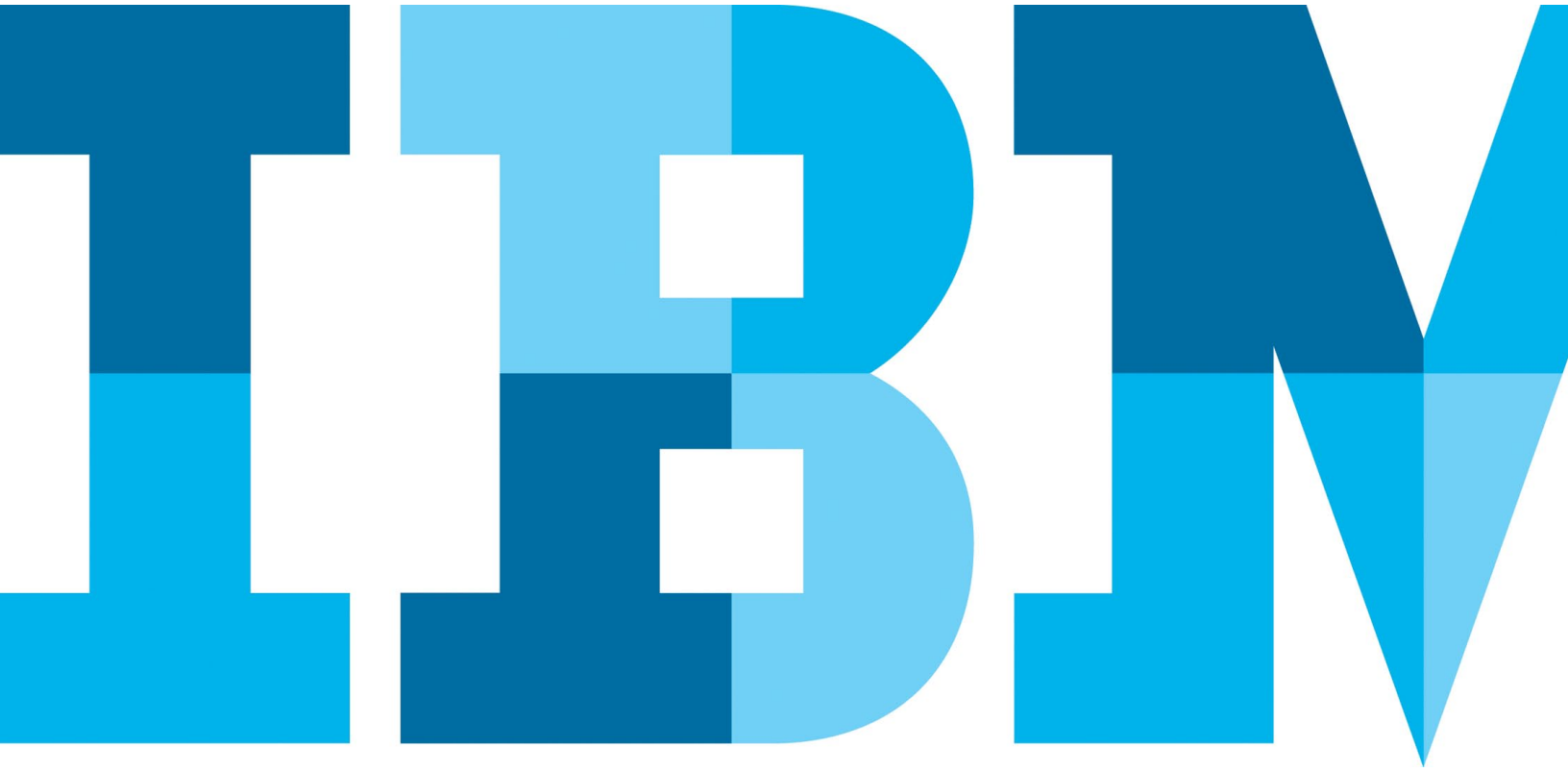
May 2014

IBM Threat Protection System

A dynamic, integrated system designed to disrupt the lifecycle of advanced attacks and help prevent loss



