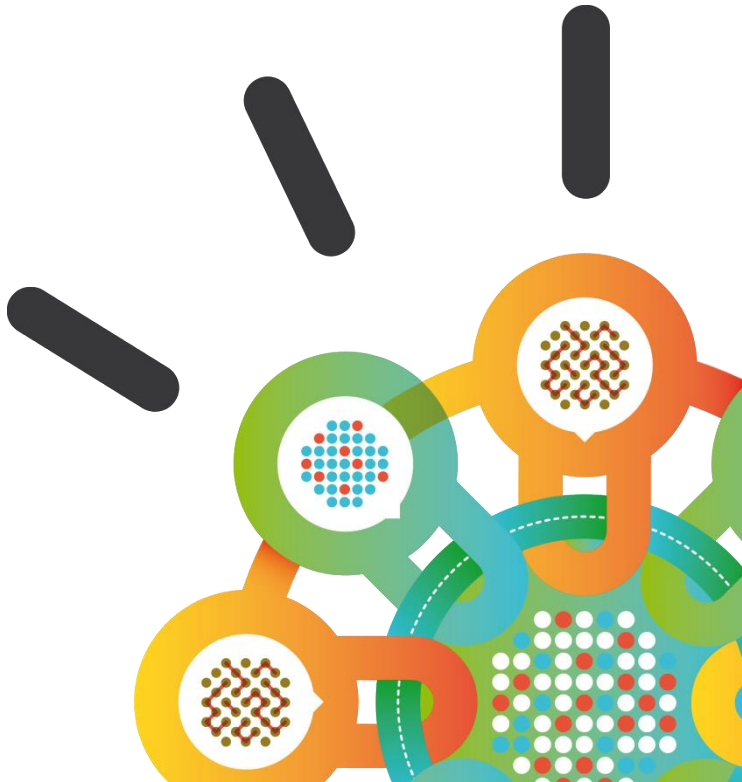
Security Intelligence.
Think Integrated.

4 Undeniable Truths of Advanced Threat Protection

March 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

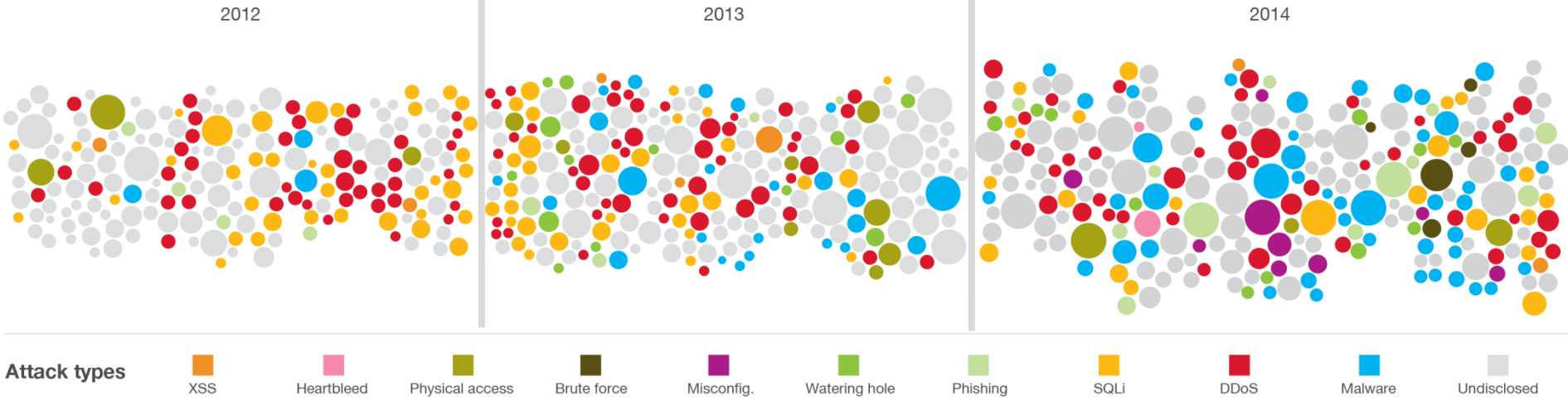
40% increase
in reported data breaches and incidents

Relentless Use of Multiple Methods

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

"Insane" Amounts of Records Breached

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



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® Research and Development

IBM X-Force Threat Intelligence Quarterly – 1Q 2015

2014 IBM Chief Information Security Officer Assessment

And the cost of a data breach is on the rise, with customers at risk

The average cost of a data breach increased

15%

in 2013

A single lost or stolen data record cost on average

$145 in 2013

A single breach of sensitive personal data cost

$3.5 million

in 2013

2014 Cost of Data Breach Study

From Ponemon Institute, sponsored by IBM

Security is a board room discussion, and security leaders are more accountable than ever before

CEO	CFO/COO	CIO	CHRO	CMO
Loss of market share and reputation Legal exposure	Audit failure Fines and criminal charges Financial loss	Loss of data confidentiality, integrity and/or availability	Violation of employee privacy	Loss of customer trust Loss of brand reputation

Your Board and CEO demand a strategy

Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series

Are security teams up for the challenge?

New threats require new thinking, but most are defending against yesterday's attacks

Threats have evolved…

Broad Attacks
Indiscriminate malware, spam and DoS activity

Targeted Attacks
Advanced, persistent, organized, and politically or financially motivated

Requiring a new approach to protection…

Tactical Approach *Compliance-driven, Reactionary*	Strategic Approach *Intelligence-driven, Continuous*
○ Build multiple perimeters	○ Assume constant compromise
○ Protect all systems	○ Prioritize high-risk assets
○ Use signature-based methods	○ Use behavioral-based methods
○ Periodically scan for known threats	○ Continuously monitor activity
○ Read the latest news	○ Consume real-time threat feeds
○ Shut down systems	○ Gather, preserve, retrace evidence

…yet the majority of security teams are still using siloed, 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.

