Security Intelligence.
Think Integrated.

Securing Information –
Enterprises' valued asset

August 2012

Raj Nagaratnam, IBM Distinguished Engineer; CTO for Security Solutions

natarajn@us.ibm.com

Evolving client priorities reflect top security business factors in 2012

1. Info Security is a boardroom topic
2. Three key objectives
3. Demand for “Global Best Practice”
4. Growth through acquisitions
5. Regulatory scrutiny is increasing
6. Increased consolidation trend
7. Value focus
8. Multi-party Collaboration Models

CIO & Team

Evolving Client Priorities – 10 Top Security Threat & Technology Factors in 2012

CIO & Team

1. Mobile / SmartPhone opens up new threat vectors
2. Social Media exacerbates other risks
3. IT must scale quickly and cost effectively (up or down)
4. Increasing attack sophistication
5. Application vulnerabilities remain a primary threat
6. Insider threat is key
7. Data & Database security focus is increasing
8. Increasing focus on multi-channel, bi-directional anomaly detection
9. Multi-layered enterprise security approaches are the goal
10. Growing concerns over PLC & related security

Data and Information services are vital to business, but providing them is fraught with risk

IT Security Risk Management

Data & Information Services

- Privacy breach/disclosure
- Insecure collaboration/data sharing
- Information Availability
- Inorganic growth of unstructured data
- Insecure archiving & test processes

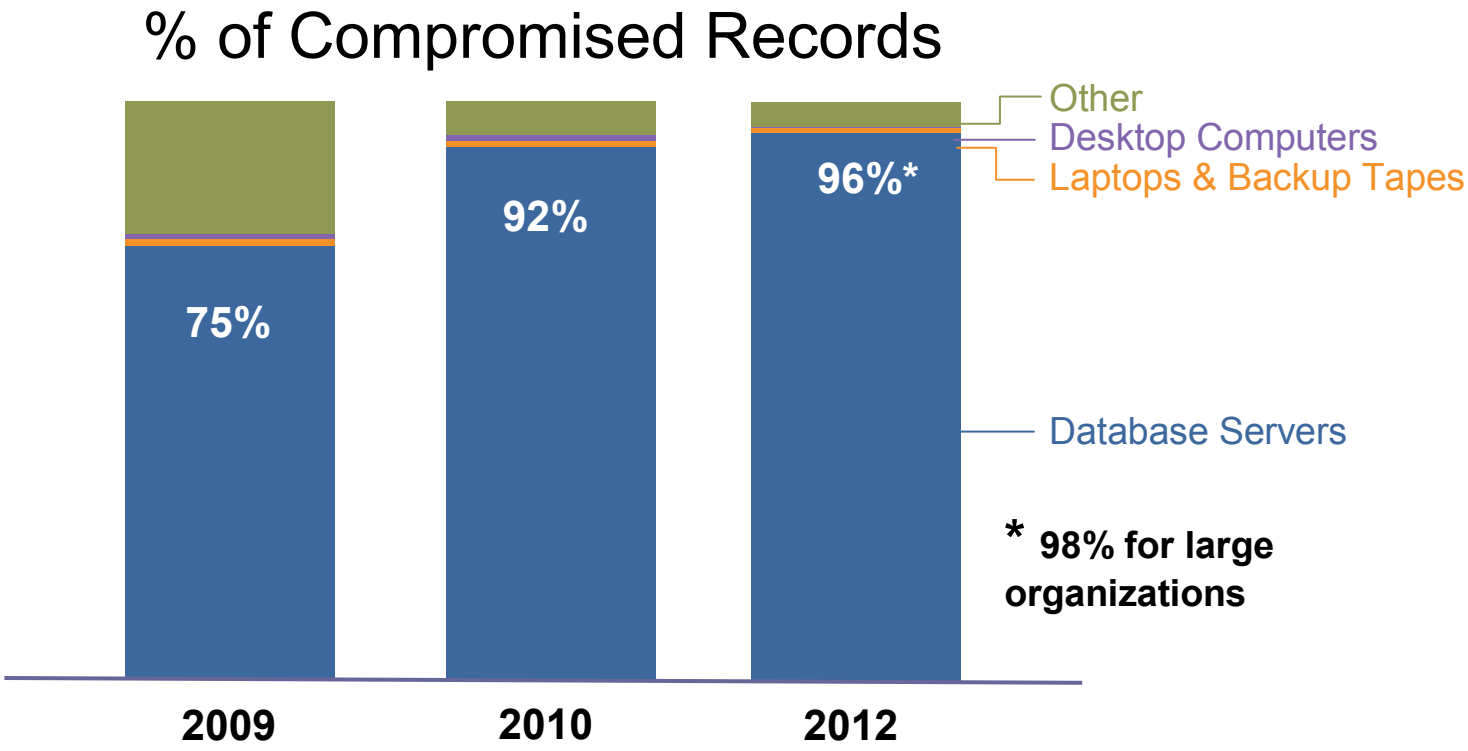
Infrastructure — Data — Application — People

