Security

Thought Leadership White Paper

September 2017

Stop endpoint security attacks in their tracks with managed detection and response from IBM Security

Rely on continuous monitoring and threat hunting to deliver decisive, rapid threat response

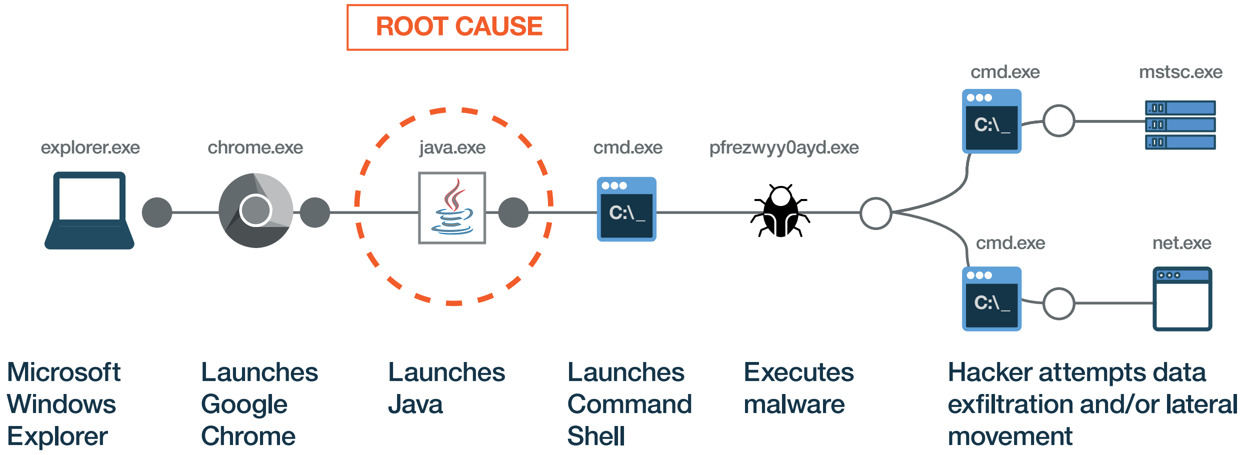
Introduction

Organizations today must assume that their environments have been compromised by a security breach. And if they haven't been compromised yet, they will be. Endpoints are the most-vulnerable and most-used point of entry into an organization's valuable assets. But endpoints have proliferated, from cloud-based or virtualized systems, mobile hardware such as phones and tablets, and Internet of Things devices, to a range of employee-owned devices. These endpoint types have made traditional, signature-based protection solutions (which are focused on prevention of known vulnerabilities) insufficient.

Today's criminal hackers have ushered in a new era of non-malware attacks that do not require them to download any files to the target endpoint. Instead, they use trusted, native operating system tools such as Microsoft PowerShell and exploit running applications such as web browsers and Microsoft Office applications. But security teams often lack the staffing and skill set needed to protect every endpoint against these emerging threats. To effectively protect endpoints takes strong detection and response solutions.

Delivered from a global network of IBM® X-Force® Command Centers, managed detection and response from IBM Security is a fully managed service that provides ongoing, intelligence-based incident response that assumes constant compromise and prioritizes high-risk assets. It provides complete visibility into the root cause of threats. It also delivers deep insight into the complete kill chain at each stage of an attack, from the time hackers are probing possible entry points to the attack delivery, exploitation and installation, and even attempts at subsequent attacks. By providing managed detection and response, IBM can help remove the blind spots that face every security team.

This white paper details the range of endpoint protection that managed detection and response from IBM Security provides, and the software that the service complements to help strengthen an organization's security posture.



Managed detection and response from IBM Security helps detect the root cause of an attack and visualize the attack's entire kill chain.

