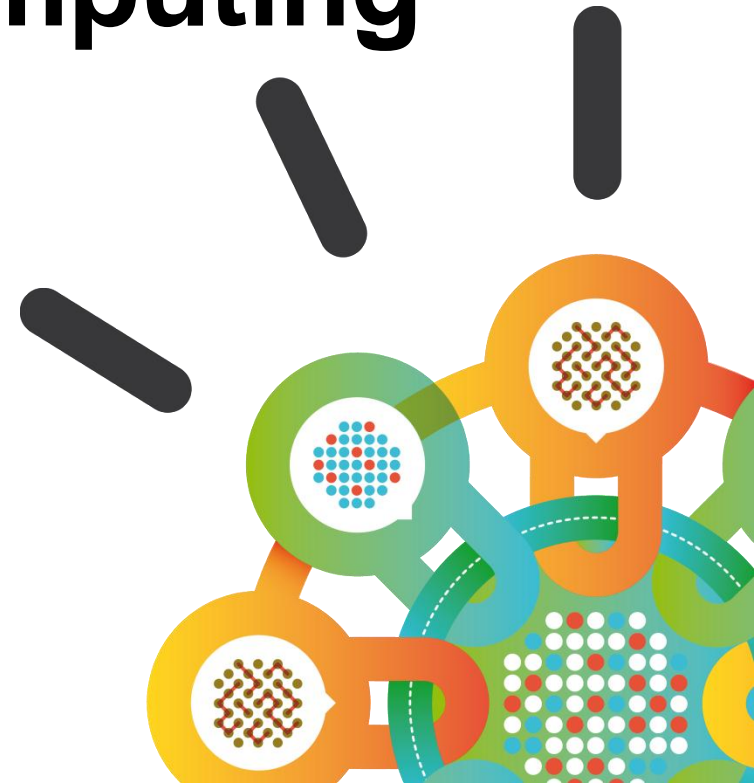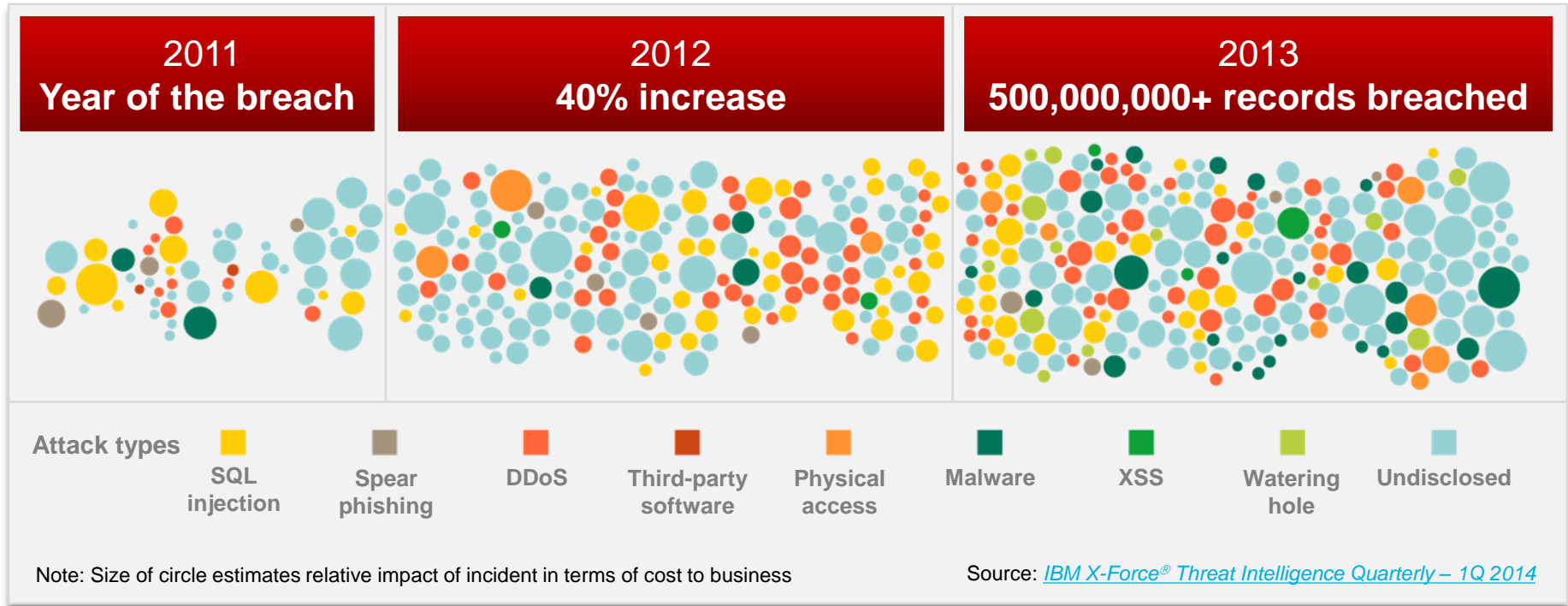Security Intelligence.
Think Integrated.