Security Intelligence & Governance, Risk and Compliance spans the organization to address business pain points

Stakeholders

- Chief Security Officer
- VP of Engineering
- Chief Risk Officer (OpRisk)
- Physical Security Manager
- Financial Crimes Unit
- Legal Officer
- Chief Risk Officer
- Chief Information Security Officer
- Chief Privacy Officer/Legal Officer
- Line of Business Owner
- Chief Risk Officer

Database Servers are the Primary Source of Breached Data



Sources: Verizon Business Data Breach Investigations Report 2009, 2010, 2012

Although much angst and security funding is given to ***offline data, mobile devices, and end-user systems,*** *these assets* ***are simply not a major point of compromise."***

Clients' data adoption pattern leads to entry points for protection

Unstructured Data	Customer info, financial reporting, etc in spreadsheets. Data exchange through email, IM,..	Design documents, Formula, Source code,… - across files, email.. in server and endpoints
Structured Data	Access to customer and business data in DBs. Privileged Users & separation of duties.	Source code, engineering design,.. – in content and data repositories. Application access.
	Compliance	**Intellectual Property protection**

Multiple Entry Points

	Comments	At Rest	Over the Network	At the endpoint
Database & content protection	▪ Most of the breaches happen ▪ Application access ▪ Privileged users	X	X	
Unstructured data	▪ Files ▪ Exchanged ad hoc ▪ Could reside anywhere		X	X

A defense in depth approach is necessary to secure information assets

Trusting Identities

Customers or criminals?

Partners or competitors?

Employees or hackers?

Managing Access

Securing Services

Payroll

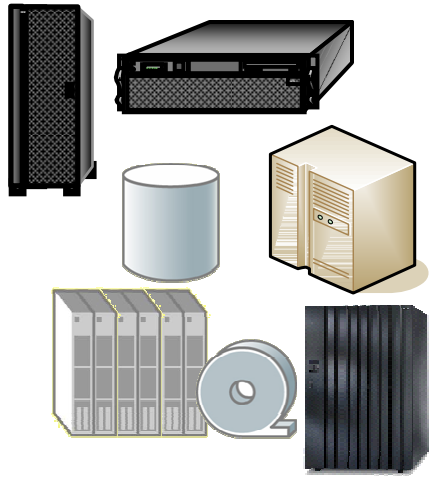
Online banking

Loan applications

Retail sales

Inventory

Protecting Data and Privacy



Security has to be applied within a business context and fused into the fabric of business and not as a widget to solve the next security threat

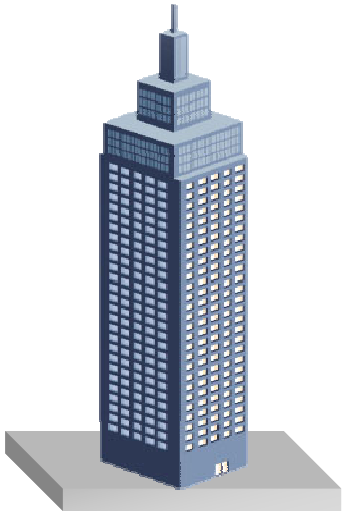
Factor in the trends driving the next wave of technical innovation

It is no longer enough to protect the perimeter – sophisticated attacks are bypassing traditional defenses, IT resources are moving outside the firewall, and enterprise applications and data are becoming distributed across multiple devices

1. Advanced Threats

Sophisticated, targeted attacks, designed to gain continuous access to critical information, are increasing in severity and occurrence.

