

Disrupting the Lifecycle of Advanced Threats



Jay Bretzmann
Segment Manager
IBM Security

October, 2015



We are in an era of continuous breaches

Attackers are relentless, victims are targeted, and the damage toll is rising

Near Daily Leaks of Sensitive Data

40% increase
in reported data
breaches and incidents

2012

Relentless Use of Multiple Methods

800,000,000+ records
were leaked, while the future
shows no sign of change

2013

“Insane” Amounts of Records Breached

42% of CISOs
claim the risk from external threats
increased dramatically from prior years.

2014



Attack types



XSS



Heartbleed



Physical access



Brute force



Misconfig.



Watering hole



Phishing



SQLi



DDoS



Malware



Undisclosed

Size of circle estimates relative impact of incident in terms of cost to business.

A historical look at security incidents by attack type, time and impact, 2012 through 2014

Source: [IBM X-Force Threat Intelligence Quarterly – 1Q 2015](#) and [2014 IBM Chief Information Security Officer Assessment](#)

Source: IBM X-Force® Research and Development

Cost of a data breach is on the rise, with most customers at risk

2015 Cost of Data Breach Study, from Ponemon Institute, sponsored by IBM

Cost per record*

Global average

\$154

12%

increase over two years

Highest countries

\$217
in the U.S.
\$211
in Germany

Highest industries

 **\$363** ↑
Healthcare

 **\$215** ↑
Financial

 **\$165** ↑
Retail

Cost per incident*

Global average

\$3.8M

23%

increase over two years

Highest countries

\$6.5M
in the U.S.
\$4.9M
in Germany

*Currencies converted to US dollars

Security leaders are more accountable than ever before



Your board and CEO demand a strategy

Is your security team prepared?

Broad Attacks

Indiscriminate malware, spam and DoS activity

Tactical Approach

Compliance-driven, reactionary

- Build multiple perimeters
- Protect all systems
- Use signature-based methods
- Periodically scan for known threats
- Read the latest news
- Shut down systems

Targeted Attacks

Advanced, persistent, organized, politically or financially motivated

Strategic Approach

Intelligence-driven, continuous

- Assume constant compromise
- Prioritize high-risk assets
- Use behavioral-based methods
- Continuously monitor activity
- Consume real-time threat feeds
- Gather, preserve, retrace evidence

New threats require a new approach to security, but most are defending against yesterday's attacks, using **siload, discrete defenses**

Four truths about advanced threat protection

Despite increasing challenges, organizations can protect themselves by adopting the right strategy

1

Prevention is mandatory

Traditional methods of prevention have often failed, leaving many to believe detection is the only way forward. This is a dangerous proposition.

2

Security Intelligence is the underpinning

Specialized knowledge in one domain is not enough. It takes enterprise-wide visibility and maximum use of data to stop today's threats.

3

Integration enables protection

The best defense is relentless improvement. Technologies must seamlessly integrate with processes and people across the entire lifecycle of attacks.

4

Openness must be embraced

Security teams need the ability to share context and invoke actions between communities of interest and numerous new and existing security investments.

A dynamic, integrated system to help stop advanced threats

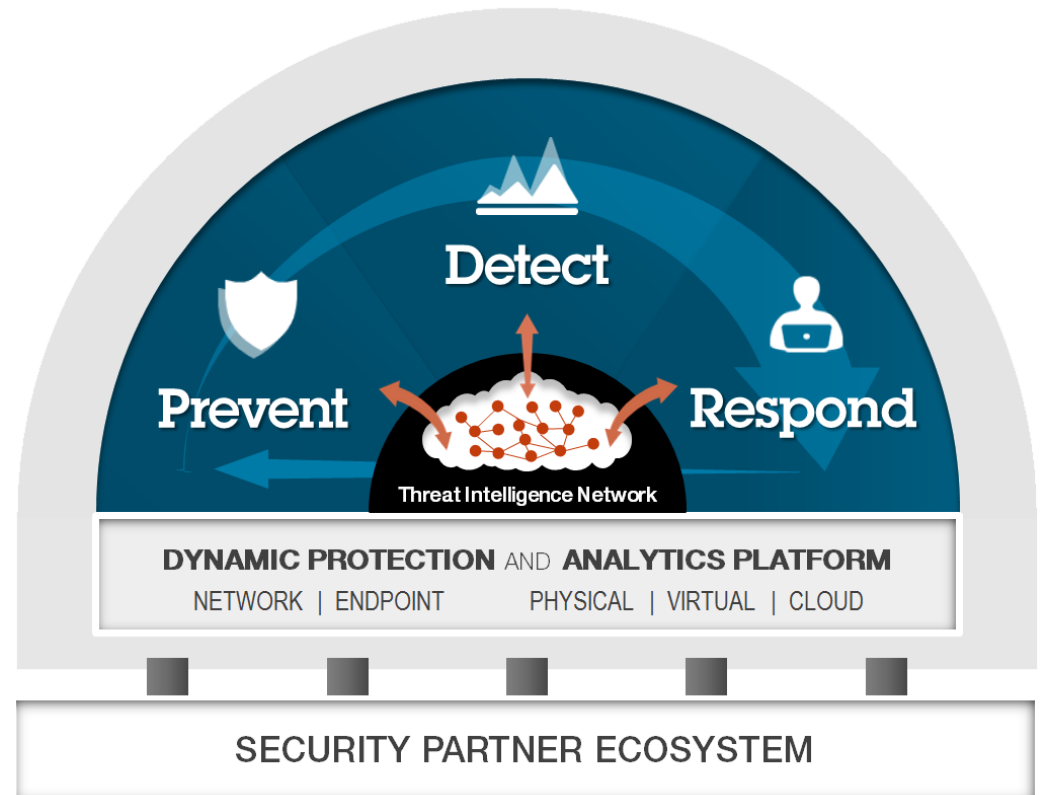
The IBM Threat Protection System

Attack Chain

- 1 Break-in
- 2 Latch-on
- 3 Expand
- 4 Gather
- 5 Exfiltrate



Prevent. Detect. Respond.