A New Era of Security for a New Era of Computing

Marc van Zadelhoff

VP, Strategy, Marketing and Product Management

IBM Security Systems

October, 2014

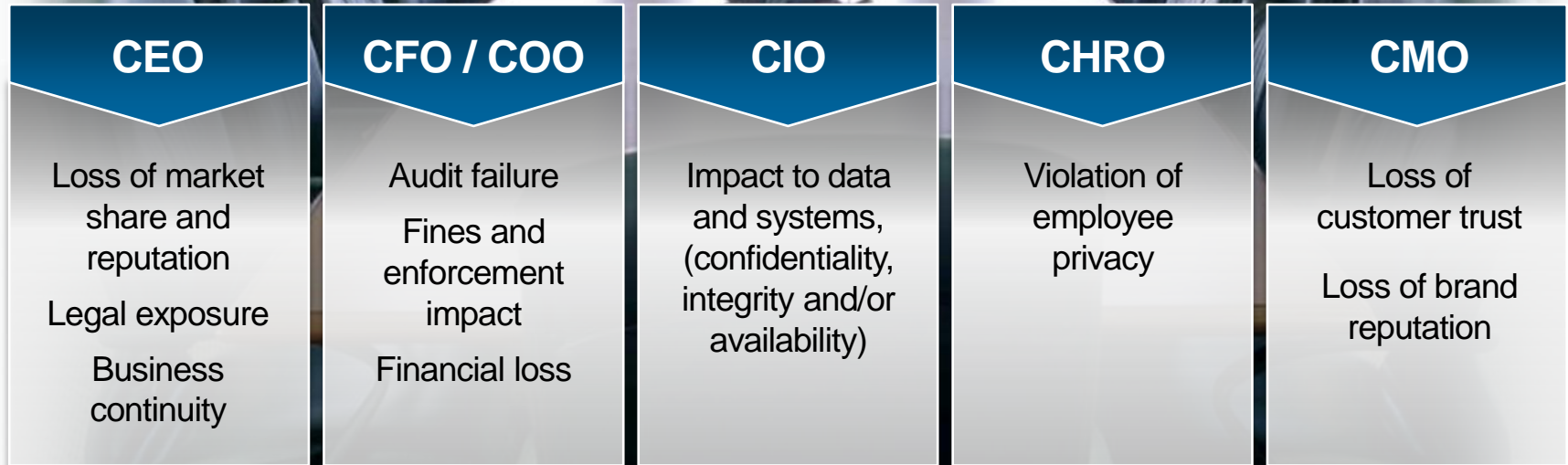# Sophisticated attackers break through safeguards every day

2011 **Year of the breach**	2012 **40% increase**	2013 **500,000,000+ records breached**

Attack types

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

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

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

61% of organizations say **data theft and cybercrime** are their greatest threats

