

BusinessConnect
A New Era of Smart
May 14, 2014

Security Intelligence

A New Era of Security

for a New Era of Computing



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.


A New Security Reality Is Here

61% of organizations say **Data theft and cybercrime** are the greatest threats to their reputation

2012 IBM Global Reputational Risk & IT Study


 **70%** of security exec's are concerned about **cloud and mobile security**

2013 IBM CISO Survey

 **83%** of enterprises have difficulty finding the security skills they need

2012 ESG Research

Mobile malware grew

614%  in one year

from March 2012 to March 2013

2013 Juniper Mobile Threat Report

85  tools from **45**  vendors

IBM client example



Average U.S. breach cost

\$11M+

*2013 Cost of Cyber Crime Study
Ponemon Institute*

We are in an era of continuous breaches

Operational Sophistication

IBM X-Force® declared

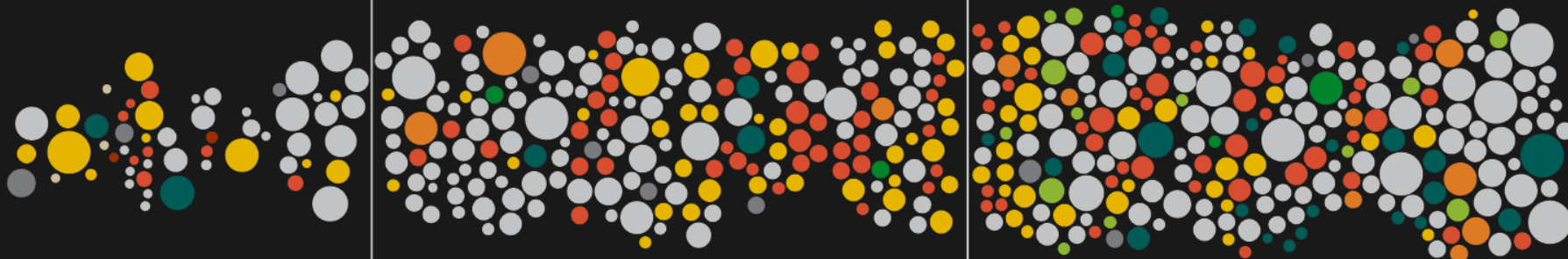
Year of the Security Breach

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



2011

2012

2013

Attack types



SQL injection



Spear phishing



DDoS



Third-party software



Physical access



Malware



XSS



Watering hole



Undisclosed

Why a New Approach

**Criminals will not relent
and every business
is a target**



**New technologies
create opportunities
to transform IT security**



**Security leaders
are more accountable
than ever before**



INTELLIGENCE

*Use insights
and analytics
to identify
outliers*

INNOVATION

*Use cloud
and mobile
for better
security*

INTEGRATION

*Develop an integrated
approach to
stay ahead
of the threat*

Strategic imperative #1

Use analytics and insights for smarter defense



Use intelligence and anomaly detection across every domain

Build an intelligence vault around your crown jewels

Prepare your response for the inevitable

Use Intelligence and Anomaly Detection Across Every Domain

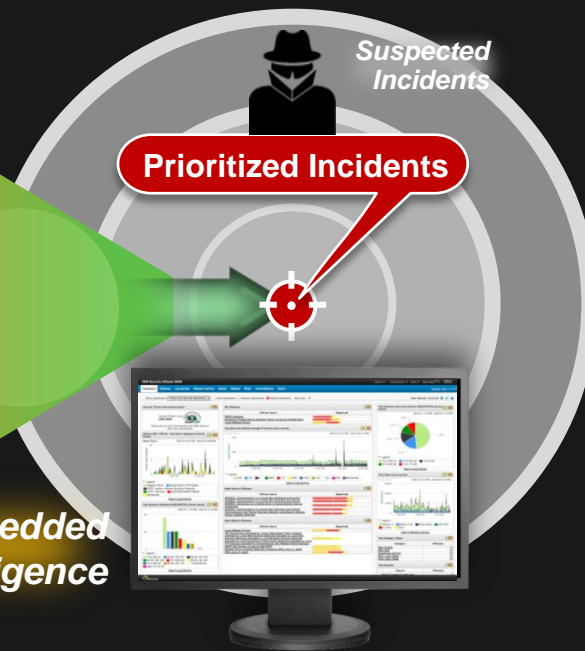
Extensive Data Sources

- 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



Gain Insights to Prioritize What Is Most Critical



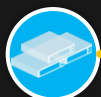
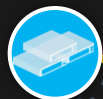
2 Billion logs and events per day



