4 Undeniable Truths of Advanced Threat Protection

Patrick Vandenberg
Program Director
IBM Security

October 22, 2014
We are in an era of continuous breaches
Attackers are relentless, victims are targeted, and the damage toll is rising

2011
Operational Sophistication
IBM X-Force® declared Year of the Security Breach

2012
Near Daily Leaks of Sensitive Data
40% increase in reported data breaches and incidents

2013
Relentless Use of Multiple Methods
500,000,000+ records were leaked, while the future shows no sign of change

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

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

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

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

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

...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.
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.

<table>
<thead>
<tr>
<th>On the Endpoint</th>
<th>Prevent malware installs</th>
<th>Prevent control channels</th>
<th>Prevent credential loss</th>
</tr>
</thead>
</table>
| Exploit Disruption | • Verify the state of applications  
• Block exploit attempts used to deliver malware  
| Prevent mutated exploits | • Stop direct outbound malware communications  
• Protect against process hijacking  
| Malware Quarantine | • Block keyloggers  
• Stop credential use on phishing sites  
• Limit reuse of passwords  
| User Protection | • Stop malware and botnet control traffic with real-time reputation and SSL inspection  
| Prevent active beaconing | Prevent malicious apps | • Block access to malicious websites  
• Protect against web application misuse  
| Prevent malicious apps | • Stop direct outbound malware communications  
• Protect against process hijacking  

On the Network:

- IBM Security Network Protection XGS

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

**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

**IBM Security QRadar**

**Security Intelligence Platform**

- Pre-Attack Analytics
- Real-time Attack Analytics

**IBM Security QRadar Vulnerability Manager**

**IBM Security QRadar SIEM**
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

**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 Security QRadar Incident Forensics**

**IBM Emergency Response Services**
Leverage threat intelligence with product integrations that draw upon human and machine-generated information

Global Threat Intelligence

- Combines the renowned expertise of X-Force + Trusteer malware research
- Catalog of 80K+ vulnerabilities, 17B+ web pages, and data from 100M+ endpoints
- Intelligence databases dynamically updated on a minute-by-minute basis
Share, analyze, and act upon information gathered from an ecosystem of third-party products

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

New Advanced Threat Protection Integrations:
- SSL Traffic Decryption for QRadar Incident Forensics investigations
- Integration with IBM XGS to block new threats and QRadar for centralized response

Additional Sample of QRadar Partners:
IBM is uniquely positioned to offer integrated protection

<table>
<thead>
<tr>
<th>Smarter Prevention</th>
<th>Security Intelligence</th>
<th>Continuous Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusteer Apex Endpoint Malware Protection</td>
<td>IBM Security QRadar Security Intelligence</td>
<td>IBM Security QRadar Incident Forensics</td>
</tr>
<tr>
<td><strong>NEW</strong> Threat Flow Visualization and Incident Analysis [Cloud-based File Inspection Feedback]</td>
<td><strong>NEW</strong> Master Console appliance for MSSPs, Greater QFlow collection and data burst handling</td>
<td><strong>NEW</strong> In-line packet compression, data import facility and integrated SSL traffic decryption with A10</td>
</tr>
<tr>
<td>IBM Security Network Protection XGS</td>
<td>Threat Monitoring and Intelligence Services</td>
<td>IBM Emergency Response Services</td>
</tr>
<tr>
<td><strong>NEW</strong> IBM XGS7100 with increased 20Gbps+ throughput for high-performance datacenters</td>
<td>Managed SIEM enhancements, cyber threat intelligence</td>
<td><strong>NEW</strong> Increased global coverage and expertise &amp; Available as Subscription via online</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Open Integrations</th>
<th>Global Threat Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready for IBM Security Intelligence Ecosystem</td>
<td>IBM X-Force Threat Intelligence</td>
</tr>
<tr>
<td><strong>NEW</strong> New integration with A10 Networks to decrypt SSL Traffic for incident forensics</td>
<td><strong>NEW</strong> New virtual real-time sharing of Trusteer threat intelligence from 100M+ endpoints with X-Force</td>
</tr>
</tbody>
</table>
Find us at IBM Booth #607…

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

© Copyright IBM Corporation 2014. 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.