Apply preemptive defenses on endpoints, the network, and critical data repositories

On the Endpoint

- Prevent malware installation
- Disrupt malware communications
- Limit the theft of user credentials



@

Break-in

On the Network

- Prevent remote network exploits
- Disrupt malware communications
- Limit the use of risky web applications



@

**Latch-on
Expand**

At Data Access

- Prevent power users from abusing access
- Prevent misuse of sensitive data
- Prevent intrusion and theft of data



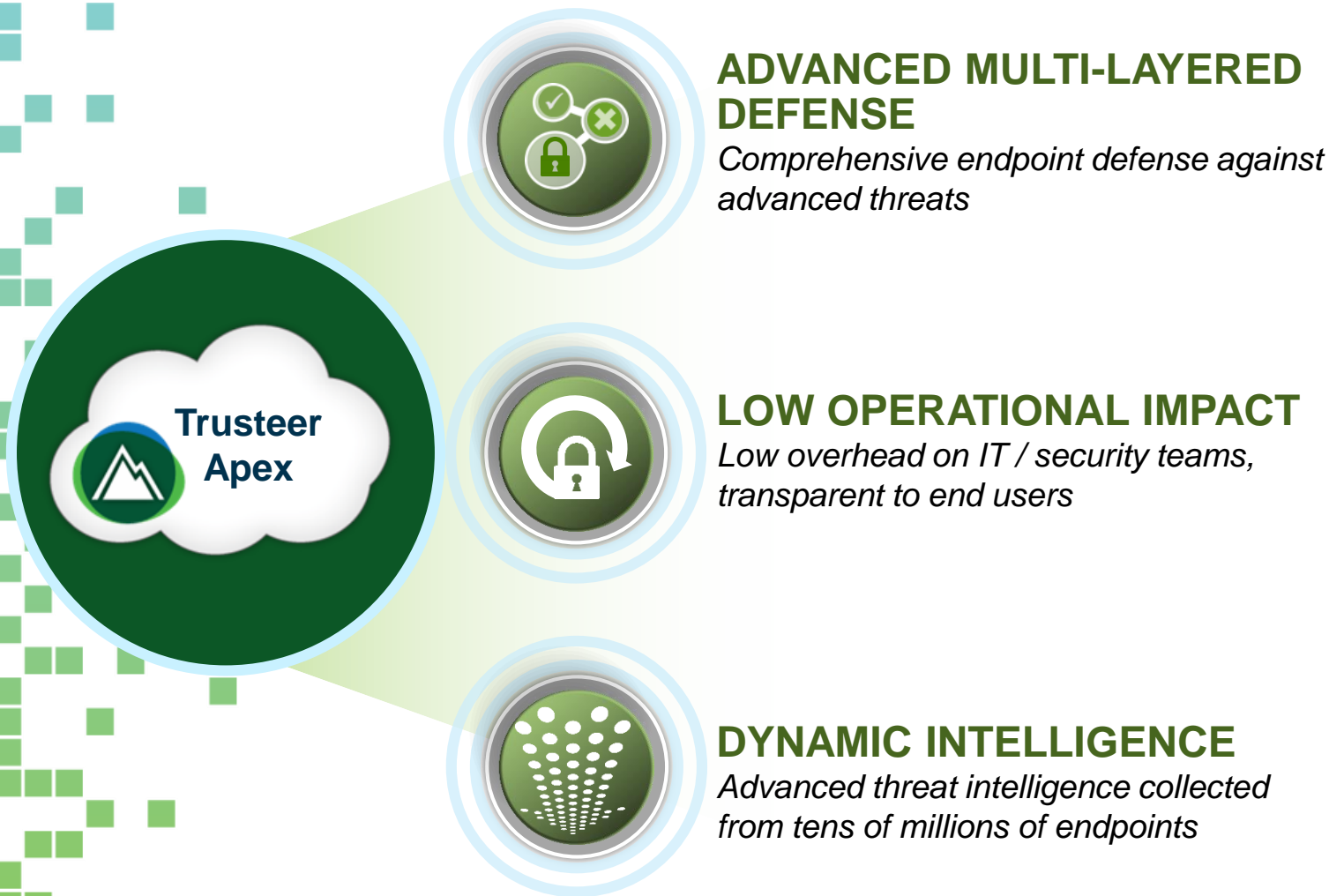
@

Gather

Prevent

Endpoint Prevention: Trusteer Apex

Preemptive, low-impact defense for enterprise endpoints



Trusteer Apex multi-layered defense architecture

Threat and Risk Reporting Vulnerability Mapping and Critical Event Reporting

Advanced Threat Analysis and Turnkey Service

Credential Protection

- Prevent reuse on non-corporate sites
- Protect against submission on phishing sites
- Report on credential usage