25 high priority offenses

QRadar Security Intelligence Platform

Reduce Blind Spots, Quickly Investigate Attacks



Incident Forensics

- Full packet capture
- Detailed incident meta-data / evidence
- Reconstruction of content and user activity



Network Security



Insider Threat Analysis



Fraud and Abuse



Evidence Gathering

Build a Vault Around Your Crown Jewels



Protect Your Most Critical Assets

QRadar Security Intelligence Platform



Monitoring / same-day de-provisioning for **100+ privileged users**

IBM Corporation

Privileged Identity Management

On over **1 million** customer endpoints zero instances of fraud reported

Banking company

Advanced Fraud Protection

Secured **2,000 critical databases** and **saved \$21M** in compliance costs

Global financial services company

Database Access and Monitoring

Managed, cloud, and professional services

Use Intelligent Defenses to Prepare for the Inevitable Attacks

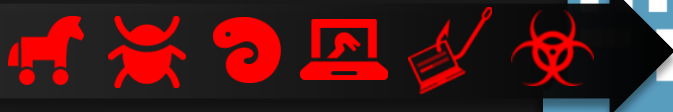
Use the cloud to identify bad activity



Prevent unknown and mutating threats



Discover anomalous activity and stop exfiltration



End-to-end Next Generation Threat Protection



Use the cloud to identify bad activity

Assess activity on **millions** of endpoints and Websites

IBM X-Force and Trusteer Research

Prevent anomalous activity and mutating threats

Stop **99%** of tested, publicly available attacks
2x more effective at stopping mutated attacks

IBM Security Network Protection

Discover anomalies and stop exfiltration

Reduce malware attacks from **500** to **0** in one month

Trusteer Apex

Strategic imperative #2

Use cloud and mobile to improve security



**Own the security
agenda
for innovation**

**Employ
innovation
to improve security**

**Embed
security
on day one**

Employ Cloud to Improve Security



Traditional Security

Manual
and static



Cloud-enhanced Security

Automated, customizable,
and elastic

Extending Enterprise Security to / from the Cloud

*Delivering
security
from the
cloud*

*Solutions
to protect
cloud
workloads*

Today		
<p>Fraud Prevention</p> <p>Millions of endpoints protected for the world's top financial institutions</p> <p>IBM Trusteer</p>	<p>Mobile Security</p> <p>Millions of cloud-managed devices for thousands of global customers</p> <p>IBM Fiberlink</p>	<p>Web Protection</p> <p>Thousands of servers providing DDoS protection in the cloud</p> <p>IBM + Akamai</p>
<p>Security Intelligence</p> <p>Analytics and real-time correlation to stop cloud threats</p> <p>IBM QRadar and Threat Monitoring</p>	<p>End-to-end Protection</p> <p>Controls for cloud users, data, apps and infrastructure</p> <p>IBM Security Systems</p>	<p>Skills and Expertise</p> <p>Services to design, deploy and manage cloud security</p> <p>IBM Security Services</p>