2012 IBM Global Reputational Risk & IT Study
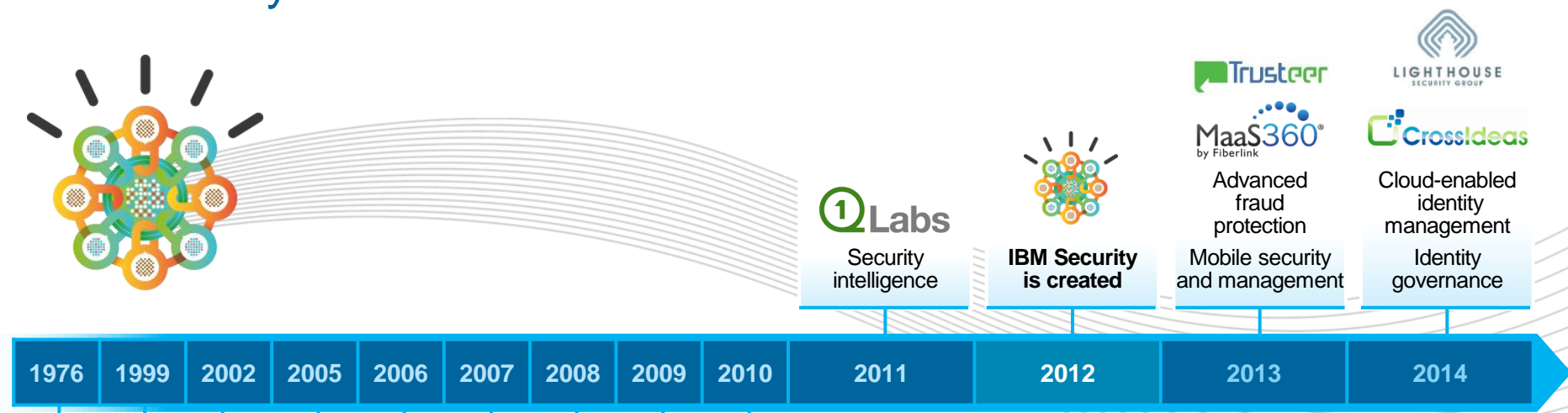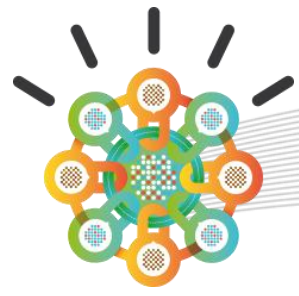
$3.5M+ average cost of a **data breach**

2014 Cost of Data Breach, Ponemon Institute

Security leaders are more accountable than ever before

CEO	CFO / COO	CIO	CHRO	CMO
Loss of market share and reputation

Legal exposure

Business continuity | Audit failure

Fines and enforcement impact

Financial loss | Impact to data and systems, (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: IBM C-Suite Study

IBM

IBM Security timeline

| 1976 | 1999 | 2002 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |

Security intelligence — ①Labs (2011)

IBM Security is created (2012)

Advanced fraud protection / **Mobile security and management** — Trusteer, MaaS360 by Fiberlink (2013)

Cloud-enabled identity management / **Identity governance** — LIGHTHOUSE SECURITY GROUP, CrossIdeas (2014)

Mainframe and server security (1976)

Identity management / Directory integration — access360, METAMERGE (1999/2002)

Security services and network security — INTERNET SECURITY SYSTEMS (2006)

Enterprise single-sign-on — ENCENTUATE (2008)

Endpoint management and security / Information and analytics management — BIGFIX, NISC National Interest Security Company (2010)

Access management — DASCOM

Service oriented architecture (SOA) management and security — DATAPOWER

Application security / Risk management / Data management — watchfire, consul, princeton softech

Database monitoring and protection / Application security — Guardium, OUNCE LABS

IBM Security Investment

- 6,000+ IBM Security experts worldwide
- 1,700+ IBM Security patents
- 4,000+ IBM Managed Security Services clients worldwide
- 25 IBM Security labs worldwide