IBM

Contents

2 Introduction

3 An integrated, three-step approach to disrupt the lifecycle of advanced attacks

4 Prevention is mandatory

5 Threats are difficult to detect without the "big picture"

6 Analysis drives a rapid, decisive response

6 Conclusion

8 For more information

8 About IBM Security solutions

Introduction

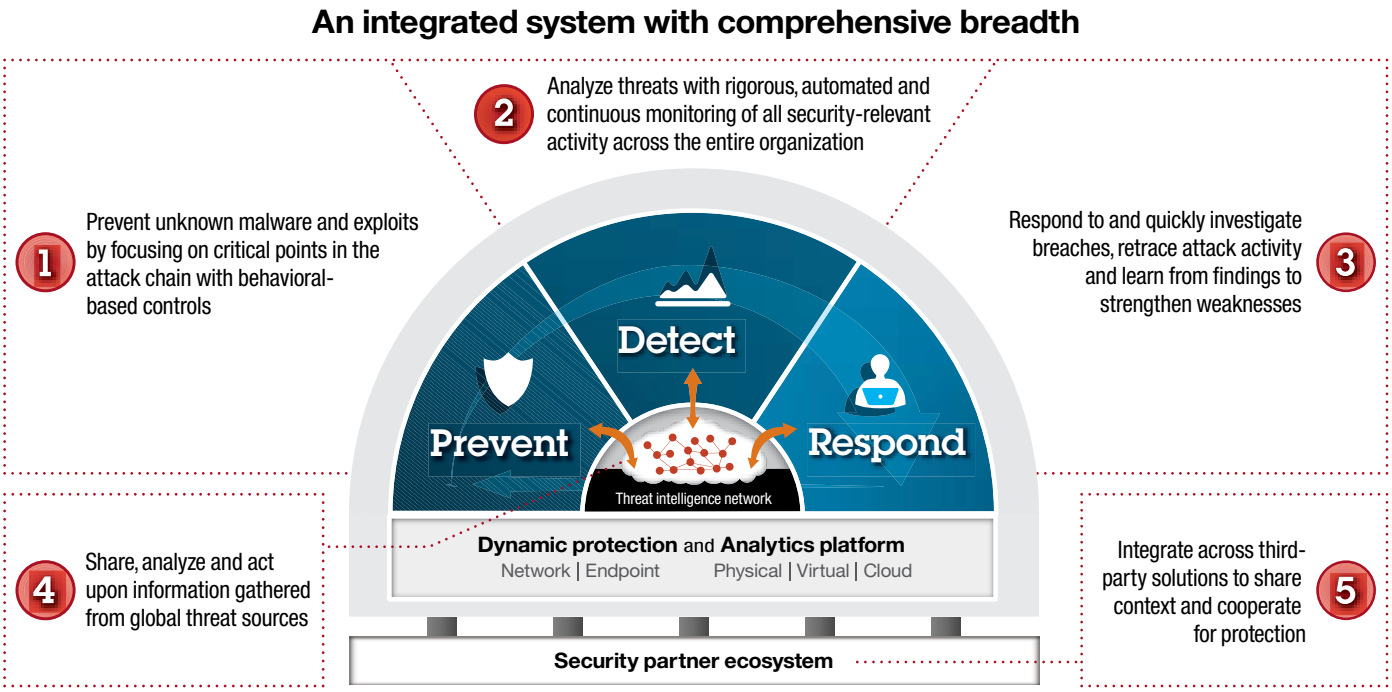
Organizations are under increasing pressure to prevent security breaches by sophisticated teams that seek to steal sensitive data or other proprietary information—attacks that potentially put the organization, its employees or its customers at great risk. These targeted attacks are designed by skilled, innovative individuals and groups who want to create maximum impact and achieve the most financial gain. That's why the attackers continually improve their techniques and evolve malware to evade detection by taking advantage of insufficient and disconnected security technologies.