The IBM Threat Protection System

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

Made possible by the following:

Accelerated Roadmap

Significant investment across 10 development labs to fast-track advanced threat protection offerings

Unique Integrations

Strategic focus on connecting IBM products to streamline intelligence sharing and take action

New Partnerships

Coordinated outreach across the industry to bring together interoperable products for our customers

Focus on critical points in the attack chain with preemptive defenses on both the endpoint and network and protecting the data

Trusteer Apex Malware Protection

On the Endpoint

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

IBM Security Network Protection XGS

On the Network

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

IBM Guardium Data Activity Monitoring

At Data Access

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

Trusteer Apex

Preemptive, low-impact defense for enterprise endpoints

ADVANCED MULTI-LAYERED DEFENSE

Comprehensive endpoint defense against advanced threats

LOW OPERATIONAL IMPACT

Low overhead on IT / security teams, transparent to end users

DYNAMIC INTELLIGENCE

Advanced threat intelligence collected from tens of millions of endpoints

Trusteer Apex multi-layered defense architecture

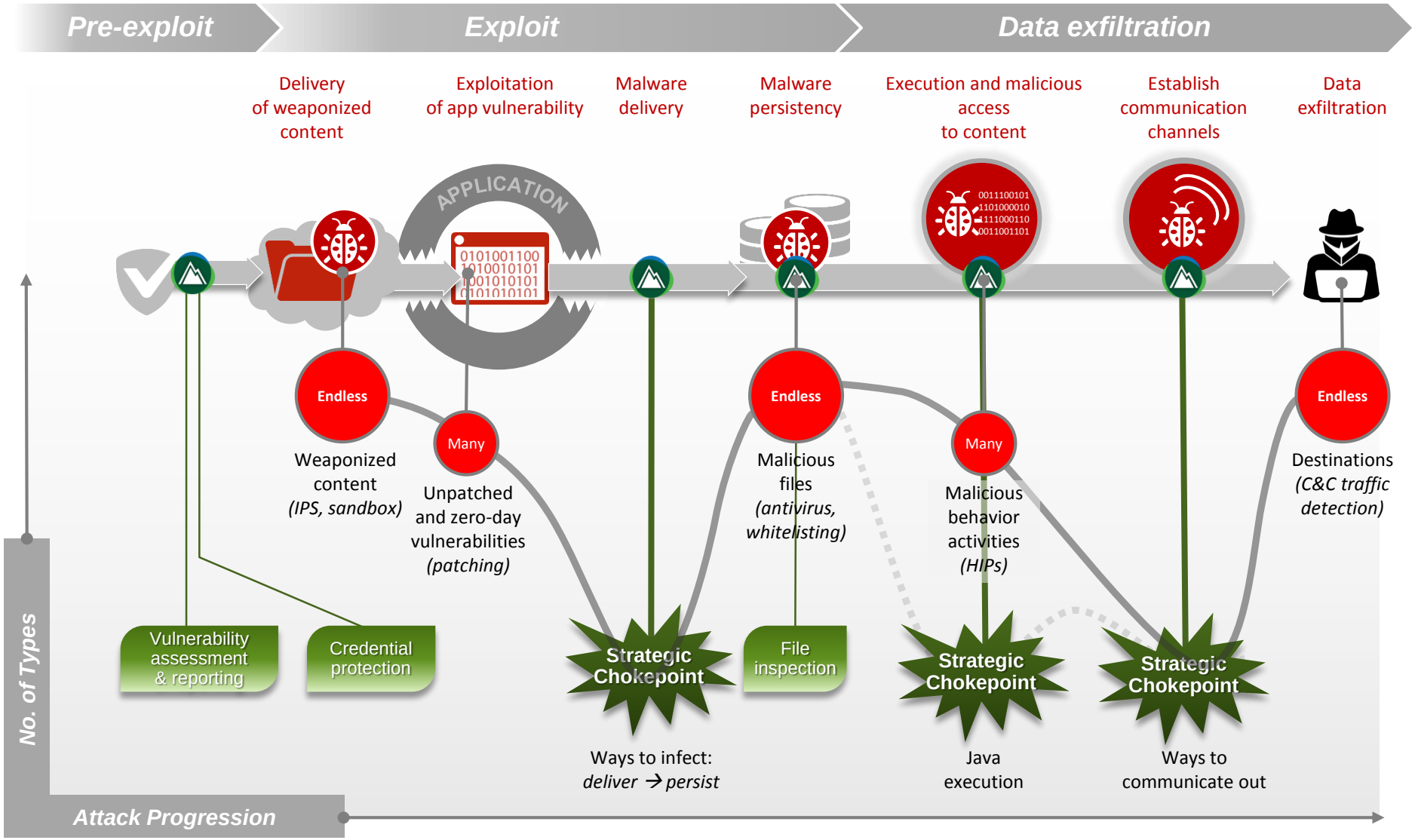
Threat and Risk Reporting
Vulnerability Mapping and Critical Event Reporting