4

IBM Security Portfolio

Consulting and Managed Services			Integrated Security Technologies			
Security Intelligence and Operations			Security Intelligence and Analytics			
Strategy, Risk and Compliance	Cloud and Managed Services		Advanced Fraud Protection			
Identity and Access Management Services	Data and Application Security Services	Cybersecurity Assessment and Response	Identity and Access Management	Data Security	Application Security	Infrastructure and Threat Protection
Advanced Threat and Security Research						

Key Security Trends

Advanced Threats

Cloud Adoption

Mobile Concerns

Compliance Mandates

Skills Shortage

IBM Security today

Top 3 enterprise security software vendor in total revenue

13 industry analyst reports rank IBM Security as a **LEADER**

133 countries where IBM delivers managed security services

10K$^+$ clients protected *including…*

24 of the top 33 banks in Japan, North America, and Australia

Top Customer Conversations

1 **Security strategy**

2 **Stopping attackers**

3 **Crown jewels**

4 **Cloud and mobile**

1. Yesterday's security does not work

83% of enterprises have difficulty finding **security skills**

2012 ESG Research

49% of IT executives have **no measure of security effectiveness**

2012 Forrester Research Study

31% of IT professionals have **no risk strategy**

2013 Global Reputational Risk & IT Study, IBM

8

1 Optimize your security program

Risk-Aware Culture & Strategy

End-to-End Security Intelligence

Intelligent Threat Protection & Response

Assess and transform your security maturity

Benchmark your security maturity versus peers and define a roadmap for the future

- IBM Security Essentials and Maturity Consulting
- IBM Security Strategy and Planning Services

Build a next generation security operations capability

Treat security as a path to reduce risk and grow your business

- IBM Security Intelligence and Operations Consulting
- IBM Managed Security Services
- IBM Security Portfolio of Solutions

Get help from the experts

Engage professionals to hunt the attackers, deploy solutions or help run operations

- IBM Security Consulting and Systems Integration
- IBM Managed Security Services
- IBM X-Force and Trusteer Research

