

## FACT SHEET

### IBM Threat Protection System

The IBM Threat Protection System includes an end-to-end architecture to help organizations continuously prevent, detect and respond to ongoing and sophisticated cyber attacks, and in some cases, before they do damage. The offering uses technology from the company's significant R&D investments from its Security Systems Division, including the recent acquisitions of Q1 Labs and Trusteer.

IBM's Threat Protection System includes:

- **IBM Security Network Protection and Trusteer Apex software:** IBM Security Network Protection and Trusteer Apex endpoint malware protection work together to help stop threats with behavioral-based prevention on both the network and "endpoint" — the systems where end users access a company's data, products, services, etc. IBM Security Network Protection's "Advanced Threat Quarantine" capability enables clients to lock down the enterprise network based on threat indicators shared directly from IBM and third party solutions.
- **IBM Security QRadar:** Includes new appliances, optimizations, and APIs enabling organizations to handle more data and speed up analytics across security events, logs, network flows, configuration information, identity data, vulnerabilities and more. IBM Security QRadar Incident Forensics enables security teams to quickly and easily retrace the step-by-step occurrences of a security incident—often in hours instead of days. This fully integrated solution extends the QRadar Security Intelligence Platform to help customers quickly verify that an incident occurred, determine the severity, reconstruct and replay the event, and take corrective and preventive action.
- **Expanded Global Emergency Response:** With greater delivery capacity and improved service delivery methodology, IBM has significantly increased global coverage and expertise related to emergency incident response, malware analysis and forensics.
- **Increased IBM X-Force Threat Intelligence:** X-Force provides subscribing IBM security products and services with the latest threat intelligence on active global attacks and insights on emerging vulnerabilities. As part of the IBM Threat Prediction System, IBM Security QRadar and IBM Security Network Protection customers can now take advantage of X-Force integration with Trusteer intelligence on malware and cybercrime campaigns gathered from an installed base of 100+ million endpoints.
- **New Open Integrations to Increase Intelligence Sharing and Collaboration:** IBM has also expanded its partner ecosystem to help customers share, analyze, and act upon information gathered from an ecosystem of third party products. As part of this announcement, IBM is working with partners, to integrate actionable threat indicators directly from their products with IBM Network Protection XGS to provide seamless integration and automated blocking of attacks.

- more -

## **Key Industry Statistics**

- While small in number — IP represents approximately 2 percent of an organization's data — it accounts for an estimated 70 percent of the value of a publicly traded corporation and subsequently are extremely valuable to hostile forces -- whether company insiders or sophisticated attackers.
- It can take days or more to discover in more than 95 percent of cases, and weeks or more to contain in more than 90 percent of cases, a lag that can have a catastrophic impact on a business.
- According to an IBM-commissioned Survey from the Ponemon Institute, the average total cost of a data breach has increased 15 percent in the last year to \$3.5 million
- According to a second IBM-commissioned Ponemon study focused on the Top Cost of Advanced Persistent Threat (APT) attacks, most data breaches are the result of advanced persistent threats, which are costing organizations and estimated \$9.2 million average loss in brand equity (customer attrition, contractual violations, regulatory action and lawsuits, etc...).
- According to X-Force – IBM's global team of security analysts – more than half a billion records of personally identifiable information were compromised last year.

## **IBM Security Sparklers**

- IBM conducts security research and development at 29 locations worldwide and manages security for thousands of customers at 10 Security Operations Centers.
- IBM has 3,000+ security related patents and more than 1,200 software developers, 2,000 security consultants, and 6,000 security researchers, developers and subject matter experts.
- IBM X-Force research has analyzed 20 billion web pages and images and built a database of 40 million spam and phishing attacks and 80,000+ vulnerabilities.
- IBM Managed Security Services (MSS) manages more than 15 billion security events per day across 133 countries, thousands of clients and more than 20,000 devices.
- 200 universities from around the globe are now partnering with IBM, focusing on cyber security.
- With nearly 50 years of security and development experience, IBM also has the world's largest security services practice with more than 3,500 skilled security services professionals who have a unique handle on the broad threat landscape.

## **About IBM Security**

IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. For more information on IBM security, please visit: [www.ibm.com/security](http://www.ibm.com/security).

## **Additional Assets:**

- [Ponemon Cost of a Data Breach 2014 Report](#)
- [Ponemon Cost of a Data Breach 2014 Press Release](#)
- [IBM Advances Fight against Cyber Threats with Comprehensive, New Threat Protection System and Critical Data Protection Services](#)