Advanced Threat Analysis and Turnkey Service

Credential Protection	Exploit Chain Disruption	Malware Detection and Mitigation	Lockdown for Java	Malicious Communication Prevention
• Prevent reuse on non-corporate sites • Protect against submission on phishing sites • Report on credential usage	• Block anomalous activity caused by exploits • Zero-day defense by controlling exploit chain	• Detection and mitigation of massively distributed APTs • Cloud-based detection of known threats	• Block high-risk actions by malicious Java applications • Administer the trust level reducing user disruption	• Block malware communication • Disrupt command and control • Protects against data exfiltration

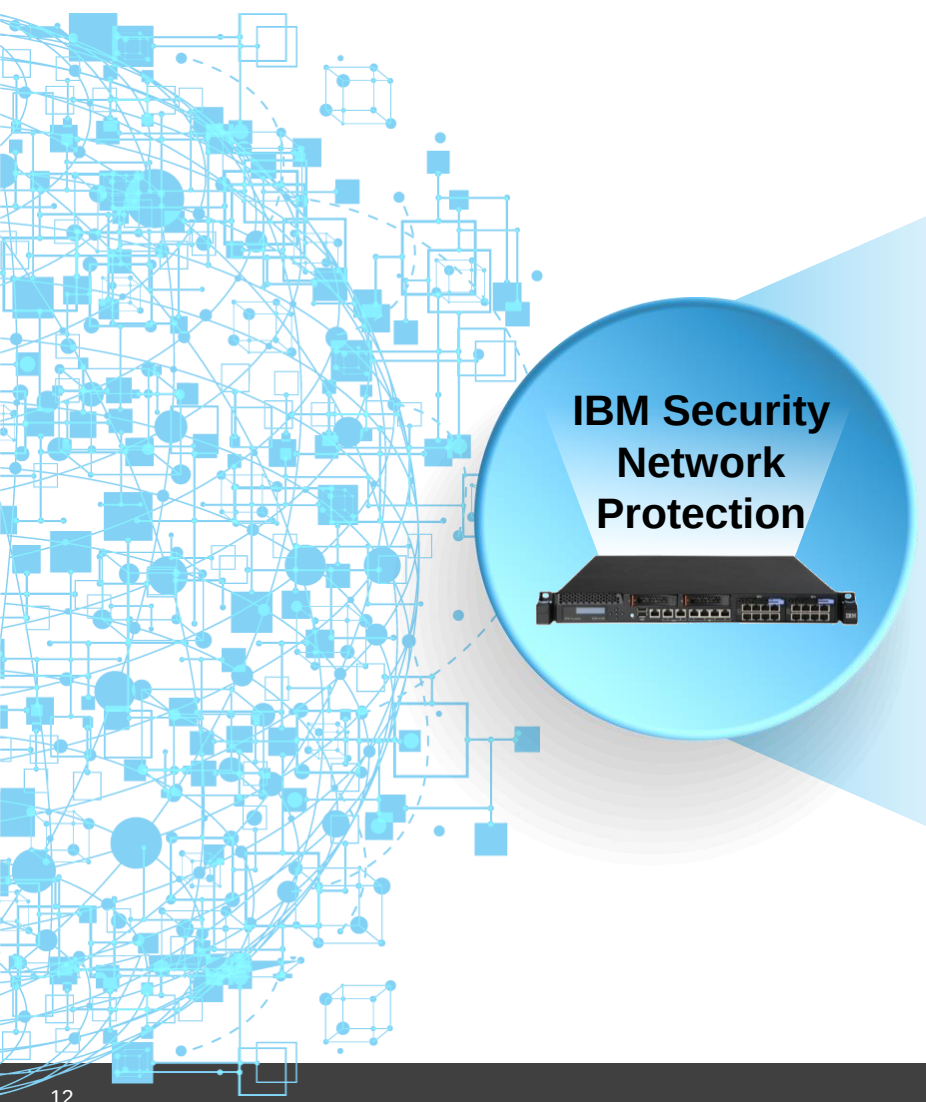
Global Threat Research and Intelligence
Global threat intelligence delivered in near-real time from the cloud

Controlling exploit-chain chokepoints



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

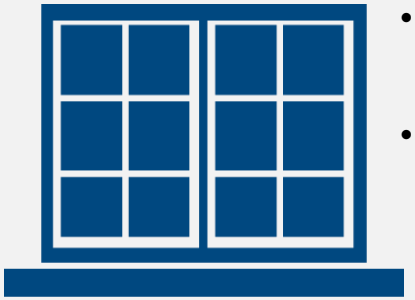
ADVANCED INTELLIGENCE

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

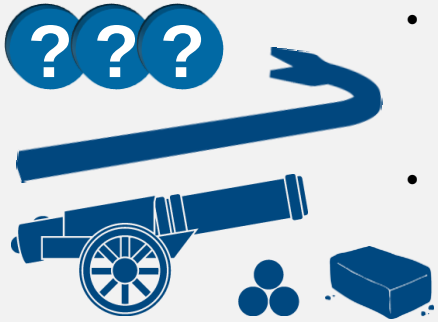
- Many different exploits can target a single vulnerability
- Not all exploits are publicly available, and mutation is common