A financial services firm teams with IBM to build its first SOC

Optimize Your Security Investments

Identified and blocked

650+

suspicious incidents
in the first 6 months
of SOC operations
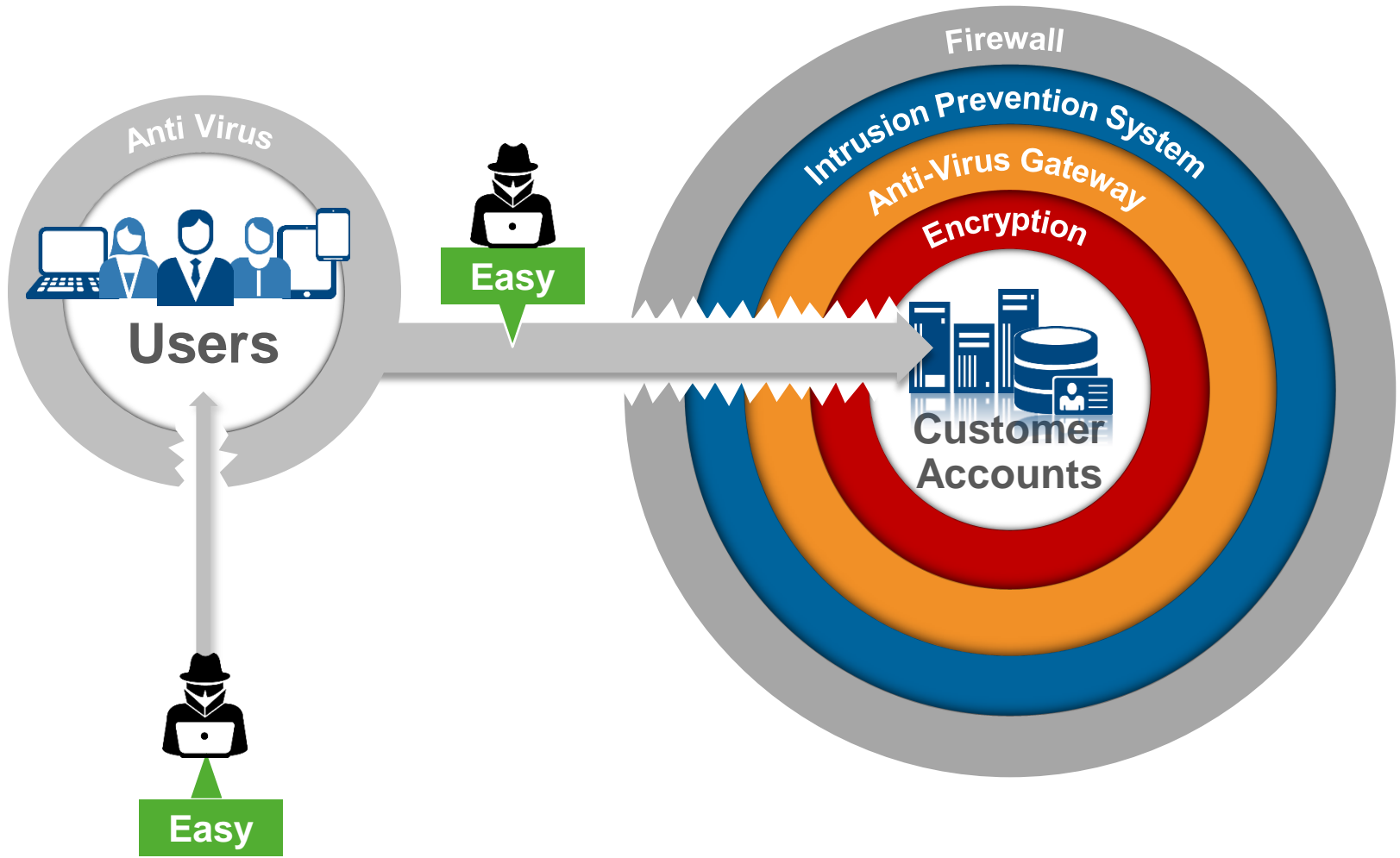
Business Challenge

- The bank did not have the security skills and resources to build its first SOC within the aggressive milestones set by their Board

- Wanted global protection for 16,000,000 accounts across 44 countries

IBM Security Solution benefits

- Provides automated, real-time advanced analytics to evaluate 13M+ events per day from 400K+ assets and 28K+ active log sources

- Provides 24x7 SOC management and incident response support at ~$2M lower cost than in-house management

Firewall

Intrusion Prevention System

Anti-Virus Gateway

Encryption

Anti Virus

Users

Easy

Easy

Customer
Accounts

2 Stop advanced threats

Detect advanced threats with security intelligence

Gain visibility and respond to breaches faster with big data analytics

- IBM QRadar Security Intelligence Platform
- IBM Managed SIEM and CyberThreat Intelligence
- Emergency Response Services

Protect against fraud and targeted attacks

Stop sophisticated threats in real-time with next-generation defenses

- IBM Threat Protection System
- IBM Trusteer Cybercrime Solutions
- IBM Managed Security Services

Deploy integrated security

Reduce operating costs and complexity with integrated controls and managed services

- IBM Security Portfolio of Solutions
- IBM Managed Security Services
- IBM X-Force® Research and Dynamic Threat Intelligence

An international energy company identifies critical events to investigate

Stop Advanced Threats with Security Intelligence

An international energy firm analyzes

2 billion

events per day to find

20 – 25

potential offenses to investigate

Business Challenge

- Reducing huge number of events to find the ones that need to be investigated
- Automating the process of analyzing security data

IBM Security Solution Benefits

- Combined analysis of historical data with real-time alerts to gain a 'big picture' view and uncover patterns of unusual activity humans miss
- Immediately block suspected traffic