Build Security into Mobile from Day One



Device, Application, and Transaction Security

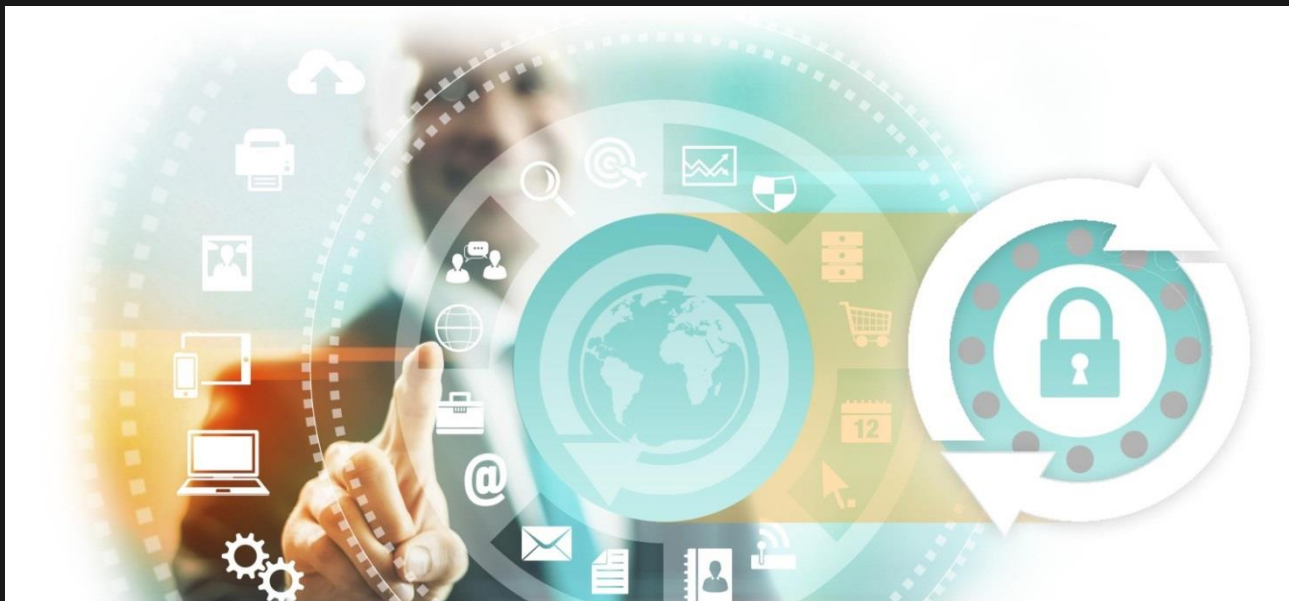


Discovered and enrolled **3,000 devices** in **under 5 minutes** each with ability to wipe the device if lost
Chemical company

Helping prevent user access to fraudulent websites for **thousands** of mobile customers
Large European bank