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

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

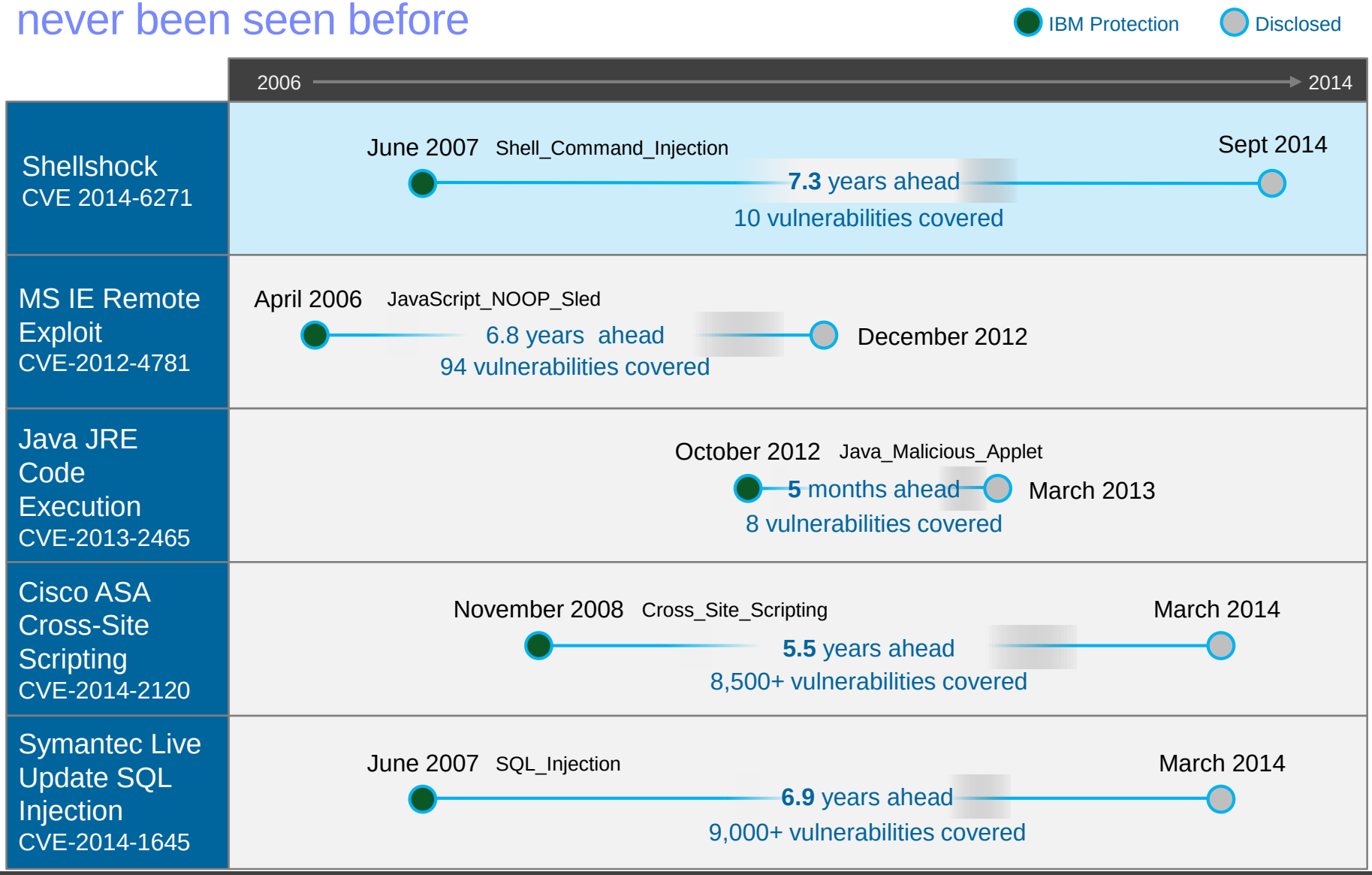
Content Analysis

File and document inspection and anomaly detection

Protocol Anomaly Detection

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

Behavioral-based detection blocks attacks that have never been seen before



IBM Guardium Advanced Data Activity Monitoring

Prevent unauthorized data access, changes and leaks

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 databased and files

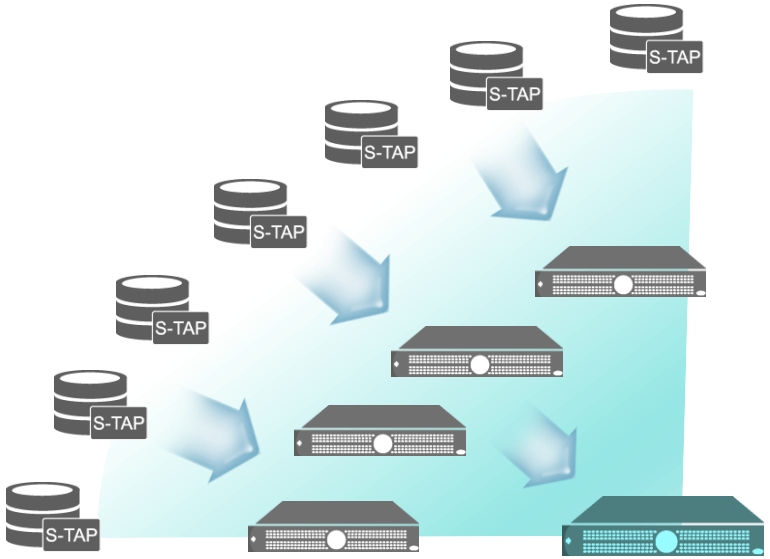
Real-time data access policy enforcement

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



Guardium host-based probes

Guardium Collector Appliance

Guardium Central Policy Manager Appliance

- 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 security-relevant activity from across the entire organization