3. Criminals want your valuable data

94% of breaches involve database servers

85% of organizations were unaware of the compromise for weeks to months
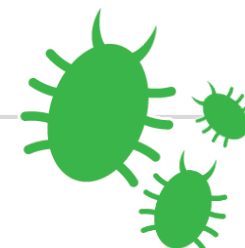
$188 Average cost of a data breach

$5.4M Per record cost of a data breach

2012 Verizon Data Breach Investigation Report   InfoSec, "Mobile Malware Infects Millions; LTE Spurs Growth," January 2014

IBM

③ Protect critical assets

Use context-aware and role-based controls to prevent unauthorized access

Validate "who is who" across the enterprise and the cloud, help defend against unauthorized access

- IBM Identity and Access Manager
- IBM Privileged Identity Manager
- IBM Cloud Identity Services

Identify and protect your "crown jewels"

Discover and classify critical data assets; monitor who is accessing that data and from where

- IBM Critical Data Protection Program
- IBM InfoSphere Guardium®
- IBM Key Lifecycle Manager

Manage application security risk

Discover and classify applications, help identify and remediate vulnerabilities, address security from day one

- IBM AppScan®
- IBM AppScan® for Mobile
- IBM Secure Engineering and Application Security Assessment

A leading provider of information technology, consulting, and business process outsourcing services safeguards privileged IDs

Protect Against Unauthorized Access

IBM Security
Privileged Identity Manager for

500

privileged administrator users

Business Challenge

- Increased security risks resulting from limited privileged activity monitoring
- Exposure to insider threat due to enterprise-wide sharing of privileged IDs
- Compliance issues due to poor privileged user management and lack of audit trail for privileged user access

IBM Security Solution Benefits

- Streamlined and automated privileged user management
- Audit trail and monitoring of privileged access to all critical systems
- Safe management of shared privileged IDs and their passwords
- Full support of periodic privileged access recertification for audit and compliance purposes
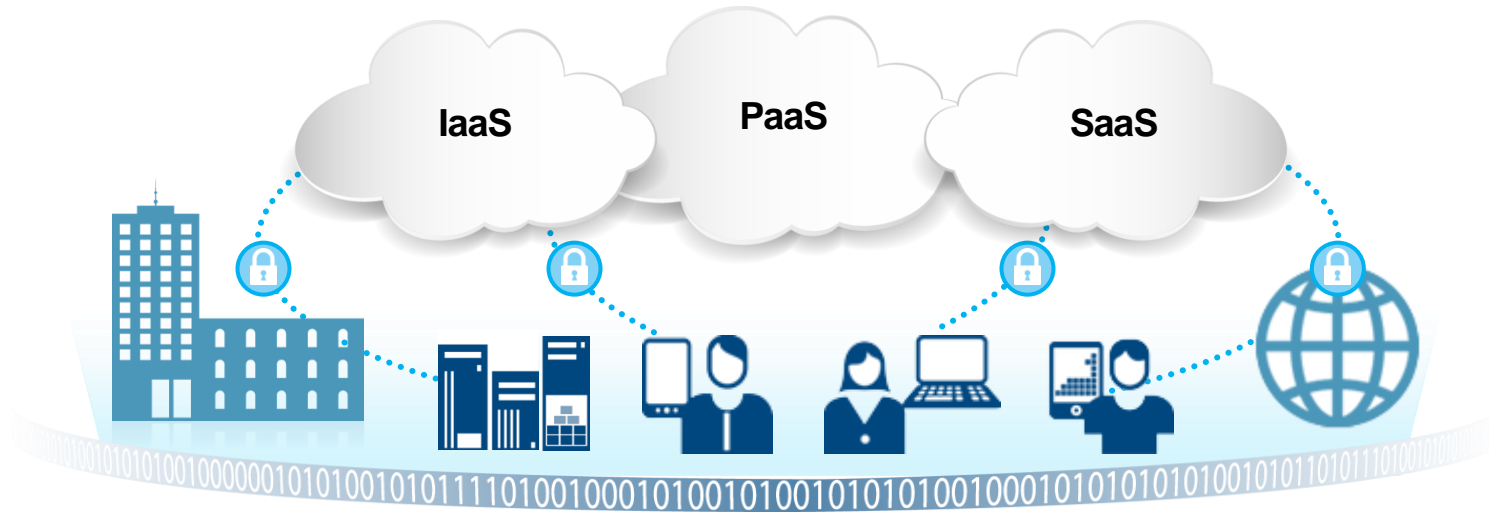
4. Cloud and mobile bring new risks