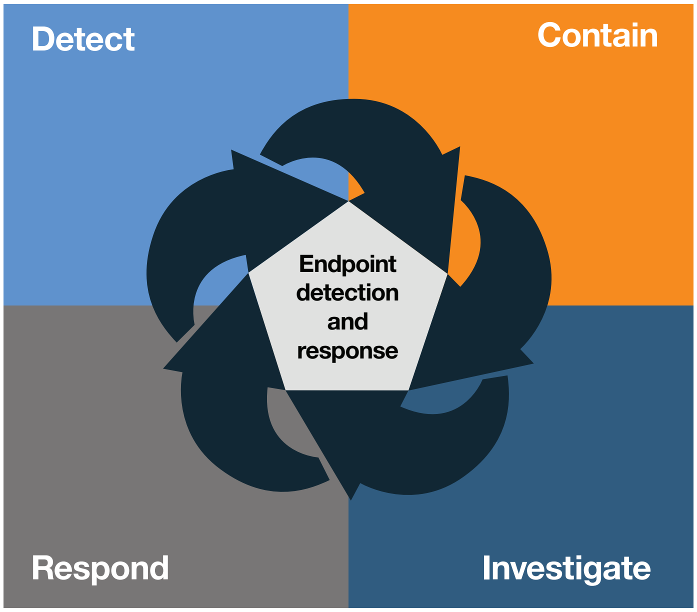
Organizations that benefit from managed detection and response from IBM Security

Instances of non-malware attacks leveraging PowerShell and Windows Management Instrumentation (WMI) increased by more than 90 percent in the second quarter of 2016 alone,[1] and 93 percent of security researchers said non-malware attacks pose more of a business risk than malware attacks.[2] Traditional anti-virus protection is simply not enough. To determine whether your organization needs managed detection and response services, consider the following:

- Are there tools in place to continuously monitor and discover endpoints and gain deep insights into their ability to see the big picture?
- Is there sufficient in-house security staff trained to detect threats and understand their scope and veracity?
- Can your current endpoint monitoring tools rapidly respond to threats and reduce the attack surface?
- Can your team quickly determine how a threat entered the network and how many endpoints are affected?

Managed detection and response from IBM Security can close gaps across discovery, containment, investigation, response and remediation.

Survey respondents said the non-malware attacks they had experienced included remote logins (55 percent), WMI-based attacks (41 percent), in-memory attacks (39 percent), PowerShell-based attacks (34 percent) and attacks leveraging Office macros (31 percent).[2]



See and detect

The ability to see what is happening on every device and the ability to detect active attacks, however simple or sophisticated

Contain the threat

The ability for administrators to contain suspected incidents, through quarantine and other actions, while they are being investigated

Respond to active threats

The ability to respond to active threats with detailed recommendations on how to remediate impacted assets

Identify root cause

The ability to quickly analyze alerts and gather artifacts necessary to identify the source and impact of an infection

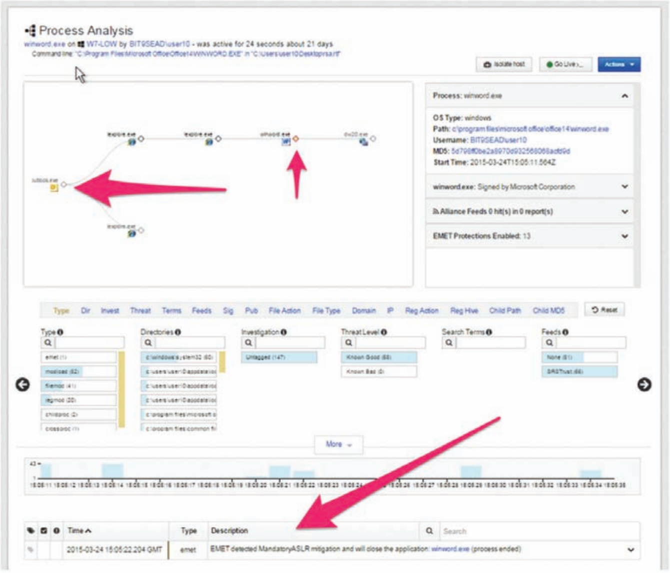
Managed detection and response from IBM Security helps organizations detect, contain, investigate, respond to and remediate threats.