Exploit Chain Disruption

- Block anomalous activity caused by exploits
- Zero-day defense by controlling exploit chain

Malware Detection and Mitigation

- Detection and mitigation of massively distributed APTs
- Cloud-based detection of known threats

Lockdown for Java

- Block high-risk actions by malicious Java applications
- Administer the trust level reducing user disruption

Malicious Communication Prevention

- Block malware communication
- Disrupt command and control
- Protects against data exfiltration

Global Threat Research and Intelligence

Global threat intelligence delivered in near-real time from the cloud

Network Prevention: IBM Security Network Protection

Evolving protection to keep you Ahead of the Threat[®]



BROAD COVERAGE

Protects against a full spectrum of attack techniques



ZERO-DAY PROTECTION

Protects against known and unknown attacks



ADVANCED INTELLIGENCE

Powered by XForce[®] global threat research

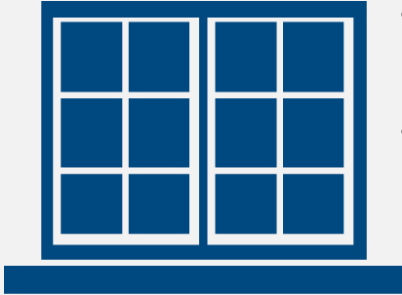
Providing protection beyond exploit matching

VULNERABILITY

vs.

EXPLOIT

A weakness in a system



- Can be used to do something unintended
- Can be exploited in multiple ways

A method used to gain system entry



- Many different exploits can target a single vulnerability
- Not all exploits are publicly available, and mutation is common

IBM PROTECTION

vs.

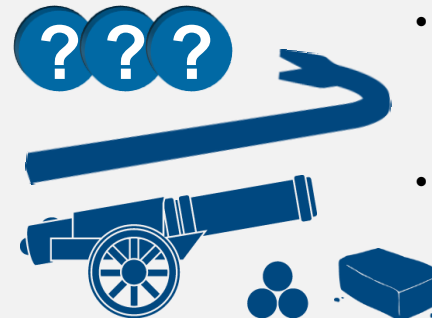
OTHER PRODUCTS

IBM protects the vulnerability



- Stays ahead of the threat with pre-emptive protection that stops things from breaking the window