SECURITY
#1 inhibitor
with Cloud Computing

70%
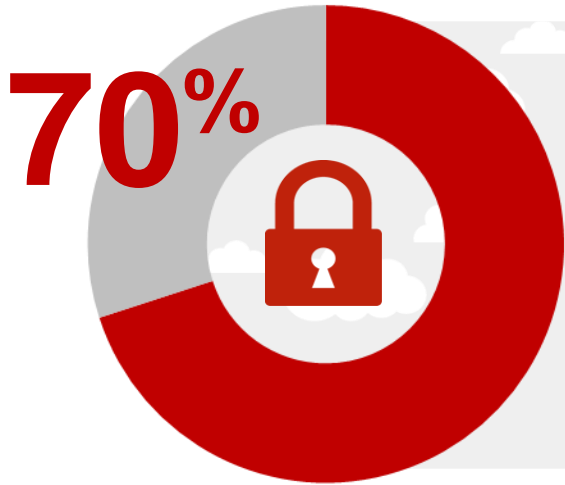
Top 5
security concerns
with Cloud Computing

Concern	
Data Security	41%
Access and Control	35%
Auditing and Compliance	32%
Control of Data	26%
Security Models / Toolsets	18%

IDG Enterprise, 2013; 451 Research, Cloud Computing - Wave 6, 2014
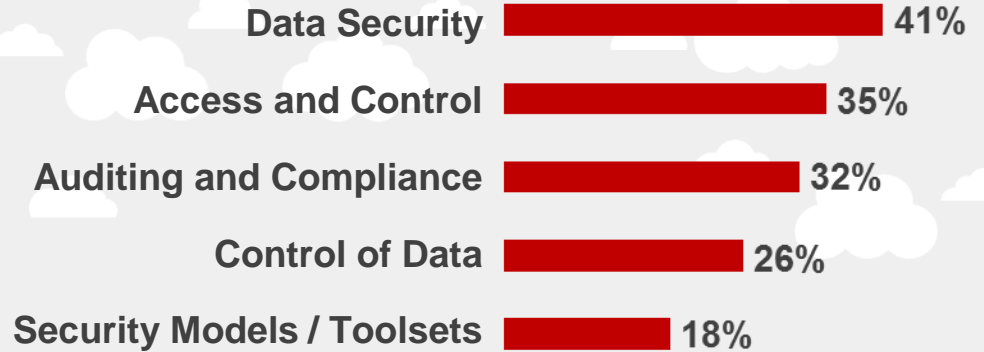
4 Safeguard cloud and mobile

IaaS   PaaS   SaaS

Maintain cloud visibility and control

Harden workloads and monitor attack activity while supporting compliance in the cloud

- IBM Security Cloud Solutions
- IBM Managed SIEM

Help protect the mobile enterprise

Protect devices, content, applications and transactions; address security from day one

- IBM MobileFirst Security Solutions
- IBM Trusteer Mobile Fraud Solutions
- Fiberlink® Mobile Security Solutions
- Mobile Application and Embedded Device Security

Adopt security-as-a-service

Leverage the ease-of-use, global availability and flexibility of cloud-based security

- IBM Cloud-based Security Services
- IBM Managed Web Defense
- IBM Trusteer Advanced Fraud Protection

Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service

Cloud-delivered IAM services provide a Fortune 10 client with a strategic business-to-customer (B2C) solution

Cloud-delivered Identity and Access Management (IAM)