Advanced Persistent Threats
Stealth Bots Designer Malware
Targeted Attacks Zero-days



Enterprise Customers

2. Cloud Computing

Security is one of the top concerns of cloud, as customers drastically rethink the way IT resources are designed, deployed and consumed.

IBM SmartCloud
vmware salesforce

3. Mobile Computing

Managing employee owned devices and securing connectivity to corporate applications are top of mind as CIOs broaden their support for mobile devices.

Windows Phone

4. Regulations and Compliance

Regulatory and compliance pressures continue to mount as companies store sensitive data and become susceptible to audit failures.

PCI Security Standards Council HIPAA Sarbanes-Oxley Financial and Accounting Disclosure Information

Getting a focused approach to securing information will be key to success

Security Intelligence
• Audit, compliance, threat intelligence

People	Data	Application	Infrastructure
• Who is accessing? •Employees •Partners •End users •Are they authorized? •Risk based access •Context aware •Entitlements •Privileged users	•Monitoring access •Who, what, when •Audit •Sensitive data •Masking •Test data •Cloud gateway	•Application access •Secure SOA • Web, mobile, cloud •Secure engineering •Vulnerability testing •Code analysis	•Network security •Intrusion prevention •Adv threat •Endpoint security •Configuration •Compliance •Patch

1. Gain visibility to your security and risk posture (Guardium, QRadar)
2. Assess your core information assets and determine your approach
3. Take a phased approach based on your environment
   - Protect your valuable data assets (encryption, access, gateway)
   - Tune down your user access (Identity, Access management)
   - Mitigate external threats (Network security)
   - Internal controls and vulnerabilities (Endpoint management)
   - Application access to data (app security)

IBM Security Systems Division Strategy

Buyers

CISO – CIO – Line-of-Business

Megatrends

- Advanced Threats
- Cloud
- Mobile
- Regulation and Compliance

Capabilities

Security Intelligence

- People
- Data
- Applications
- Infrastructure

Placeholder – a little deep dive into Guardium capabilities

Data: A major French bank deploys an enterprise-wide solution to help protect the privacy and integrity of trusted information

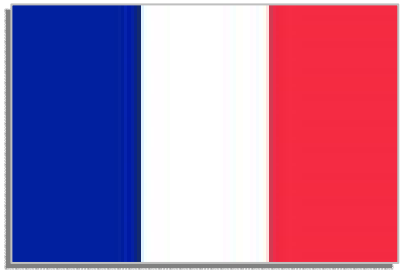
Monitor

150

sensitive applications on over

450

Oracle, Sybase and SQL servers



Business challenge:

- Improve control of database access via strong authentication mechanisms
- Audit and monitor on database operations
- Help prevent unauthorized database operations performed via client applications

Solution: (IBM InfoSphere Guardium Database Activity Monitor)

Monitor, capture and report on DB activity, alert and block sessions where warranted

Security Intelligence and Analytics: A financial information provider hardens defenses against threats and fraud

An international financial firm tracks

250

activity baselines dynamically adjusted over time and saved

50 – 80 %

on staffing versus alternative solutions

Business challenge:

- Detect wide range of security threats affecting public-facing Web applications
- Help identify subtle changes in user behavior that could indicate fraud or misuse

Solution: (QRadar SIEM, QFlow)

Real-time correlation of hundreds of data sources, anomaly detection to help identify “low and slow” threats, flexibility for easy customization and expansion

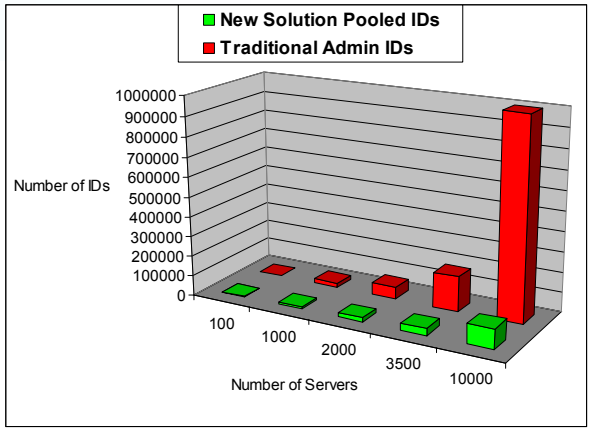
People: IBM Privileged ID Management for System Administrators

