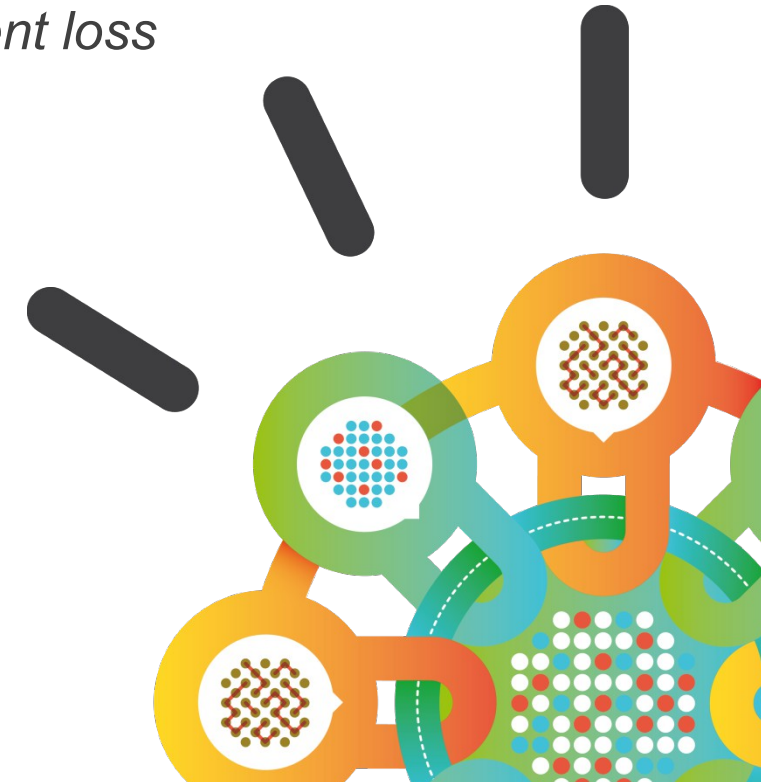
Security Intelligence.
Think Integrated.

IBM Threat Protection System

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



- April 30, 2014

- **Jim Brennan**
- Director, Strategy and Product Management
- Infrastructure Security & X-Force

Disclaimer

Please Note:

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

We are in an era of continuous breaches

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

Operational Sophistication

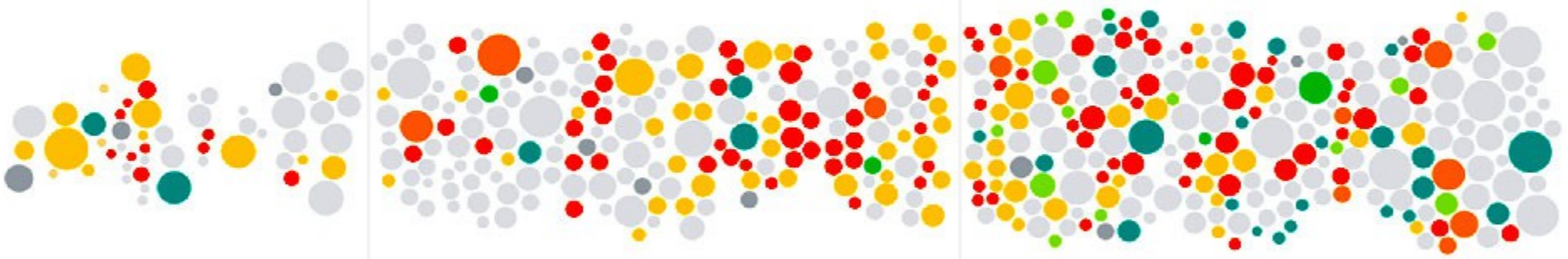
IBM X-Force declared **Year of the Security Breach**

Near Daily Leaks of Sensitive Data

40% increase in reported data breaches and incidents

Relentless Use of Multiple Methods

500,000,000+ records were leaked, while the future shows no sign of change



Attack types

- SQL injection
- Spear phishing
- DDoS
- Third-party software
- Physical access
- Malware
- XSS
- Watering hole
- Undisclosed

Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2014

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

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.