Other products only block the exploits

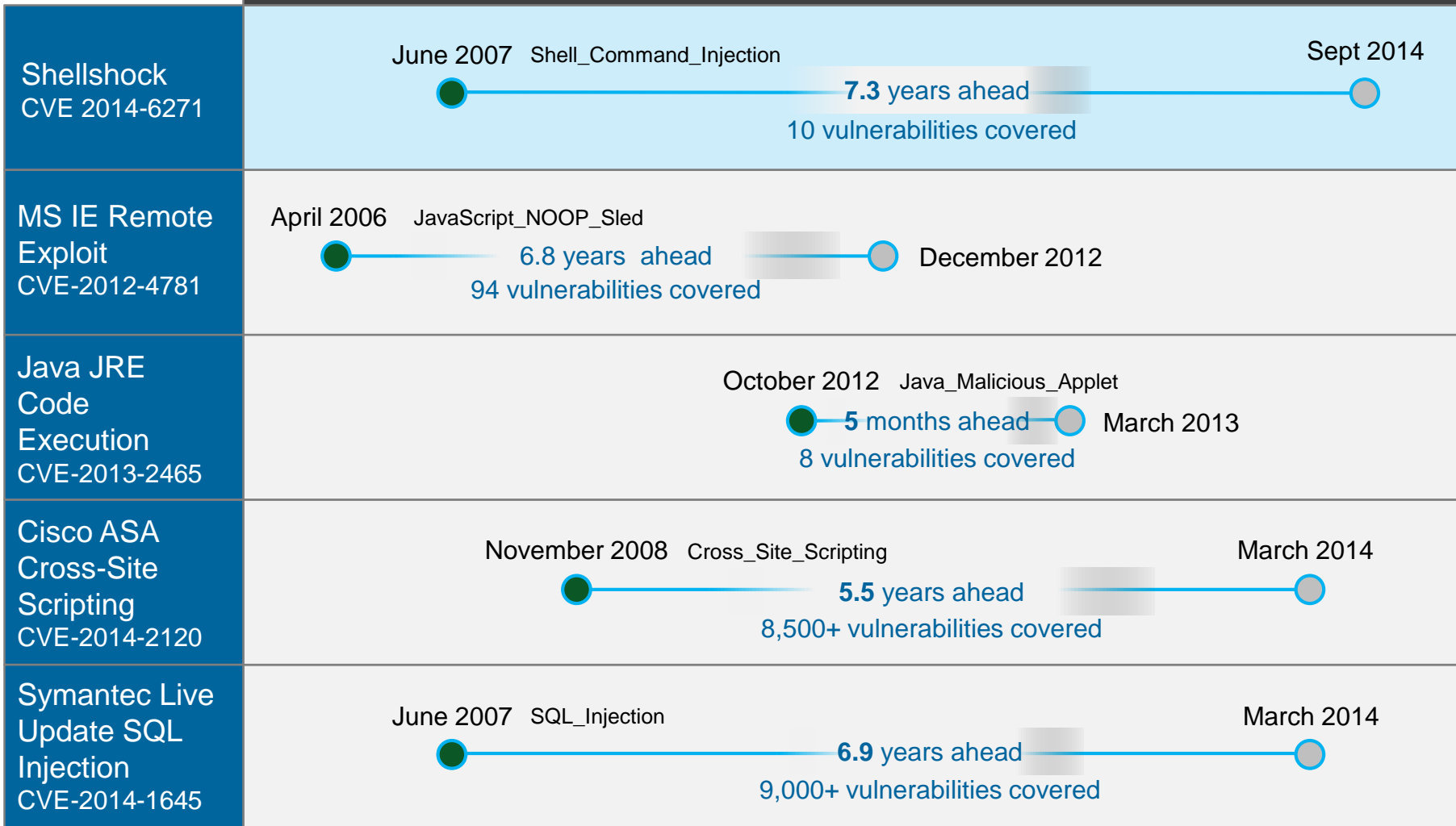


- Looks for methods that can break the window
- Keeping up can be challenging

Behavioral-based detection blocks attacks never before seen

● IBM Protection ● Disclosed

2006 —————> 2014



IBM goes beyond pattern matching with a broad spectrum of vulnerability and exploit coverage

Exploit Signatures

Attack-specific pattern matching

Other IPS solutions stop at pattern matching

Vulnerability Decodes

Focused algorithms for mutating threats

Application Layer Heuristics

Proprietary algorithms to block malicious use

Web Injection Logic

Patented protection against web attacks, e.g., SQL injection and cross-site scripting

Shellcode Heuristics

Behavioral protection to block exploit payloads

Content Analysis

File and document inspection and anomaly detection

Protocol Anomaly Detection

Protection against misuse, unknown vulnerabilities, and tunneling across 230+ protocols

Data Prevention: IBM Guardium Advanced Data Activity Monitoring

Prevent unauthorized data access, changes and leaks

IBM Guardium Data Activity Monitoring



CONTAIN ACCESS ABUSE

Prevent power user abuse to sensitive data access



ENFORCE LEGITIMATE USE OF DATA

Prevent misuse or change to sensitive data



BLOCK DATA LEAKAGE

Prevent intrusion, theft and leaks from databases and files

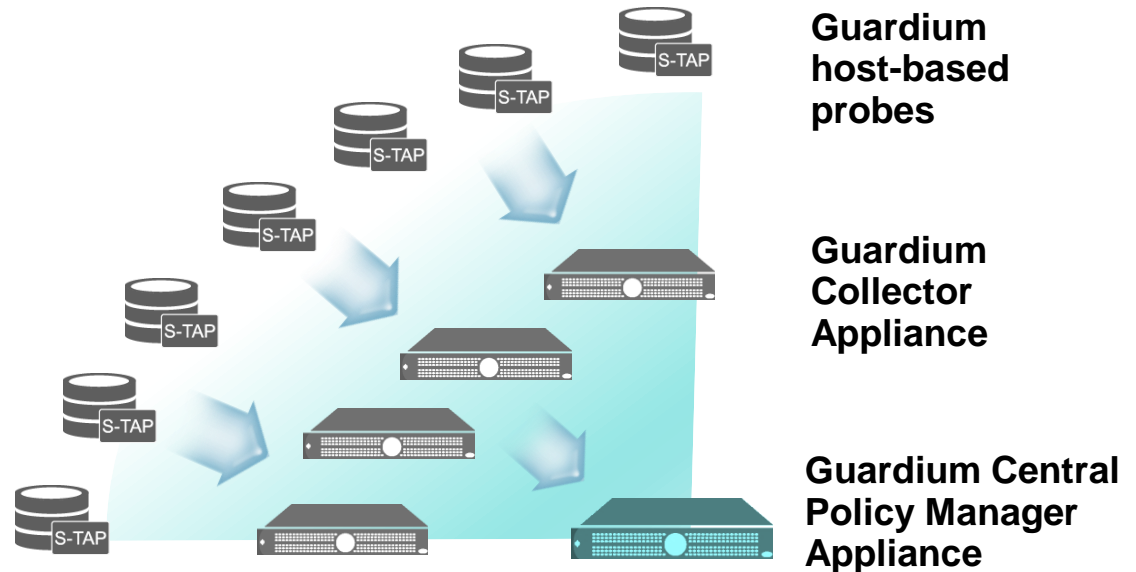
Real-time data access policy enforcement

IBM Guardium Data Activity Monitoring - Advanced

Increase efficiency via automation and reduce cost of manual redaction

Control the data viewed by each user

Address both external attacks AND block unauthorized access by privileged users



- Continuous, policy-based, real-time monitoring of all data traffic activities, including actions by privileged users
- Database infrastructure scanning for missing patches, mis-configured privileges and other vulnerabilities
- Data protection compliance automation

Continuously monitor activity from across the attack chain

Pre-Attack Analytics

Predict and prioritize security weaknesses before adversaries

- Use automated vulnerability scans and rich security context
- Emphasize high-priority, unpatched, or defenseless assets requiring attention

Centralized Vulnerability Management



Real-time Attack Analytics

Detect activity and anomalies outside normal behavior

- Correlate and baseline massive sets of data
- From logs, events, flows, user activity, assets, locations, vulnerabilities, external threats, and more