Advance beyond signature-based protection

The average organization takes 191 days to identify a data breach.[3] To rapidly respond to today's cyber threats, organizations need ways to detect attacks in real time without relying on signatures. That requires the ability to first see and then understand the behavior of the attack components. Managed detection and response from IBM Security works seamlessly with managed IBM QRadar® SIEM, which provides security information and event management for continuous monitoring and recording of endpoint activity, powerful analytics and the ability to decipher them.

In addition, IBM X-Force Research provides continuous threat hunting, using detailed analysis of global online threat conditions to help organizations detect threats much earlier than they could unassisted and mitigate the damage that can occur as an attack lingers in their network—often for months. X-Force researchers provide actionable data and recommendations to help strengthen an organization's security posture on an ongoing basis. Specifically, managed detection and response from IBM Security provides:

- Continuous recordings of endpoint activity and traffic without affecting system performance
- Endpoint traffic analysis and security intelligence customized according to an organization's most-likely potential threats
- Live response from X-Force endpoint security specialists for escalated security events
- Continuous threat hunting, threat quarantine and malware bans
- Integration with existing workflow and controls, and coordination with in-house incident response and forensics teams



Process Analysis

winword.exe on W7-LOW by BIT9SEAD\user10 - was active for 24 seconds about 21 days

Command line: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\user10\Desktop\rsa.rtf"

Process: winword.exe

OS Type: windows
Path: c:\program files\microsoft office\office14\winword.exe
Username: BIT9SEAD\user10
MD5: 5d798f0be2a8970d932568068adfd9d
Start Time: 2015-03-24T15:05:11.564Z

winword.exe: Signed by Microsoft Corporation

Alliance Feeds 0 hit(s) in 0 report(s)

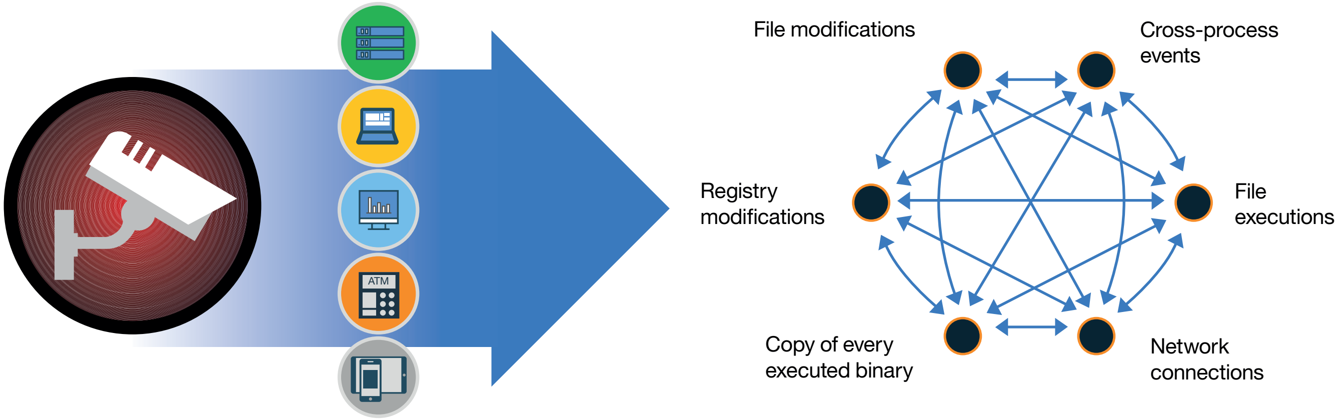
EMET Protections Enabled: 13

Time	Type	Description
2015-03-24 15:05:22.204 GMT	emet	EMET detected MandatoryASLR mitigation and will close the application: winword.exe (process ended)

With managed detection and response from IBM Security, security analysts can see how and when an attack has been addressed.

Empower security analysts with actionable data

Today's attacks are becoming more advanced; 80 percent of them are executed by organized cybercriminals.[4] Managed detection and response from IBM Security relies on an executable file installed on each protected endpoint that operates like a "security camera" for data, capturing information streams that the human eye is incapable of collecting. This distributed software element provides around-the-clock event monitoring, and tracks and collects log data, which is also known as telemetry data. This data is derived from network connections, downloaded files, website visits and more. It then transmits that data to a management console, from which X-Force personnel can conduct continuous threat investigations. Managed detection and response from IBM Security is a standalone service. It provides a management console built specifically for threat investigations that works with a wide range of underlying software as well as support across a range of devices running Microsoft Windows XP and later versions, Microsoft Server 2003 and later versions, Apple macOS, and selected Linux and legacy UNIX systems. This allows you to have coverage across your environment, helping to eliminate gaps in visibility.