Strategic Imperative #3

Get help to develop an integrated approach

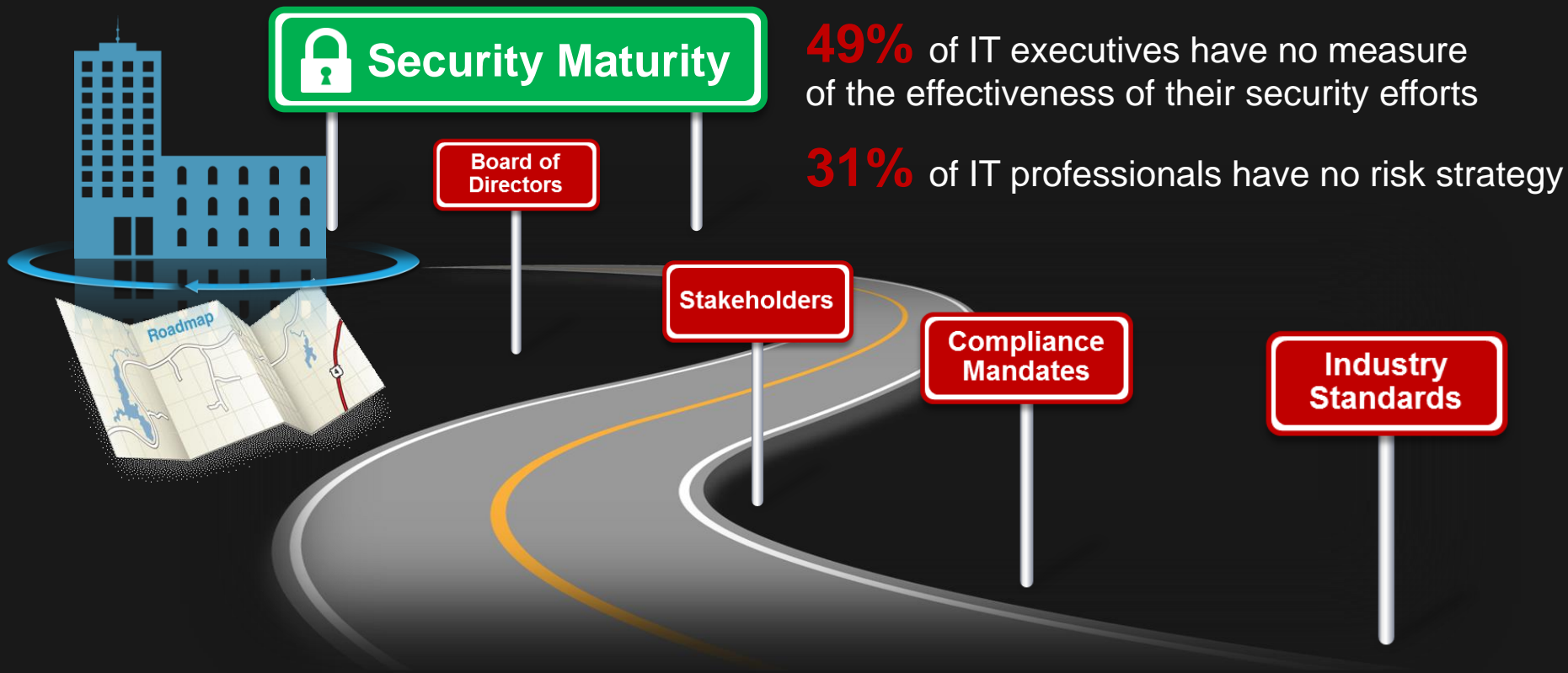


**Develop a
risk-aware
security strategy**

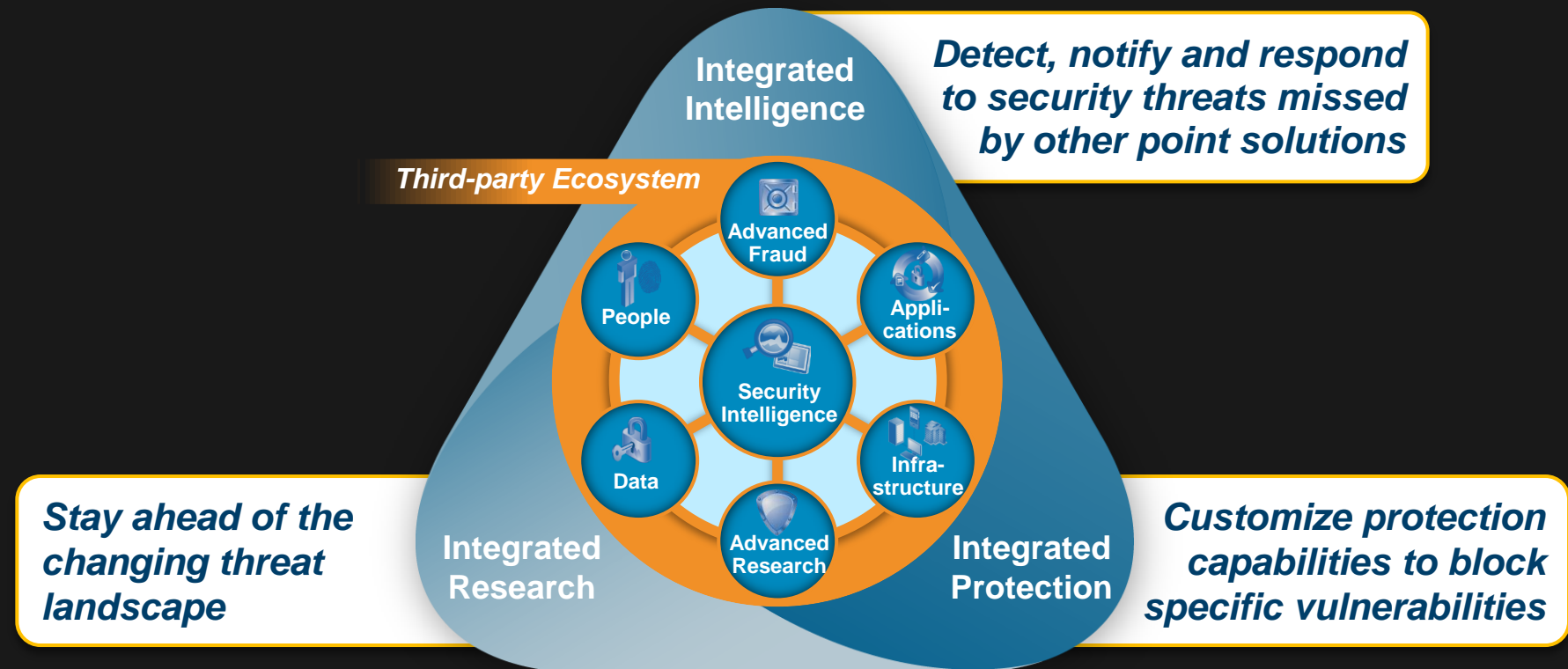
**Deploy a
systematic
approach**

**Harness the
knowledge
of professionals**

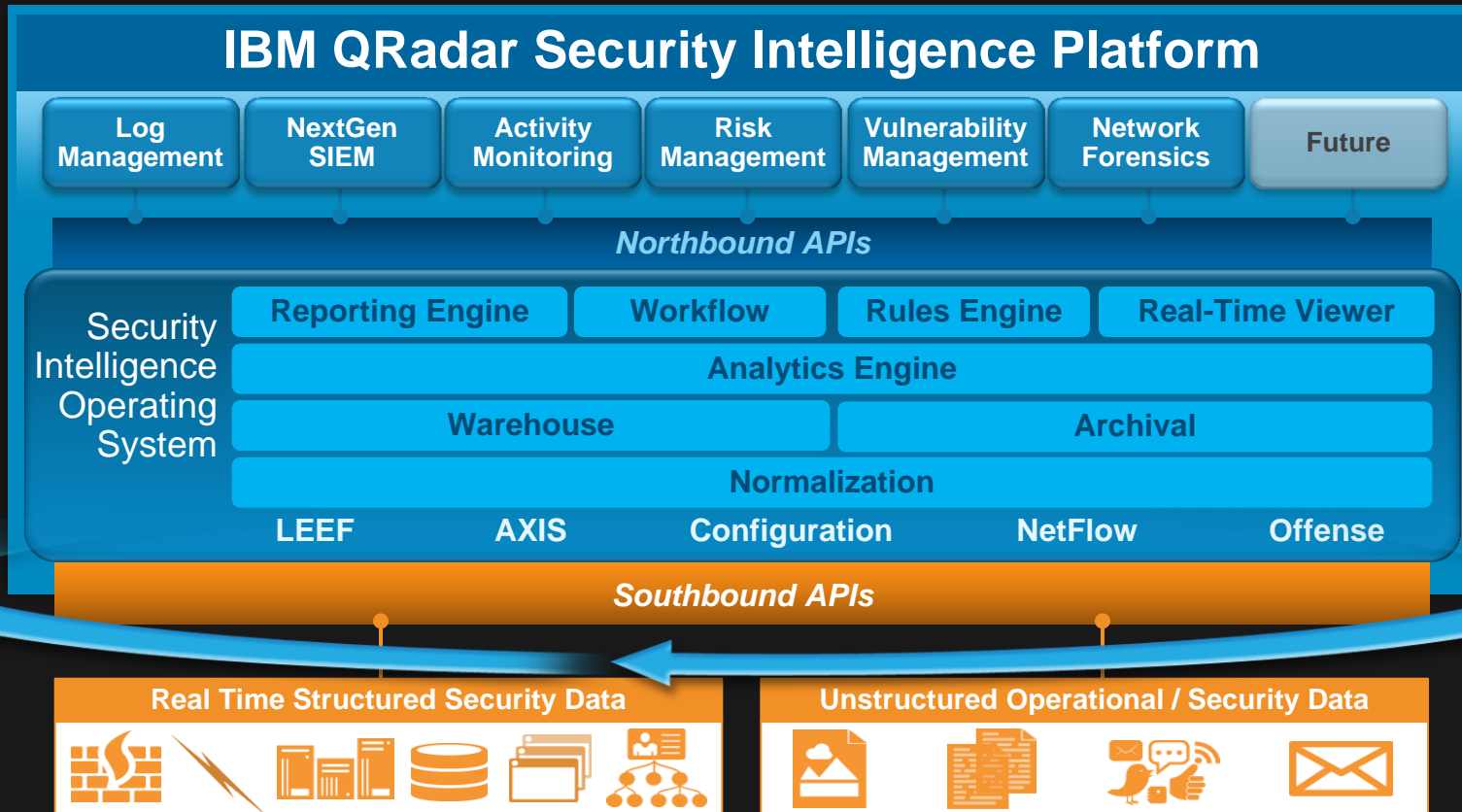
Develop a Risk-aware Security Strategy



Deploy a Systematic Approach with Integrated Capabilities

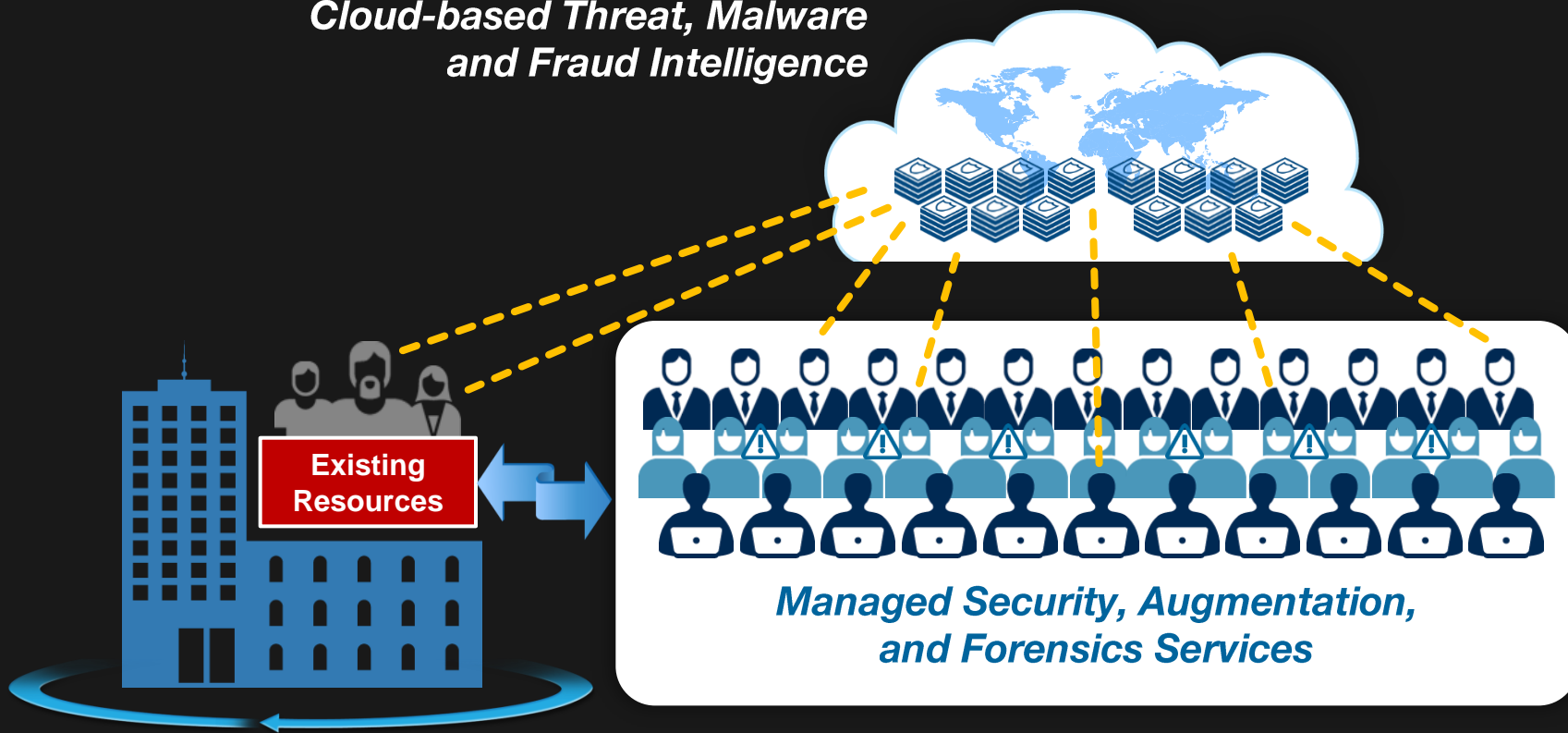


The Advantage of an Extensible Security Platform



Harness the Knowledge of Professionals

*Cloud-based Threat, Malware
and Fraud Intelligence*



IBM Provides Unmatched Global Coverage and Security Awareness



6,000+

security specialists