Introducing 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

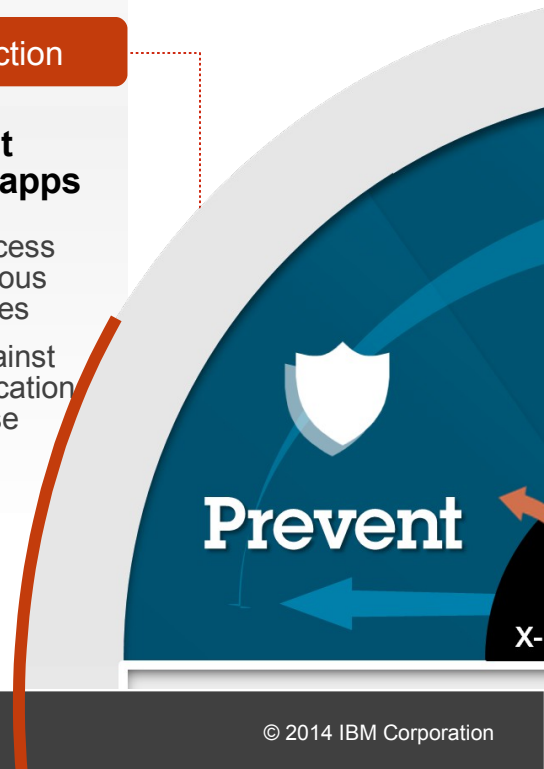
Trusteer Apex Malware Protection

On the Endpoint

On the Network

IBM Security Network Protection XGS

Exploit Disruption	Malware Quarantine	User Protection
Prevent malware installs • Verify the state of applications • Block exploit attempts used to deliver malware	**Prevent control channels** • Stop direct outbound malware communications • Protect against process hijacking	**Prevent credential loss** • Block keyloggers • Stop credential use on phishing sites • Limit reuse of passwords
Prevent mutated exploits • Verify the state of network protocols • Block unknown exploits with behavioral heuristics	**Prevent active beaconing** • Stop malware and botnet control traffic with real-time reputation and SSL inspection	**Prevent malicious apps** • Block access to malicious websites • Protect against web application misuse



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

Rapidly 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

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

IBM Emergency Response Services

Respond

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

Global Threat Intelligence

- Combines the renowned expertise of X-Force with Trusteer malware research
- Catalog of 70K+ vulnerabilities, 22B+ web pages, and data from 100M+ endpoints
- Intelligence databases dynamically updated on a minute-by-minute basis

Real-time sharing of Trusteer intelligence

Zero-day Research | Malware Analysis | Exploit Triage

IP/Domain Reputation | URL/Web Filtering | Web App Control

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

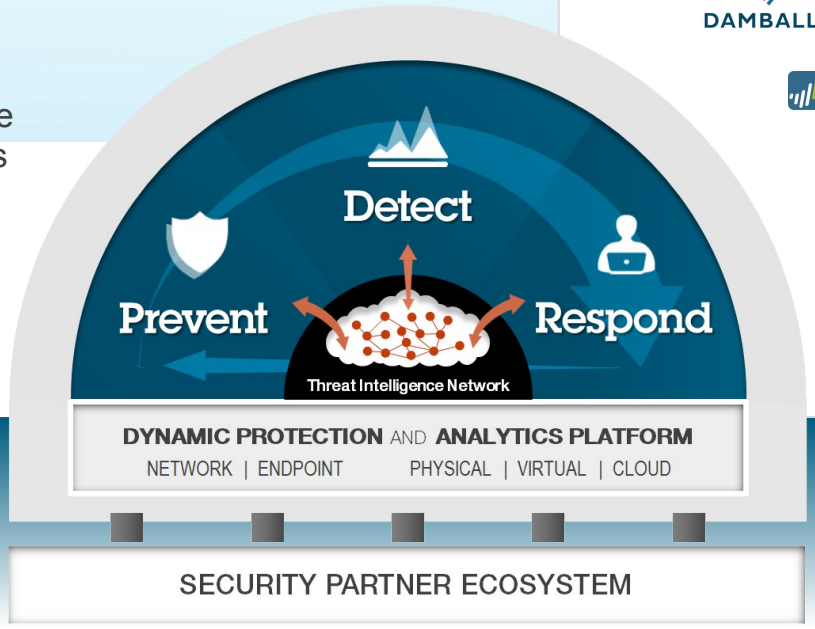
Security Partner Ecosystem Integrations

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

IBM Security Partner Ecosystem 90+ vendors and 400+ products



Planned Advanced Threat Protection Integrations:

TREND MICRO — *Trend Micro Deep Security*
IBM XGS Quarantine and Blocking

FireEye — *FireEye Web Malware Protection System*
IBM XGS Quarantine and Blocking

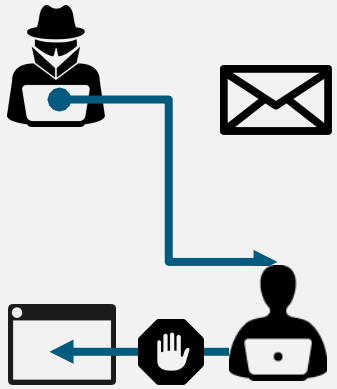
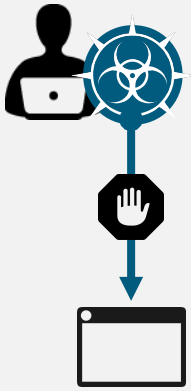
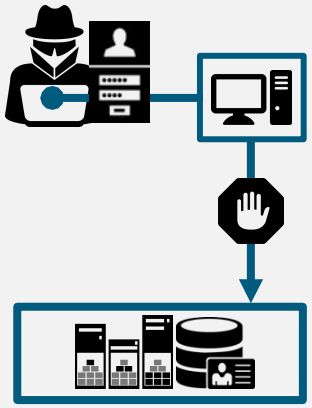
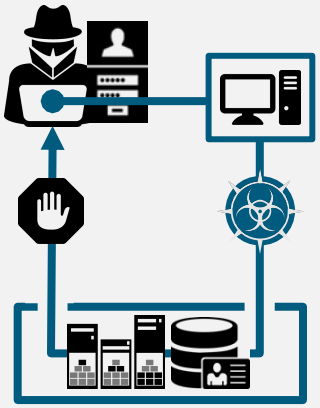
DAMBALLA — *Damballa Failsafe*
IBM XGS Quarantine and Blocking