Unfortunately, too many organizations continue to be vulnerable because they rely on technologies that are incapable of effectively detecting and stopping these attacks. Signature-based capabilities can miss new and mutated threats, while traditional antivirus capabilities cannot detect emerging vulnerabilities or zero-day attacks.

In addition, many organizations have responded to security concerns by deploying separate new tools to address each new risk. This "security sprawl" introduces excess complexity as security teams try to make sense of dozens of disconnected solutions with limited and isolated views of the threat landscape. Siloed tools simply do not provide the visibility necessary to detect and prevent these advanced attacks. Nor do they provide an easily followed trail to understand what happened and how to remediate vulnerabilities.

To stay ahead of advanced threats, security teams need integrated solutions that are designed to help disrupt the entire lifecycle of an attack—from the initial break-in to the final exfiltration of sensitive data—with pre-emptive defenses, powerful analytics and open integrations. Security teams need evolving defenses that are able to actively *prevent* threats that have never been seen before. They need real-time analytics on massive amounts of security-relevant data from across the enterprise to *detect* stealthy attackers lurking within the enterprise—as well as the ability to predict and prioritize security weaknesses before an attack occurs. They also need incident forensics to help identify root causes and *respond* to future attacks.

This report will explore the tactics of today's extremely motivated and well-trained attackers and explain how to foil them with the IBM® Threat Protection System. It is a system designed to effectively address today's toughest enterprise security challenges. IBM Threat Protection System offers an integrated, contextually-aware approach to security with next-generation prevention, comprehensive detection across the enterprise, and dynamic, automated response capabilities.



An integrated system such as the one provided by IBM that delivers capabilities for prevention, detection and response—with support from an intelligent threat network and a partner ecosystem—can disrupt the various stages of an attack to improve protection.

An integrated, three-step approach to disrupt the lifecycle of advanced attacks

Today's organizations need more integrated and effective solutions to help them withstand—and overcome—the onslaught of criminal activity designed to steal information, damage organizations and demoralize consumer confidence in online security. An integrated, three-step approach can help organizations combat advanced attacks.

Prevent even the most sophisticated attacks

With attacks growing more sophisticated than ever, organizations need new capabilities to block the attacks *as* they happen. In fact, real-time prevention remains essential to any successful strategy for stopping advanced attacks from penetrating the organization. It can be the key for helping to protect business-critical assets, including networks, servers, endpoints and applications, from malicious attacks that cause serious harm.

Detect stealthy threats across the entire infrastructure

To identify unknown or previously undetected threats already within the organization, security teams need a "big picture" view of activity from across the infrastructure. They need capabilities that automatically perform real-time aggregation and correlation of massive amounts of data from hundreds of data sources, and that combine analysis of historical data with real-time alerts. This comprehensive analysis must flag patterns of unusual activity and enable immediate blocking of any suspicious traffic.

Respond continuously to security incidents

In the case of a breach, organizations need to investigate and mitigate attacks quickly and comprehensively with solutions that stop attacks in progress, minimize the impact of these intrusions, and enable systems to recover promptly, while ensuring that detailed forensic analysis begins as soon as a threat is detected.

Prevention is mandatory

In today's environment, prevention is more critical than ever. Organizations that practice real-time prevention, as opposed to after-the-fact detection alone, are much better prepared to stop or mitigate an attack.

For complex, multi-faceted attacks, organizations need tools that enable them to block phishing tactics, help prevent user attempts to visit illegitimate or malicious websites, as well as disrupt the constant onslaught of remote exploits being launched against the enterprise and its applications. On the endpoint and network, organizations require new approaches for stopping the newest weapons in the hackers' arsenal—zero-day application exploits, mutated attacks and custom malware—so that they can accurately determine if application behaviors are legitimate or malicious.

