enabling them to change potential outcomes before, during and after an attack:

- **Preparation instead of infiltration:** A solid foundational security program allows an organization to put itself in the best possible position in case of attack—and to maintain that position continuously.
- **Prevention instead of exploitation:** Continuous, prioritized endpoint management can prevent the majority of attacks that exploit known vulnerabilities to gain entry.
- **Detection instead of expansion:** Comprehensive endpoint activity collection and correlation accelerates detection to prevent attackers from moving laterally around the network and exploiting other vulnerabilities once they have gained access.
- **Analysis instead of data exfiltration:** Context-based analysis and response can be used to generate a remediation Fixlet or to alert administrators to malicious activity before data can be exfiltrated.
- **Response instead of attack execution:** Administrators can evaluate and execute multiple remediation options immediately.

For more information

To learn more about IBM BigFix, visit ibm.com/security/bigfix to watch a video demo of the product in action, or contact your IBM representative or IBM Business Partner to arrange a proof of concept for your environment.

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.

[1] Chris Bing, "NSA: no zero days were used in any high profile breaches over last 24 months," *FedScoop*, September 15, 2016. http://fedscoop.com/nsa-no-zero-days-were-used-in-any-high-profile-breaches-over-last-24-months

[2] "2016 Cost of Data Breach Study: Global Analysis," *Ponemon Institute LLC*, June 2016. http://www-03.ibm.com/security/data-breach/

[3] "2015 Data Breach Investigations Report," *Verizon Enterprise Solutions*, 2015. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

[4] "McAfee Labs Threat Report," *McAfee Labs*, February 2015. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2017

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.

Please Recycle