Help secure access for

8.5M internal users and external

automobile customers

Help secure access for

50K union workers to manage their own

identities, according to union contract

Business Challenge

- Users need multiple discrete logins / passwords to access and use different web properties

- Unable to identify and track customers to enable development of targeted offers and a more personalized web experience

- Lack of internal security skills for deploying a strategic IAM solution in house

IBM Security Solution Benefits

- **Simplified web / mobile experience** via IAM integration with cloud-based social identities

- A single login providing access to a **more personalized online experience**

- **Reduced time to market** for realizing **IAM as a business enabler**

- **Agile and scalable** managed service that allows the client to "turn-on" and utilize additional services as the initiative expands globally

IBM

A global bank enables security-rich mobile access for millions of users

Safeguard Mobile Deployments

North American entity protects
user access to mobile and
web channels for

10,000

internal users

Mobile Users

Mobile Devices

Web and Mobile Apps

Business Challenge

- Protect employee and contractor access to web and mobile applications
- Roll out new application to customers and help protect access for mobile devices

IBM Security Solution Benefits

- Centralized user access control across web and mobile channels
- Reduced IT cost with self-care, single sign-on and session management
- Introduced risk-based access and multi-factor authentication for 10M+ customers

IBM Security has global reach

Security Operations Centers
Security Research Centers
Security Solution Development Centers
Institute for Advanced Security Branches

Map locations:
Ottawa, CA · Fredericton, CA · Almaden, US · Detroit, US · Waltham, US · Boulder, US · IAS Americas · TJ Watson, US · Costa Mesa, US · Raleigh, US · Austin, US · Atlanta, US · Heredia, CR · Belfast, N IR · Delft, NL · Brussels, BE · Wroclaw, PL · IAS Europe · Zurich, CH · Haifa, IL · Herzliya, IL · Riyadh, SA · Pune, IN · New Delhi, IN · Bangalore, IN · Nairobi, KE · Hortolandia, BR · Tokyo, JP · Taipei, TW · Singapore, SG · IAS Asia Pacific · Perth, AU · Brisbane, AU · Gold Coast, AU

IBM Security by the Numbers

133 + monitored countries (MSS)

3300 + service delivery experts

270000000 + endpoints protected

15000000000 + events managed per day

IBM X-Force® delivers expert analysis and threat intelligence

Attack Types
Backdoors
Botnets
Buffer Overflow Attacks
Client Side Attacks
Cross-site Scripting (XSS)
Distributed Denial of Service (DDoS)
Exploit Toolkits
Malicious Content
Peer-to-Peer Networks
Protocol Tunneling
Reconnaissance
SQL Injection
Trojans
Worms

Sharing real-time and anonymized threat intelligence

IBM Security Operations Centers and Security Products

X-Force Helps Keep Customers Ahead of the Threat

- Cataloging, analyzing and researching vulnerabilities since 1997
- Providing zero-day threat alerts and exploit triage to IBM customers worldwide
- Building threat intelligence from collaborative data sharing across thousands of clients
- Analyzing malware and fraud activity from 270M+ Trusteer-protected endpoints

1 Optimize your security plan and get help from experts

2 Stop advanced threats with security intelligence

3 Use a risk-based approach to protect your most valuable assets

4 Employ cloud and mobile to improve security

Learn more about IBM Security
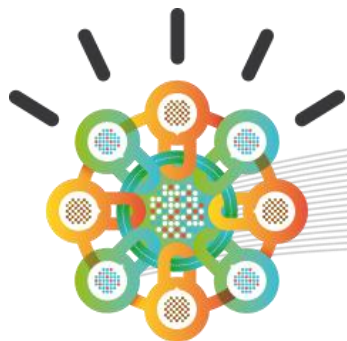
IBM Security
Intelligence. Integration. Expertise.

Visit our website
IBM Security Website

Watch our videos
IBM Security YouTube Channel

Read new blog posts
SecurityIntelligence.com

Follow us on Twitter
@ibmsecurity

Thank You

www.ibm.com/security