IBM provides strategic outsourcing services for

over 1200

Clients globally, with a high concentration in the

Financial Services Sector



Business challenge:

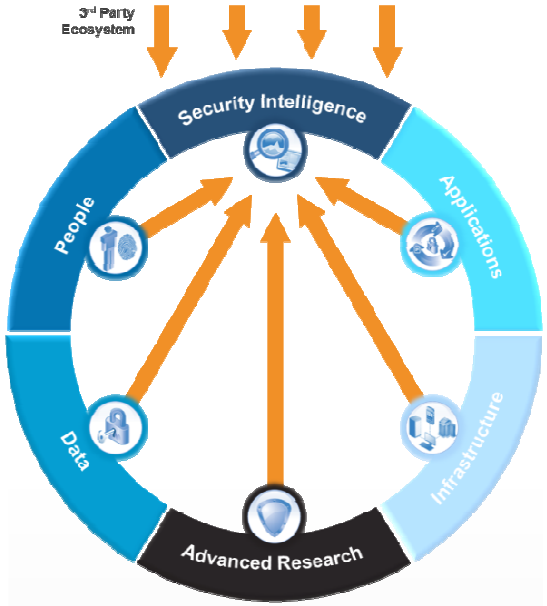
- IBM provides Server Outsource services to hundreds of customers globally
- Managing hundreds of servers across dozens of administrators quickly yields millions of privileged credentials (traditional approach)
- Alternately, sharing credentials decreases accountability
- More Privileged credentials = More risk and potential for loss/theft

Solution: (IBM Privileged ID Management)

- Centralized Privileged ID management improves IT control and **reduces risk**
- Automated sign on and check-in/out simplifies usage and **reduces cost**
- Comprehensive tracking and reporting **enhances accountability and compliance**
- Integration with IBM's personnel management system enables **automatic termination of access credentials** when employee or contractor leaves IBM

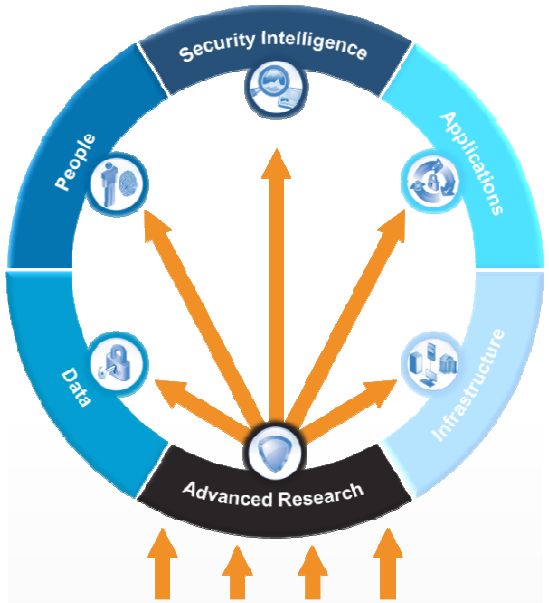
Integration: Help increase security, collapse silos, and reduce complexity

Integrated Intelligence.



- Consolidate and correlate siloed information from hundreds of sources
- Designed to help detect, notify and respond to threats missed by other security solutions
- Automate compliance tasks and assess risks

Integrated Research.