Predict and prioritize security weaknesses before adversaries do

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

Pre-Attack Analytics

IBM Security QRadar Vulnerability Manager

IBM Security QRadar Security Intelligence Platform

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

Real-time Attack Analytics

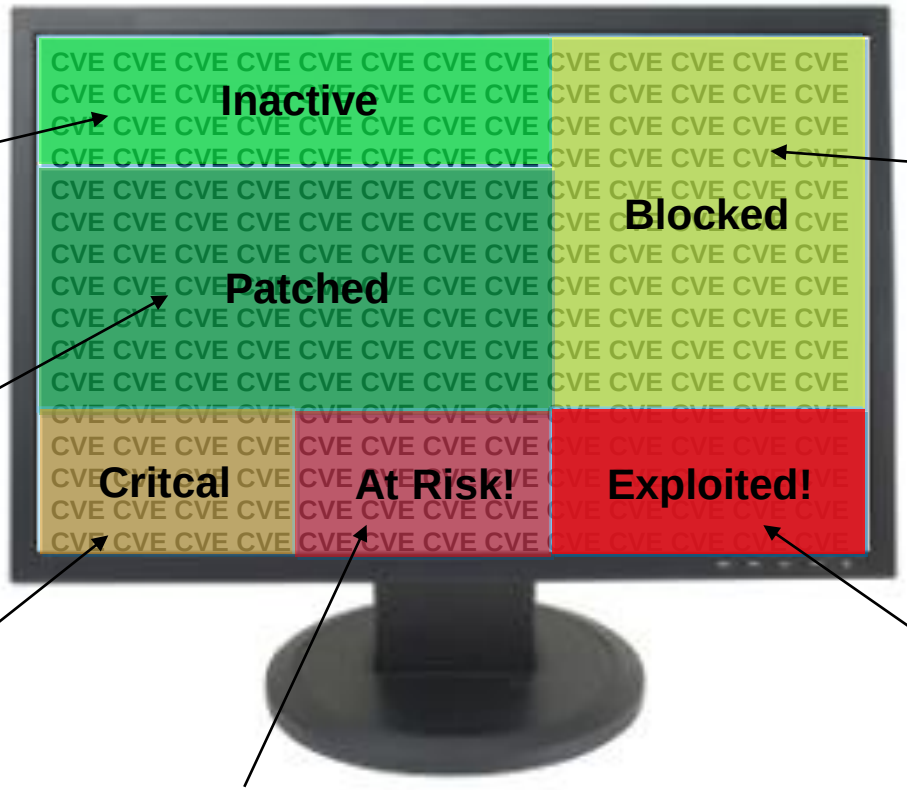
IBM Security QRadar SIEM

Vulnerability management to detect and prioritize weaknesses

Inactive: Flow analytics sense application activity

Patched: Endpoint management indicates which vulnerabilities will be patched

Critical: Vulnerability knowledge base, remediation flow and risk management policies identify business critical vulnerabilities



At Risk: X-Force Threat and SIEM security incident data, coupled with network traffic flow information, provide visibility to assets communicating with potential threats

Blocked: Risk Management shows which vulnerabilities are blocked by firewalls and IPSs

Exploited: SIEM correlation and IPS data help reveal which vulnerabilities have been exploited

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

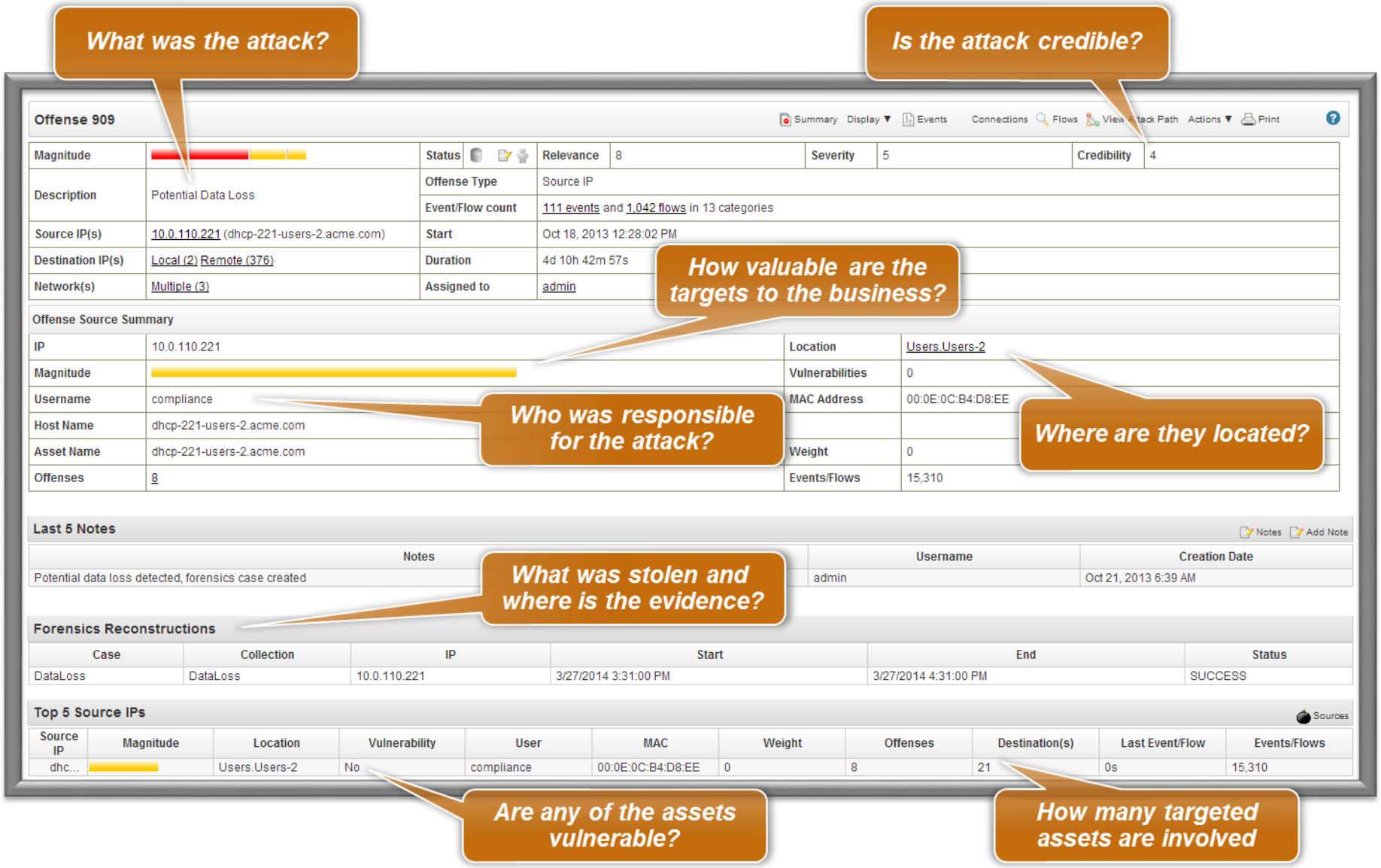
- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents of the box