10

security operations centers

133

monitored countries

18B

events per day

Real-world Examples

Better secure data and protect privacy



A large Canadian pharmaceutical company improves its ability to protect against internal and external threats with an IBM Information Security Assessment

Build a risk-aware culture



An Austrian bank conglomerate establishes a consistent security policy with IBM Security Services

Security-rich services by design



A bank in Kuwait gains a better view of its security posture and network vulnerabilities by conducting real-world security testing

Manage third-party security compliance



A US retailer identifies gaps to achieve Payment Card Industry (PCI) compliance and maintains operations

Control network access and assure resilience



A Danish dairy company protects users and its infrastructure from malicious content and limits administration

Defend mobile and social workplace



A leading manufacturer in India identifies potential security threats, strengthens its security levels and improves customer confidence

Address new complexity of cloud and virtualization



An urban services organization in Portugal improves employee productivity through e-mail filtering and cloud / managed security services

How IBM Can Help

Use insights and analytics to identify outliers

Security intelligence

- IBM Security Intelligence Solutions
- IBM Threat Management and Monitoring Services

Crown jewels protection

- IBM “Crown Jewels” Protection Program
- IBM Identity and Access Management
- IBM Application and Data Security

Next Gen defense

- IBM Emergency Response Services
- IBM Security Network Protection
- IBM Trusteer Cybercrime Solutions

Use cloud and mobile for better security

Cloud security

- IBM Cloud Security Solutions

Mobile security

- IBM MobileFirst Security Solutions
- IBM Trusteer Mobile Fraud Solutions
- IBM Fiberlink Mobile Security Solutions

Security-as-a-Service

- IBM Cloud-based Security Services
- IBM Web Presence Protection Service
- IBM Trusteer Advanced Fraud Protection