Next-Generation SIEM

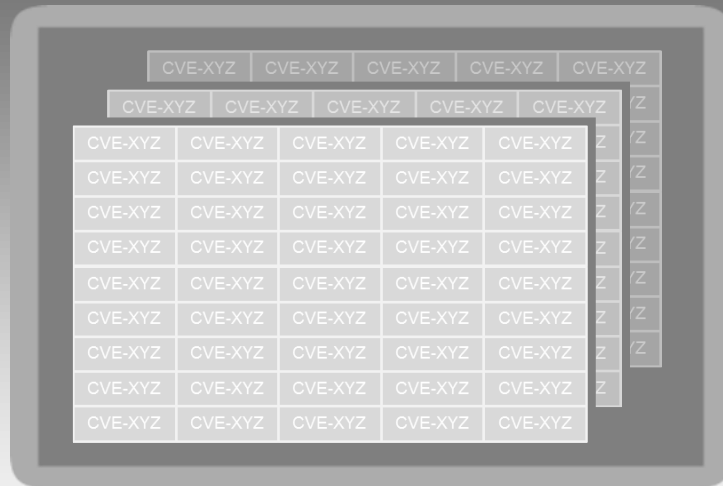
Security Analytics Platform

Detect

Vulnerability management to detect and prioritize weaknesses

Traditional Security

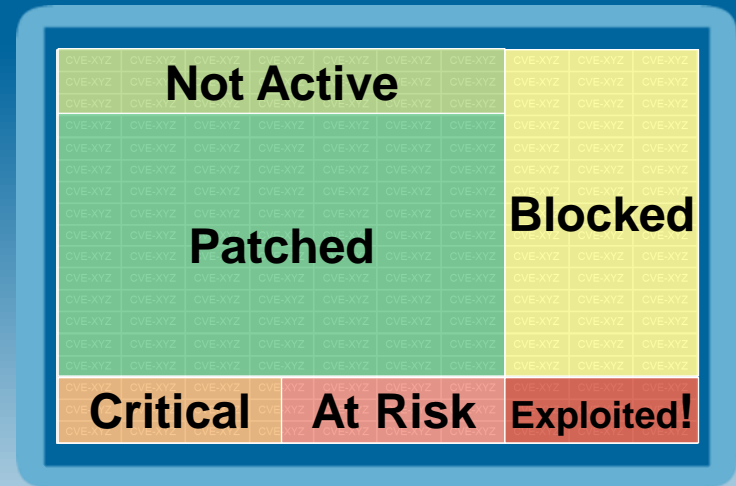
Common Vulnerabilities and Exposures (CVEs)



A computer monitor icon with a grid of CVEs. The grid consists of 10 rows and 5 columns of boxes, each containing the text 'CVE-XYZ'. The grid is slightly offset to the left, revealing another identical grid behind it, suggesting a large volume of data.

IBM Security QRadar

Vulnerability Management



A computer monitor icon with a grid of CVEs. The grid is color-coded and categorized. The top two rows are green and labeled 'Not Active'. The middle three rows are yellow and labeled 'Blocked'. The bottom row is red and labeled 'Critical', 'At Risk', and 'Exploited!'. The grid is slightly offset to the left, revealing another identical grid behind it.

Embedded intelligence offers automated offense identification

Extensive Data Sources



Security devices



Servers and mainframes



Network and virtual activity



Data activity



Application activity



Configuration information



Vulnerabilities and threats



Users and identities



Global threat intelligence

Automated Offense Identification

- Built in data classification
- Automatic asset, service, user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection

Embedded Intelligence



Suspected Incidents

Prioritized Incidents



Answering questions to help detect and remediate attacks

What was the attack?

Is the attack credible?

Offense 909
Summary Display ▾ | Events | Connections | Flows | View Attack Path | Actions ▾ | Print | ?

Magnitude	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>	Status		Relevance	8	Severity	5	Credibility	4	
Description	Potential Data Loss	Offense Type	Source IP							
		Event/Flow count	111 events and 1,042 flows in 13 categories							
Source IP(s)	10.0.110.221 (dhcp-221-users-2.acme.com)		Start	Oct 18, 2013 12:28:02 PM						
Destination IP(s)	Local (2) Remote (376)		Duration	4d 10h 42m 57s						
Network(s)	Multiple (3)		Assigned to	admin						

Offense Source Summary

IP	10.0.110.221	Location	Users.Users-2
Magnitude	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	Vulnerabilities	0
Username	compliance	MAC Address	00:0E:0C:B4:D8:EE
Host Name	dhcp-221-users-2.acme.com	Weight	0
Asset Name	dhcp-221-users-2.acme.com	Events/Flows	15,310
Offenses	8		

Last 5 Notes

Notes	Username	Creation Date
Potential data loss detected, forensics case created	admin	Oct 21, 2013 6:39 AM

Forensics Reconstructions

Case	Collection	IP	Start	End	Status
DataLoss	DataLoss	10.0.110.221	3/27/2014 3:31:00 PM	3/27/2014 4:31:00 PM	SUCCESS

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
dhc...	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	Users.Users-2	No	compliance	00:0E:0C:B4:D8:EE	0	8	21	0s	15,310

Who was responsible for the attack?

How valuable are the targets to the business?

Where are they located?

What was stolen and where is the evidence?

Are any of the assets vulnerable?

How many targeted assets are involved?