Managed detection and response from IBM Security endpoint software operates like a "security camera" for data, recording the interactions an adversary might use to attack an organization's most valuable assets.

Progress along the security maturity continuum

Managed detection and response from IBM Security is designed to help organizations move to the next level in their security maturity, whether they are in the initial stage or have progressed to a developed, defined, managed or optimized security posture. The service helps organizations close the loop between prevention, detection and response, with both a proactive and reactive approach.

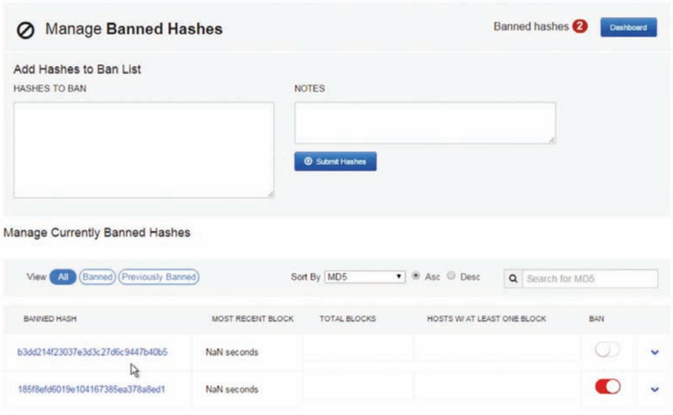
Proactive threat detection

Tap into continuous threat hunting

X-Force Research is one of the most renowned security research teams in the world. X-Force security professionals monitor and analyze security issues from a variety of sources, including 35 billion events per day and 32 billion web pages and images. The X-Force team has documented 100,000 vulnerabilities and monitors 270 million endpoints for malware alone. Managed detection and response from IBM Security provides continuous, proactive threat hunting in collaboration with X-Force Research. Out-of-the-box X-Force threat intelligence can be modified for the highest level of efficacy, helping organizations to cultivate their threat intelligence and customize it based on threats likely to occur their industry or locale.

Bolster prevention capabilities

Managed detection and response from IBM Security also enables organizations to block known malware by banning hashes, or MD5 files, associated with that malware, making it an ideal complement to IBM managed next-generation anti-virus protection (NGAV): IBM Endpoint Managed Security on Cloud. The NGAV solution goes above and beyond traditional anti-virus protection by not only preventing signature-based (traditional) malware but also detecting and blocking sophisticated attacks that are system-centric (e.g., fileless/non-malware attacks). IBM Endpoint Managed Security on Cloud is available in three service levels, with multiple add-on options to customize the solution to an organization's needs. With IBM Endpoint Managed Security on Cloud and managed detection and response from IBM Security, organizations can obtain an optimal solution for endpoint prevention as well as detection and response.



BANNED HASH	MOST RECENT BLOCK	TOTAL BLOCKS	HOSTS W/ AT LEAST ONE BLOCK	BAN
b3dd214f23037e3d3c27d6c9447b40b5	NaN seconds			
185f8efd6019e104167385ea378a8ed1	NaN seconds			

Managed detection and response from IBM Security enables security administrators to easily manage known threats by banning associated hashes.

Reactive threat response

Strengthen SIEM

Many organizations are already tapping into the capabilities of QRadar SIEM. Available on the cloud, as an on-premises solution, or (for organizations that only want to collect log data) as a multi-tenant option, QRadar SIEM detects anomalies, uncovers advanced threats and removes false positives. It consolidates log events and network flow data from the thousands of devices, endpoints and applications that may be distributed throughout a network, and enables organizations to cross-reference endpoint data with network data sources, such as firewalls or intrusion detection systems, to gain a big-picture view of the environment.