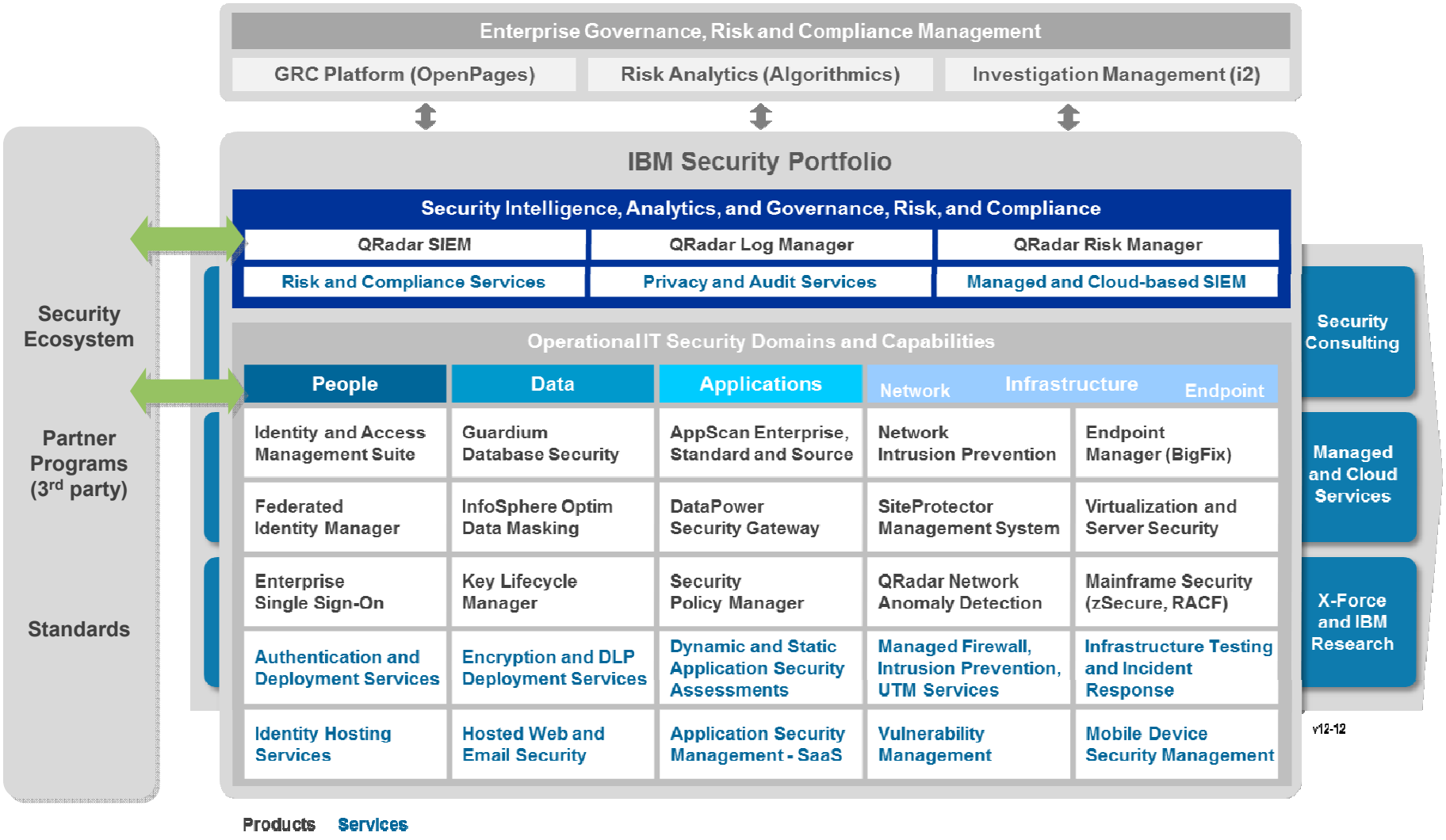


- Stay ahead of the changing threat landscape
- Designed to help detect the latest vulnerabilities, exploits and malware
- Add security intelligence to non-intelligent systems