paloalto NETWORKS — *Palo Alto Firewalls*
Trusteer Apex integration

Additional Example QRadar Partners:

CISCO, websense, QUALYS, BLUE COAT, proofpoint, JUNIPER NETWORKS

Examples of breaking the attack chain through integrated intelligence

Break-in	Latch-on	Expand	Gather	Exfiltrate
Attacker sends a phishing email to an unsuspecting user, a link is clicked, an exploit is sent to the browser	Remote employee executes untrusted code from an attachment, which tries to download and install malware	Attacker finds a way in and tries to search for usernames and passwords to access critical systems	Internal system attempts to access and export data from critical resources	Malware made its way through an unprotected system and attempts to quietly siphon out data
				
XGS prevents the remote exploit from reaching the vulnerable browser and alerts QRadar to the intrusion attempt	**Apex prevents malware from installing, shares an event to QRadar through the cloud, and enforces an XGS quarantine rule**	**XGS prevents the attempt to scan internal systems, while QRadar detects abnormal traffic patterns on the network**	**QRadar detects user logins and database activity revealing abnormal access to sensitive servers**	**QRadar detects the slow data transfer, sends a quarantine rule to XGS, while Incident Forensics investigates attack activity**

IBM is uniquely positioned to offer integrated protection

1 Smarter Prevention

Planned **Trusteer Apex Endpoint Malware Protection**

NEW *Java Lockdown Protection - granular control of untrusted code, cloud-based file inspection, and QRadar integration*

IBM Security Network Protection XGS

NEW *Advanced Threat Quarantine integration from QRadar and third-party products, inclusion of Trusteer intelligence into XGS*

2 Security Intelligence

IBM Security QRadar Security Intelligence

NEW *Data Node appliance, new flow and event APIs, and QRadar Vulnerability Manager scanning improvements*

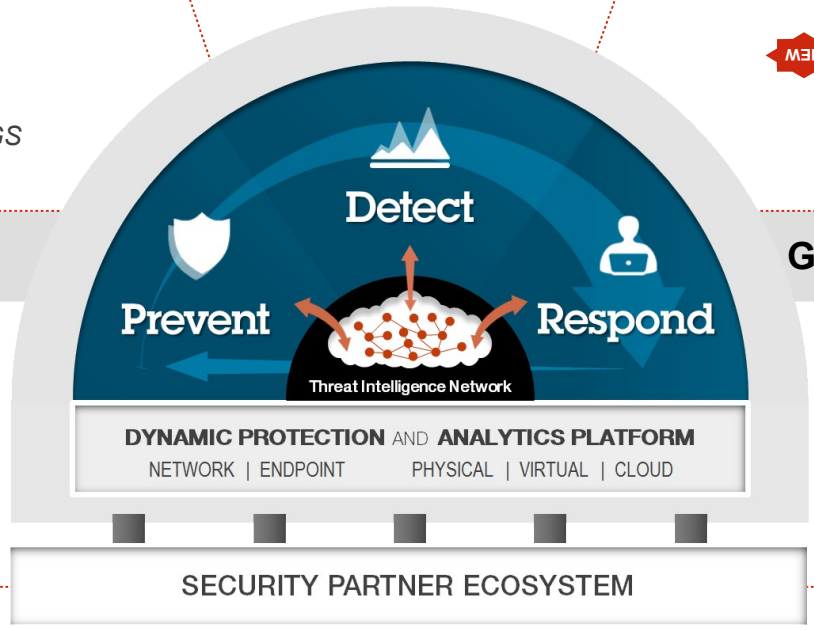
Continuous Response 3

IBM Security QRadar Incident Forensics

NEW *Integrated forensics module with full packet search and visual reconstruction of threat actor relationships*

IBM Emergency Response Services

NEW *Increased global coverage and expertise related to malware analysis and forensics*



5 Open Integrations

Ready for IBM Security Intelligence Ecosystem

NEW *New functionality from partners including FireEye, TrendMicro, Damballa and other protection vendors*

Global Threat Intelligence 4

IBM X-Force Threat Intelligence

NEW *New virtual real-time sharing of Trusteer threat intelligence from 100M+ endpoints with X-Force*

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