Embedded Intelligence

Suspected Incidents

Prioritized Incidents

Answering questions to help prevent and remediate attacks



Offense 909

Summary | Display | Events | Connections | Flows | View Attack Path | Actions | Print

Magnitude		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		Vulnerabilities	0
Username	compliance	MAC Address	00:0E:0C:B4:D8:EE
Host Name	dhcp-221-users-2.acme.com		
Asset Name	dhcp-221-users-2.acme.com	Weight	0
Offenses	8	Events/Flows	15,310

Last 5 Notes

Notes | Add Note

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

Sources

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
dhc...		Users.Users-2	No	compliance	00:0E:0C:B4:D8:EE	0	8	21	0s	15,310

Quickly investigate breaches, retrace activity, and learn from findings to remediate weaknesses

Post-Attack Incident Forensics

Reduce the time to fully discover what happened and when it occurred

- Index and reconstruct attack activity and content from full-packet network data
- Apply search engine technology and advanced visualizations

IBM Security QRadar Incident Forensics

Rapid Response Integrations

Quickly expand security coverage to prevent further harm

- Share indicators across control points
- Dynamically apply customized rules

IBM Security Framework Integrations

Real-time Incident Response

Enforce continuous endpoint compliance

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

IBM Endpoint Manager

Emergency Response Services

Help prepare for and withstand security breaches more effectively

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

24x7

IBM Emergency Response Services

Respond

IBM Security QRadar Incident Forensics

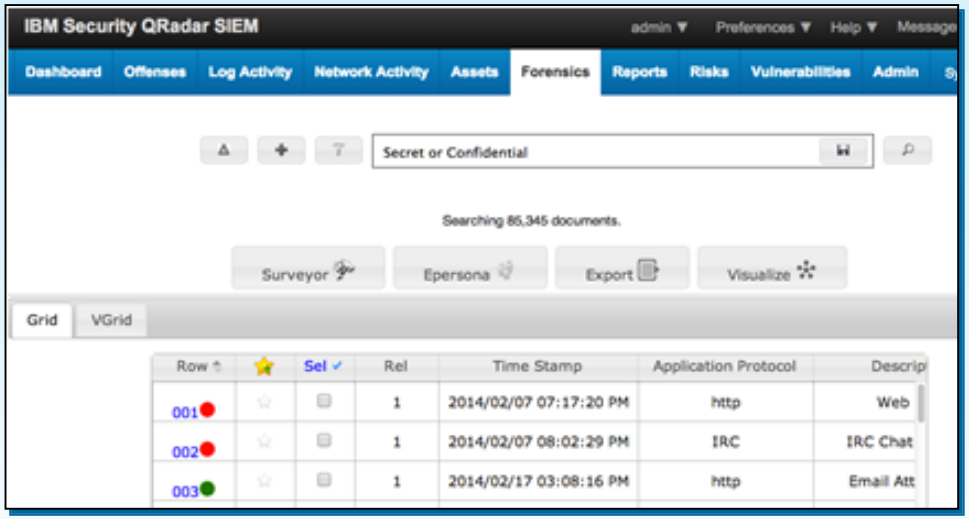
Intuitive investigation of security incidents

QRadar® Incident Forensics

Drastic reduction of investigation time

Evidence gathering against malicious entities

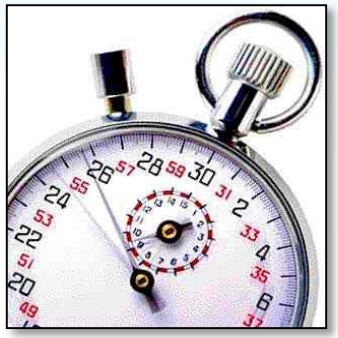
Root cause identification of successful breaches