Develop an integrated approach

Security strategy

- IBM Security Maturity Benchmarking
- IBM Security Risk Assessment

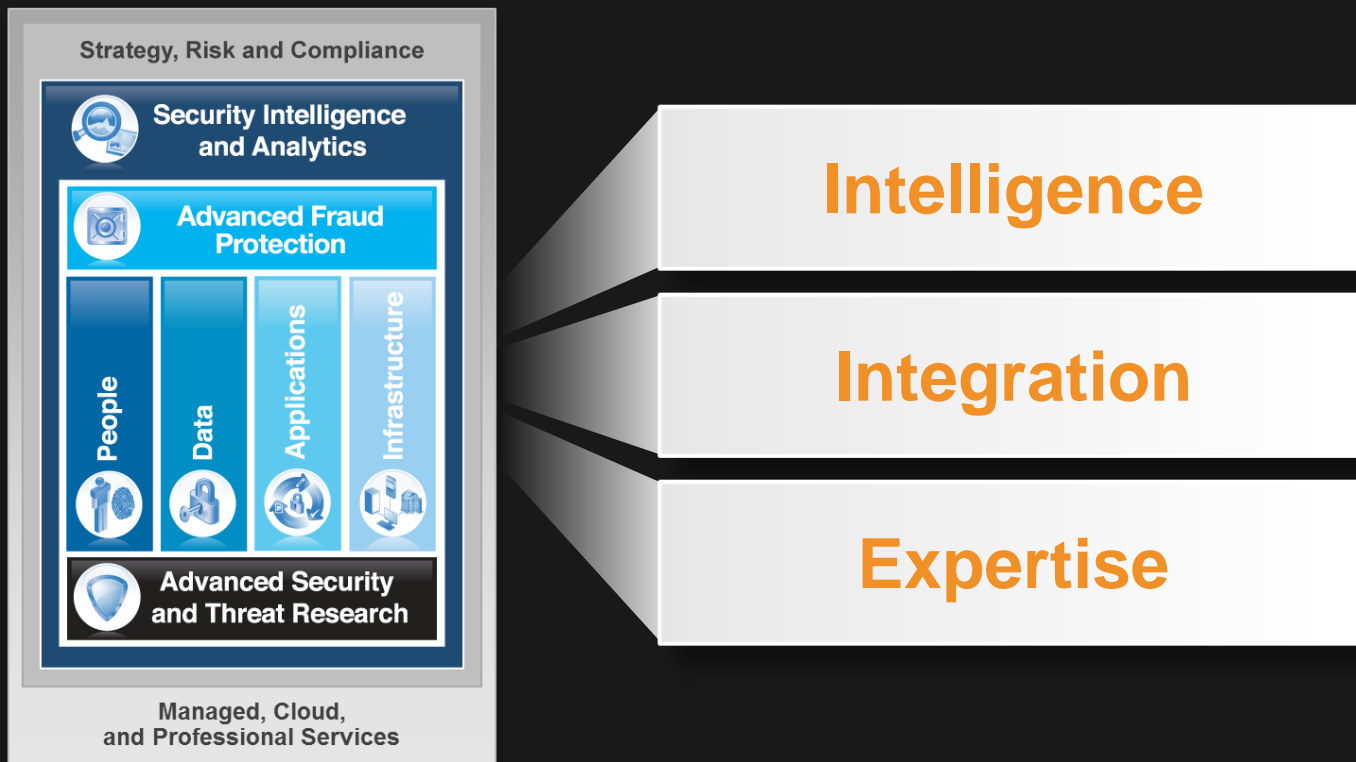
Integrated operations

- IBM Security Framework of Solutions
- IBM Security Operations Optimization

Expertise

- IBM Security Consulting Services
- IBM X-Force and Trusteer Research

IBM Security Framework



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.

Top 4 mitigation strategies from Australia Department of Defence



Use application whitelisting of permitted / trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers

Patch applications, e.g., Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch / mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications

Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing

Patch operating system vulnerabilities. Patch / mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP



INTELLIGENCE

*Use insights
and analytics
to identify
outliers*



INNOVATION

*Use cloud
and mobile
for better
security*

INTEGRATION

*Develop an integrated
approach to
stay ahead
of the threat*

End-to-end Next Generation Threat Protection



Use the cloud to identify bad activity

Assess activity on **millions** of endpoints and Websites

IBM X-Force and Trusteer Research

Prevent anomalous activity and mutating threats

Stop **99%** of tested, publicly available attacks
2x more effective at stopping mutated attacks

IBM Security Network Protection

Discover anomalies and stop exfiltration

Reduced malware attacks from **500** to **0** in just one month

Trusteer Apex