The challenge

Traditional security defenses—such as firewalls and anti-viruses—have proven insufficient against today's threats. And in response, organizations have turned to new, threat-detection solutions. Some have gone so far as to abandon prevention as a core methodology for defense. But this can be a costly mistake. Detection-only technologies may help in identifying attacks, but they are effective only after the attacks have been successfully executed. Detection is absolutely important, but it is not a deterrent. Prevention is sometimes harder, but it can also be much more effective against threats.

Strong, real-time prevention is the cornerstone of an advanced threat protection strategy. Prevention needs to go beyond "pattern matching" techniques designed to recognize attacks based on previous experience. Solutions must instead be capable of detecting and, more importantly, disrupting and blocking unknown and zero-day attacks in real time. This requires algorithms, heuristics and other behavioral-based mechanisms. It also necessitates continually updating threat intelligence that extends through the network to every endpoint.

The solution

IBM Threat Protection System offers integrated solutions that provide a powerful combination of next-generation intrusion prevention capabilities on the network and advanced malware protection on endpoints.

On the network, *IBM Security Network Protection (XGS)* can prevent a broad range of threats from reaching into the network. This includes zero-day and mutated attacks that are often able to circumvent traditional forms of network security. By protecting against entire classes of vulnerabilities and using a behavior-based detection approach, IBM Security Network Protection offers broad coverage, while effectively addressing new attacks as they emerge.

On the endpoint, *Trusteer*[1] Apex is redefining endpoint security with a radical new approach to stopping zero-day application exploits and data exfiltration. By analyzing what the application is doing and why it is doing it, Trusteer Apex can automatically and accurately determine if an application action is legitimate or malicious, and block the behavior without blocking legitimate activity. Endpoints can be protected even if the attack was able to circumvent existing network security controls or the user is not on the corporate network. To reduce risks further, Trusteer Apex helps protect credentials by warning users attempting to reuse corporate passwords on applications outside the enterprise and by preventing keystroke logging.

In addition, IBM solutions are backed by real-time threat intelligence that helps drive advanced threat protection. IBM Security Network Protection comes with built-in integration with *IBM X-Force® research and development*, which manages a database of more than 20 billion URLs to help disrupt advanced attacks, such as spear-phishing, that often attempt to redirect users to a site hosting malware. Trusteer Apex incorporates real-time intelligence crowd-sourced from more than 100 million protected endpoints to help prevent malware infections on endpoints.

Threats are difficult to detect without the "big picture"

To gain visibility and insight into advanced threats, organizations need to be able to consolidate and correlate vast amounts of disparate data across a broad range of disparate security technologies. As security teams try to assess and respond to threats, they are deluged by an enormous volume of security data being generated by separate, disconnected tools, often in different parts of the organization.

What organizations really need is comprehensive analysis of data from before, during and after an attack so they can truly understand how much damage occurred, what information was compromised, the best strategy for responding to a given attack and how to thwart new attacks in the future.

The challenge

Many organizations still rely for protection almost exclusively on specialized point technologies or on rules and reactive policies established long before the advent of the latest attack strategies. As a result, they lack accurate, detailed threat detection and informed risk-management capabilities. Plus, they cannot effectively share vital information between networks and platforms. These shortcomings dramatically slow the pace and effectiveness of analyzing and understanding the source, purpose and ramifications of any given attack.

Looking at a small set of security data, such as event logs, does not give an organization the ability to detect advanced, multi-faceted attacks. What is required is clear and complete contextual awareness. The more data an organization can examine and analyze, the higher the chance of detecting stealthy attacks attempting to circumvent security controls. Organizations need to analyze a wide range of security data across multiple sources to help them understand their vulnerabilities and to isolate and pinpoint attacks.

The solution

IBM Threat Protection System provides integrated solutions that empower organizations with intelligence for responding to existing attacks and for preventing future incursions that use similar strategies.

Designed to detect and defend against security threats, *IBM QRadar® Security Intelligence Platform* provides a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, and configuration and vulnerability management.