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

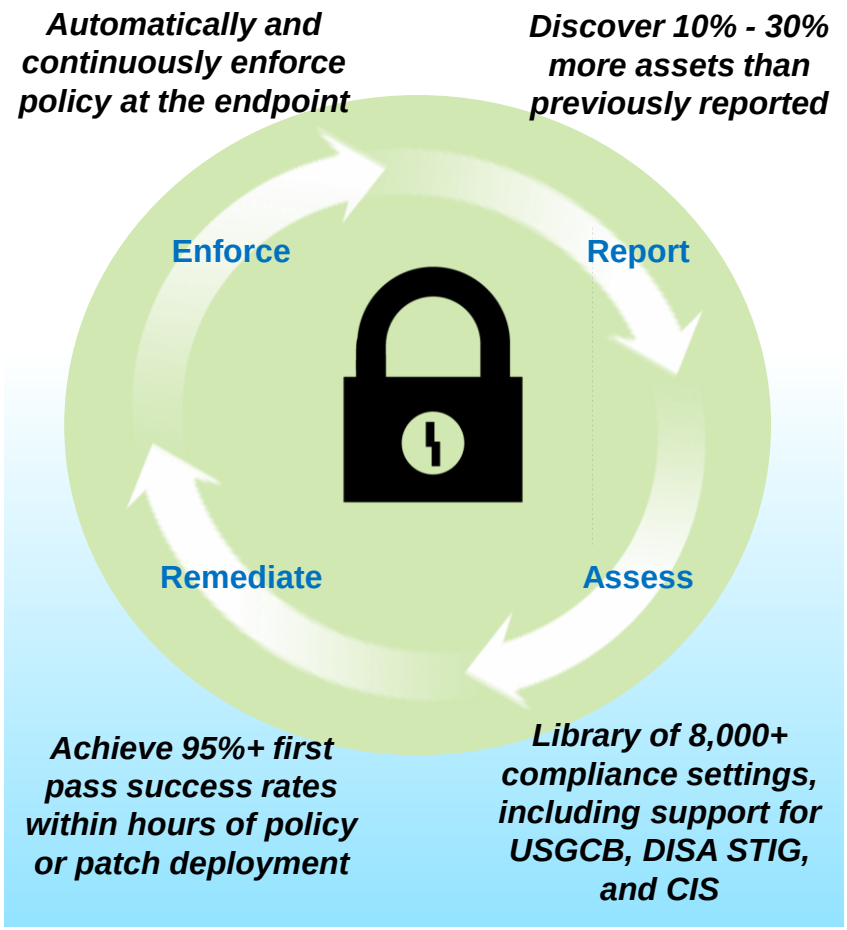
Jon Oltsik, Enterprise Systems Group (ESG)

Win the race against time



IBM Endpoint Manager 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.
- Coordinated Endpoint Management:
  - **Patch**
  - **Vulnerability**
  - **Security Configuration**
  - **Multi-vendor**

Experienced services aiding the response process

Prepare for and withstand sophisticated attacks

ERS subscription includes:

- ✓ Initial planning workshop
- ✓ 120 hrs/yr for incident response or planning
- ✓ Quarterly updates and remote support
- ✓ Access to X-Force Threat Analysis Service
- ✓ Worldwide, around-the-clock coverage
- ✓ Cross-platform support (mainframe to mobile)

- **24x7x365 emergency response** provides access to key resources that can enable faster recovery and reduce business impact from incidents
- **Proven methodology and advanced tools** for incident investigation for forensic level details and to prevent reoccurrence
- **Periodic review and incident case management** enable a broader view and deeper understanding of incidents using intelligence data and analytics
- **Preemptive incident preparation services** reduce risk and exposure to cyber threats ahead of an attack

Cyber Emergency Hotline

(US) 1-888-241-9812
(Worldwide) 1-312-212-8034

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

Global Threat Intelligence

NEW Trusteer an IBM Company

Real-time sharing of Trusteer intelligence

IP/Domain Reputation

URL/Web Categories

Phishing Sites

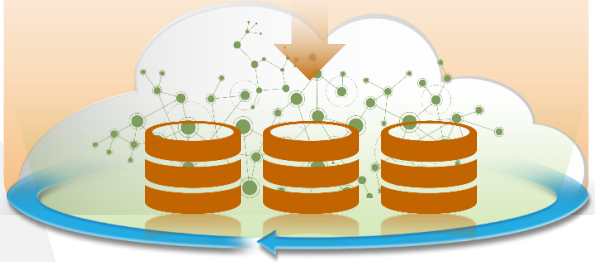
- Combines the renowned expertise of X-Force + Trusteer malware research
- Catalog of **96K+** vulnerabilities,**17B+** web pages, and data from **270M+** endpoints
- Intelligence databases dynamically updated on a minute-by-minute basis