Rapidly investigate breaches, retrace activity, and learn from findings

Post-Attack Incident Forensics

Reduce the time to discover what happened and when

- Reconstruct attack activity and content from full-packet data
- Apply search engine technology and visualizations

Rapid Forensics Investigation



Real-time Incident Response

Enforce continuous compliance at the endpoint

- Automatic quarantine of non-compliant endpoints
- Custom remediation and patching of affected machines

Endpoint Policy Enforcement



Emergency Response Services

Prepare for and withstand security breaches

- Gain access to key resources that enable faster recovery and reduce incident impact

Breach Management Expertise



Respond

IBM Security QRadar Incident Forensics

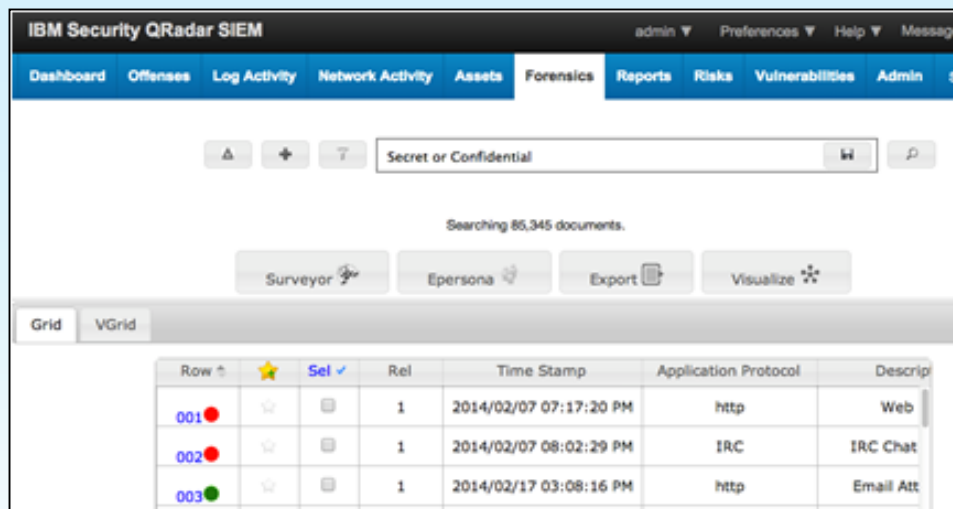
Intuitive investigation of security incidents



Drastic reduction of investigation time

Evidence gathering against malicious entities

Root cause identification of successful breaches



“Research findings indicate enterprise organizations want increased awareness of advanced threats without the need for additional resources and forensics expertise.”

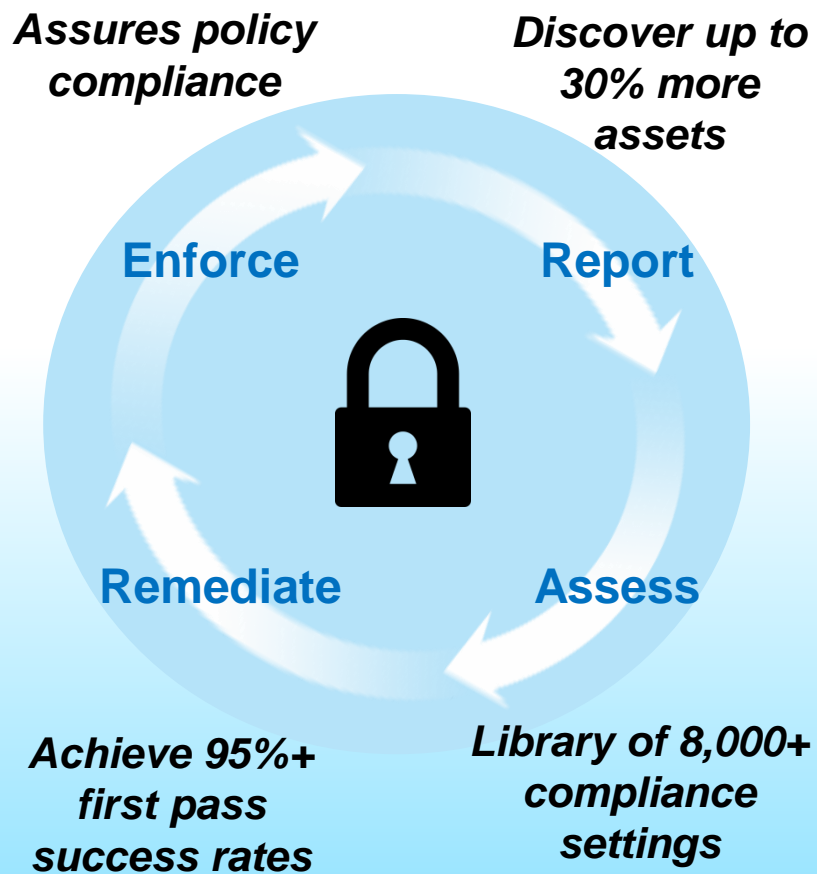
Jon Oltsik, Enterprise Systems Group (ESG)

Win the race against time



IBM BigFix for Security and Compliance

Automatically and continuously enforce policy at the endpoint



- Automates and enforces **continuous security configuration policy compliance**.
- Easily and quickly assess endpoint **security posture**.
- Automatically **patch** and **remediate** non-compliant endpoints.
- Deploy, update, and health-check **third party antivirus** solutions.
- Identify, manage, and report on policy **exceptions and deviations**.
- Automatic policy based **quarantine** of non-compliant endpoints.