Using powerful security analytics capabilities, augmented by X-Force threat intelligence, *IBM Security QRadar* solutions enable organizations to analyze massive amounts of data from network traffic, user behavior, security events and numerous other sources—and automatically identify unknown or previously undetected threats. The solutions leverage real-time analytics to help find stealthy attackers lurking within the enterprise, as well as pre-attack analytics to help predict and prioritize security weaknesses before an attack.

With QRadar solutions, security personnel can quickly identify high-priority updates, changes, or patches, and take action to reduce the impact of the initial attack, while slowing or eliminating the propagation of additional malevolent activity. They can minimize false positives and filter out non-threatening vulnerabilities to improve response and remediation time for unpatched vulnerabilities.

Analysis drives a rapid, decisive response

Effective security requires continual improvement, innovation and vigilance that can keep pace with more frequent and complex advanced threats. This means organizations need to incorporate systems that will improve the pace, agility and effectiveness of their response to attacks.

In the event of a successful breach, it is crucial to quickly understand how the event occurred, know what action is required to minimize its impact, and learn from findings to help prevent additional breaches.

The challenge

Even with security threats on the rise, organizations often have no way to conduct forensic analysis on suspected incidents. They are faced with a sea of security information, coming from dozens of tools from different parts of the organization. And since their tools are not integrated, they cannot retrace the evidence to understand what happened and develop a response.

Designing and developing targeted responses to thwart attacks or limit their impact requires the use of security forensics to analyze existing breaches, understand their severity and identify the implications of a given attack. Organizations also need to implement systems for continually improving security at the prevention and detection stages in order to remediate vulnerabilities, fine-tune intrusion prevention configurations and improve existing security policies.

The solution

IBM Threat Protection System gives organizations the data and analysis they need to rapidly and decisively respond to existing attacks, as well as potential threats on the horizon.

IBM Security QRadar Incident Forensics enables security teams to easily retrace the step-by-step occurrences of a security incident. Using deep packet collection and full indexing of data, QRadar Incident Forensics can help security teams quickly verify that an incident occurred, determine the severity, reconstruct and replay the event, determine the root cause, and take corrective and preventive action. Additionally, QRadar Incident Forensics can show the full extent of a breach via its data pivoting and comprehensive indexing capabilities. Organizations can investigate breaches more rapidly than ever—often in hours instead of days.

Understanding the magnitude and nature of a security breach can be challenging, especially with limited resources or a lack of in-house forensics expertise. *IBM Emergency Response Services* provide breach preparedness program development and immediate guidance and support to help organizations recover from attacks, remediate vulnerabilities, and improve security policies and procedures.

Conclusion

IBM understands the very real security threats organizations face every day from malware, phishing and zero-day attacks. These schemes are designed and developed by smart, malevolent individuals and groups seeking to steal, disclose or destroy private data, or disrupt or damage the enterprise.

Threat events funnel into the IBM Security QRadar console

IBM QRadar Security Intelligence Platform captures data across a broad range of feeds, reducing it to a manageable list of offenses using pre-existing and customer-defined rules.

IBM is helping organizations thwart these attacks with the IBM Threat Protection System. This integrated system empowers clients with proven capabilities to prevent, detect and respond to sophisticated, advanced attacks. IBM takes protection beyond the limited effectiveness of point solutions with next-generation systems for intrusion prevention, malware protection and intelligent diagnostic forensics. Organizations benefit from attack prevention, comprehensive detection across the enterprise and automated, dynamic response capabilities.

Importantly, IBM also provides a valuable ecosystem of Business Partners whose solutions can integrate with the IBM Threat Protection System for an even deeper level of security intelligence and insight. The Ready for IBM Security Intelligence program supports this vibrant ecosystem to nurture and support Business Partners that extend the core value of IBM Security solutions for the design, development and delivery of software and systems. Technology collaboration and integration help to increase security coverage, bridge or collapse silos of information, and increase situational awareness and insights.

For more information

To learn more about IBM Threat Protection System, 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 can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, 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 Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
May 2014

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] Trusteer, Ltd. was acquired by IBM in September of 2013.

Please Recycle

WGW03057-USEN-00