For organizations with managed QRadar SIEM, IBM Security provides triage for offenses, and, depending on the severity of the offense, can escalate it to managed detection and response from IBM Security for Tier-2 investigation. The team can not only isolate affected endpoints and prevent the offense from propagating within the environment, but can also provide organizations with detailed reports on severe incidents. Less severe responses such as those that can be managed with a simple patch are escalated to the organization's own security team.

Speed incident response

With the cautious assumption that every organization has been or will be compromised, it's essential to prepare for the inevitable. The IBM X-Force Incident Response and Intelligence Services (X-Force IRIS) team brings decades of forward-thinking incident management, security intelligence and remediation experience to help organizations rapidly respond to a critical security incident. They have consulted on hundreds of the world's largest breach investigations across 17 industries in the public and private sectors. Organizations can enlist the X-Force IRIS team to triage a security breach and enact immediate remediation. Once an immediate threat has been addressed, managed detection and response from IBM Security can help organizations transition to a steady state, providing the recommended tools and visibility the organization needs, such as managed SIEM, to prevent future breaches.

Solidify remediation and patching

IBM BigFix® is an endpoint security and management platform that provides real-time visibility and control across endpoints, regardless of how they are connected. When used with managed detection and response from IBM Security, BigFix provides organizations with additional capabilities for remediating and patching security vulnerabilities.

Obtain customized intelligence and alerts

IBM works closely with organizations to fine-tune managed detection and response from IBM Security to carefully align their security and business goals. It offers the flexibility for organizations to choose the endpoint coverage they need, from all endpoints to a select few, such as Microsoft Active Directory servers or desktops belonging to the executive and accounting teams. Customized alerts and intelligence, including feeds obtained through other providers, can also be integrated. The implementation includes a tuning phase with weekly meetings to assess malware events and recommended remediation actions, and quarterly reviews thereafter. The service is priced by endpoint volume, with the first level from 300 to 999 endpoints, and a lower per-endpoint price for installations of 1,000 or more endpoints—and is scalable to as many endpoints as need to be supported within the environment.

Conclusion

Traditional signature-based protection that is focused on prevention isn't enough to guard against today's emerging threats. In this new era of non-malware attacks, organizations need around-the-clock monitoring and threat intelligence that delivers the visibility and insights they require to rapidly respond to and remediate threats. Managed detection and response from IBM Security delivers. With deep security insights from thousands of global analysts based on X-Force research, around-the-clock monitoring from QRadar SIEM, and financial threat data derived from IBM Trusteer®—a holistic, integrated cyber-crime fraud prevention platform—organizations can tap into the resources they need to protect endpoints from today's emerging threats.

For more information

To learn more about managed detection and response from IBM Security, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security/services/managed-detection-response/

For more information about endpoint detection and response, watch these webinars:

Back to School: Endpoint Security Basics

Mind the Endpoint Gap: Why You Need Managed Detection and Response

IBM & Carbon Black: Fixing Endpoint Blindness

Learn more in these IBM blog posts:

Threat Hunting Services are Now a Basic Necessity

In Prevention We Trust? When and How to Use Endpoint Detection and Response

Transform Your SOC with Managed Services Using Carbon Black and QRadar

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

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.

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
September 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

[1] “Non-Malware Attacks and Ransomware Take Center Stage in 2016,” *Carbon Black*, 2016. https://www.carbonblack.com/wp-content/uploads/2016/12/16_1214_Carbon_Black-_Threat_Report_Non-Malware_Attacks_and_Ransomware_FINAL.pdf

[2] “Beyond the Hype: Security Experts Weigh in on Artificial Intelligence, Machine Learning and Non-malware Attacks,” *Carbon Black*, 2017. https://www.carbonblack.com/wp-content/uploads/2017/03/Carbon_Black_Research_Report_NonMalwareAttacks_ArtificialIntelligence_MachineLearning_BeyondtheHype.pdf

[3] “2017 Cost of a Data Breach Study,” *Ponemon Institute*, June 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

[4] “IBM X-Force Threat Intelligence Index 2017,” *IBM X-Force*, March 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03140USEN&