Experienced services aiding the response process

Prepare and more quickly respond to security threats and incidents



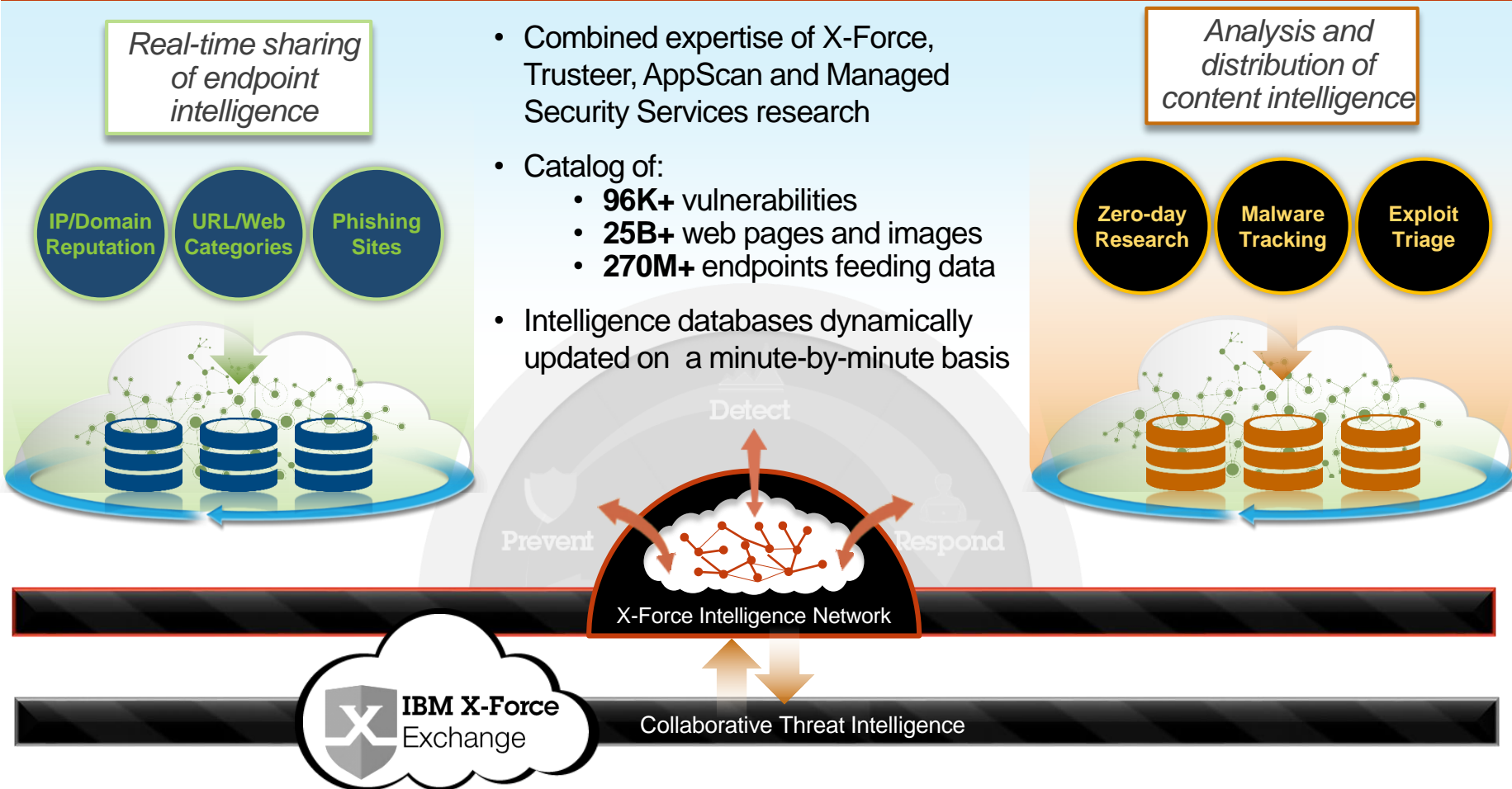
Plan, prepare and respond with proven expertise from mainframe to mobile

The complex block contains four square icons on a dark blue background. From left to right: 1. A document icon with three checkmarks (two green, one red) indicating a checklist or assessment. 2. A stack of three document icons representing reports or plans. 3. A red circular icon with a white telephone handset and a white cross, with "24/7" in a blue circle above it, representing 24/7 emergency services. 4. A blue globe icon with a smartphone on top, surrounded by various mobile app icons, representing mobile security.

Emergency Response Services	Penetration Testing	Incident Response Planning
Executive Protection	APT Survival Kit	Active Threat Assessment
Application Security Assessment	Smart and Embedded Device Security	Application Source Code Security Assessment

Leverage threat intelligence with product integrations that draw upon human and machine-generated information