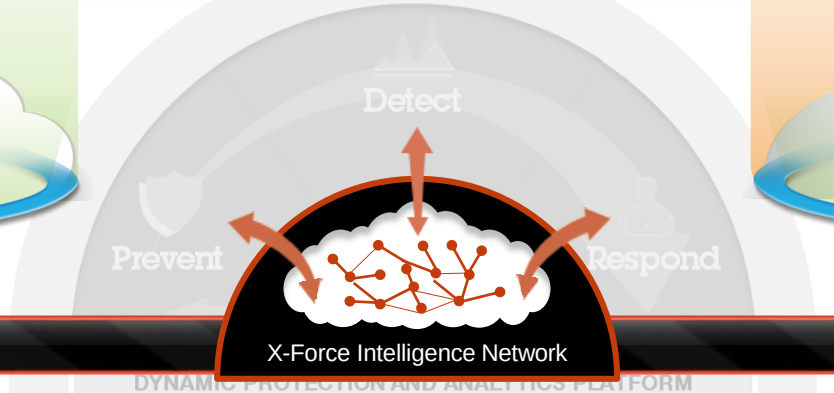
IBM X-Force Research

Zero-day Research

Malware Tracking

Exploit Triage





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

Security Partner Ecosystem and Integrations

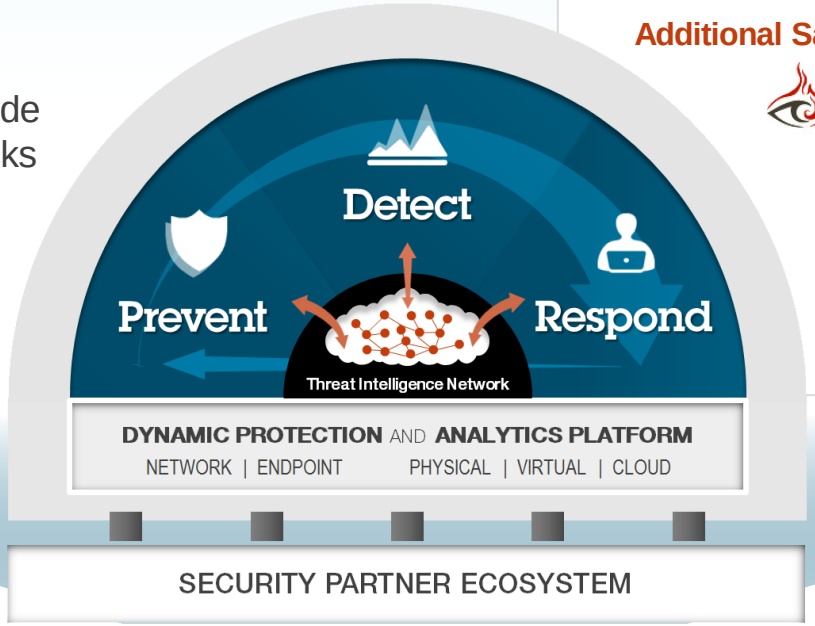
IBM works with a broad set of technology vendors who provide complementary solutions and are integrated with our security products

Strengthen the threat protection lifecycle

- Leverage a vibrant ecosystem of security products
- Increase visibility, collapse information silos, and provide insights on advanced attacks

Ready for IBM Security Intelligence Partner Ecosystem

100+ vendors and 400+ products



Advanced Threat Protection Integrations:

A10 Networks — *SSL Traffic Decryption for QRadar Incident Forensics investigations*

TREND MICRO — *Integration with IBM XGS to block new threats and QRadar for centralized response*

Additional Sample of QRadar Partners:

FireEye, paloalto NETWORKS, DAMBALLA, CISCO, QUALYS, websense, BLUE COAT, JUNIPER NETWORKS, proofpoint

IBM Intelligent Threat Protection

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

Smarter Prevention

Trusteer Apex Endpoint Malware Protection

- Prevent malware installation and disrupt malware communications

IBM Security Network Protection XGS

- Prevent remote network exploits and limit the use of risky web applications

IBM Guardium Data Activity Monitoring

- Prevent remote network exploits and limit the use of risky web applications

Security Intelligence

IBM Security QRadar Security Intelligence

- Discover and prioritize vulnerabilities
- Correlate enterprise-wide threats and detect suspicious behavior

Continuous Response

IBM Security QRadar Incident Forensics

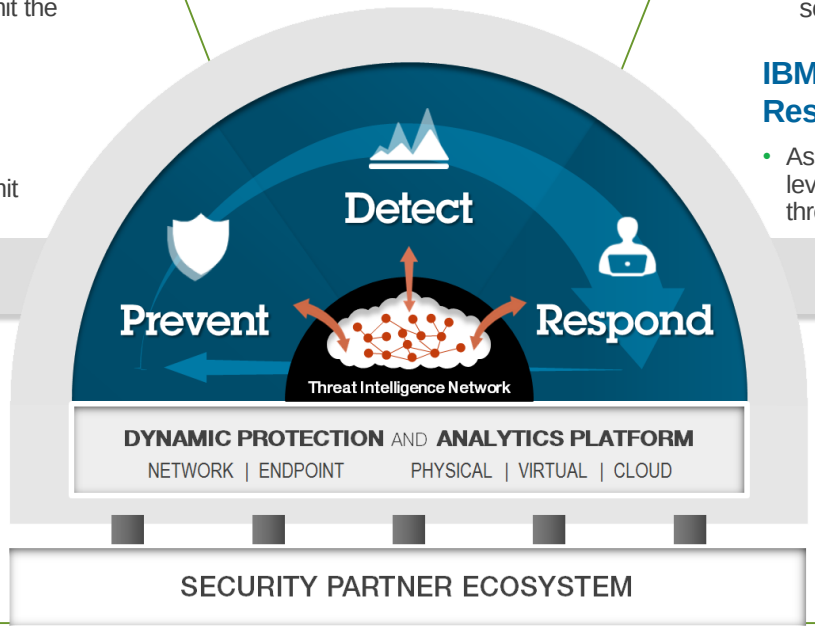
- Retrace full attack activity, Search for breach indicators and guide defense hardening

IBM Endpoint Manager

- Automate and manage continuous security configuration policy compliance

IBM Emergency Response Services

- Assess impact and plan strategically and leverage experts to analyze data and contain threats



Open Integrations

Ready for IBM Security Intelligence Ecosystem

- Share security context across multiple products
- 100+ vendors, 400+ products

Global Threat Intelligence

IBM X-Force Threat Intelligence

- Leverage threat intelligence from multiple expert sources

Find out more…

Twitter
@ibmsecurity

YouTube
youtube.com/user/IBMSecuritySolutions

IBM X-Force Threat Intelligence Reports
http://www.ibm.com/security/xforce/

IBM X-Force Security Insights Blog
www.SecurityIntelligence.com/x-force

Website
ibm.com/security/threat-protection/

And visit us on SecurityIntelligence.com

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.

Thank You

www.ibm.com/security