Global Threat Intelligence by IBM X-FORCE Research

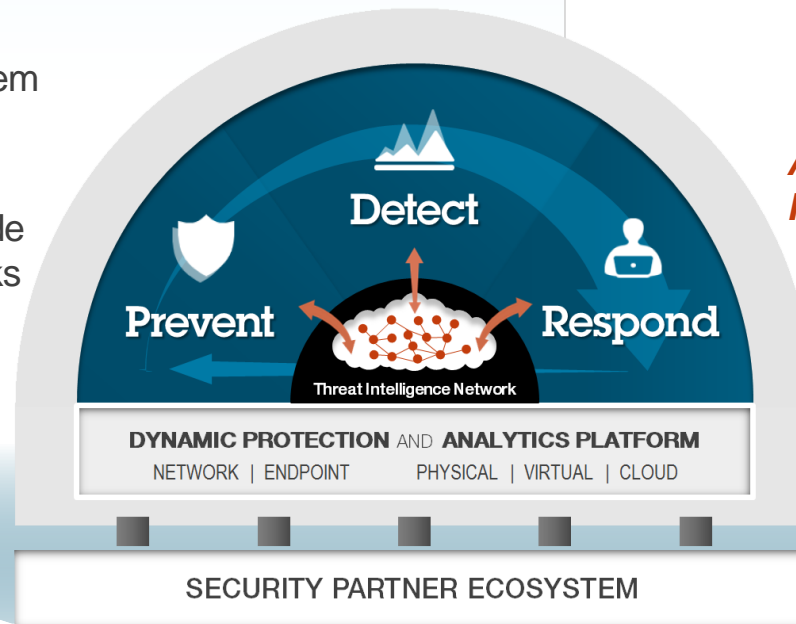


Share, analyze, and act upon information gathered from an ecosystem of third-party products

Security Partner Ecosystem Integrations

IBM Security Partner Ecosystem

- 100+ vendors
- 450+ products
- Complementary integrated solutions
- Strengthens the threat protection lifecycle
 - Leverage a vibrant ecosystem of security products
 - Increase visibility, collapse information silos, and provide insights on advanced attacks



Advanced Threat Protection Integrations



TREND
MICRO™



DAMBALLA

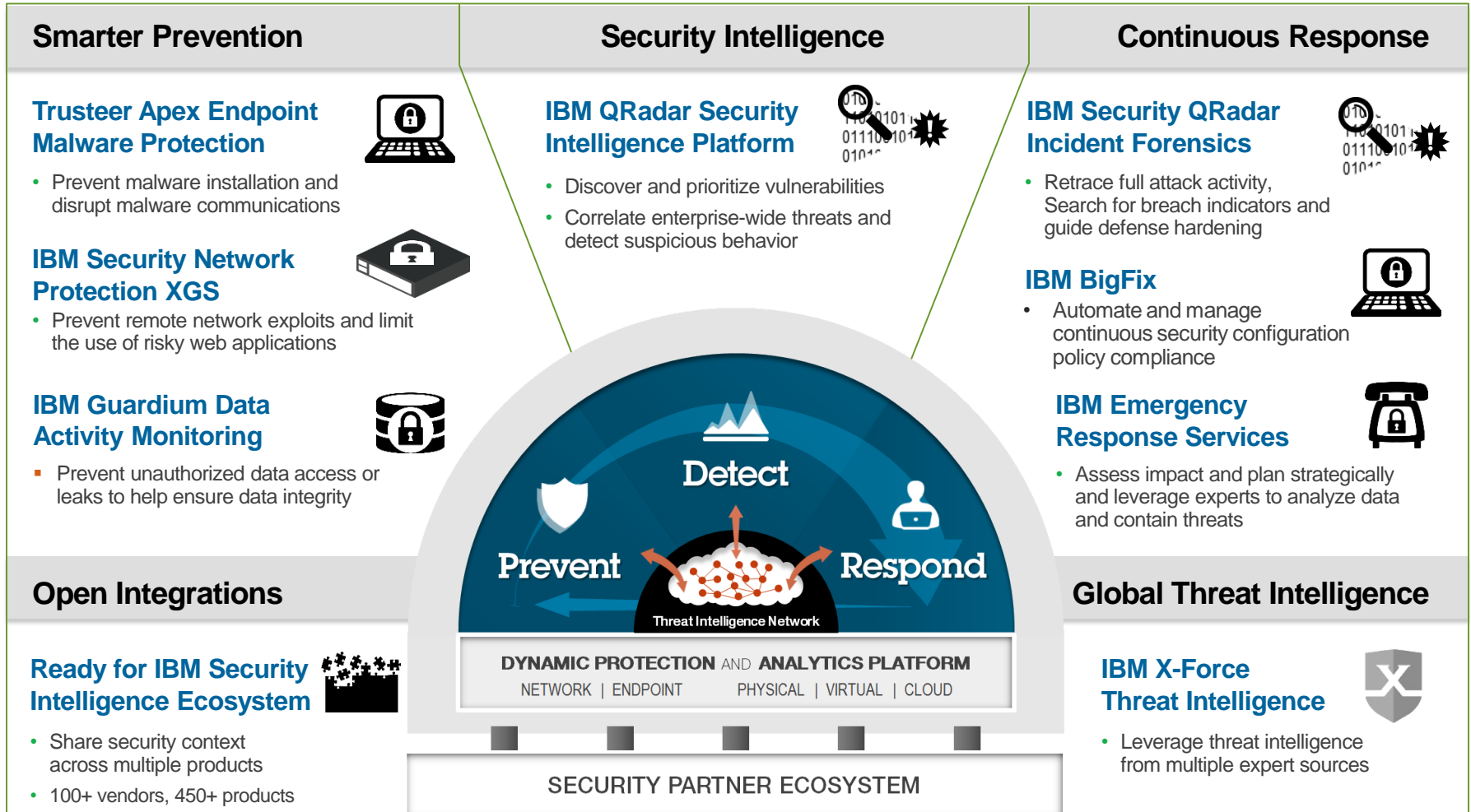


Additional IBM QRadar Partners Include



IBM Threat Protection System

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



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.

THANK YOU

www.ibm.com/security



IBM Security

Intelligence. Integration. Expertise.

© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.