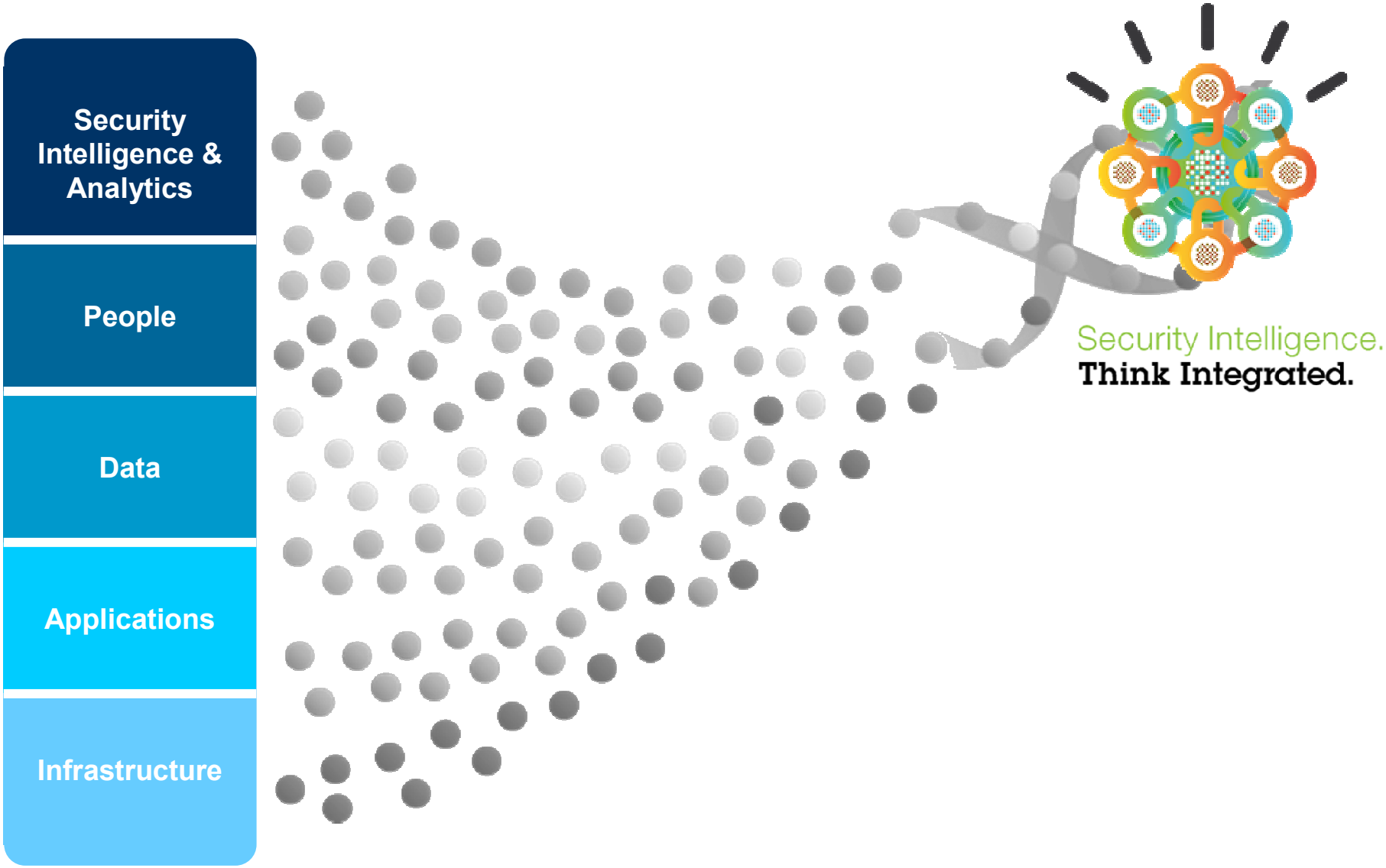
Integrated Protection.

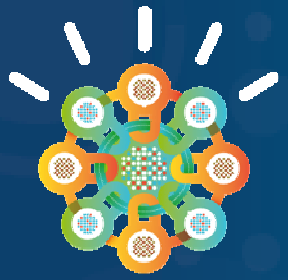
- Customize protection capabilities to block specific vulnerabilities using scan results
- Converge access management with web service gateways
- Link identity information with database security

Intelligence: Comprehensive portfolio across security domains

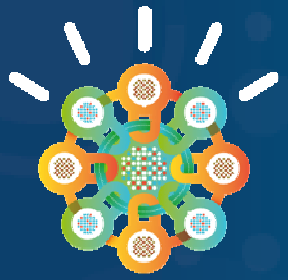


Intelligent solutions provide the DNA to secure a Smarter Planet



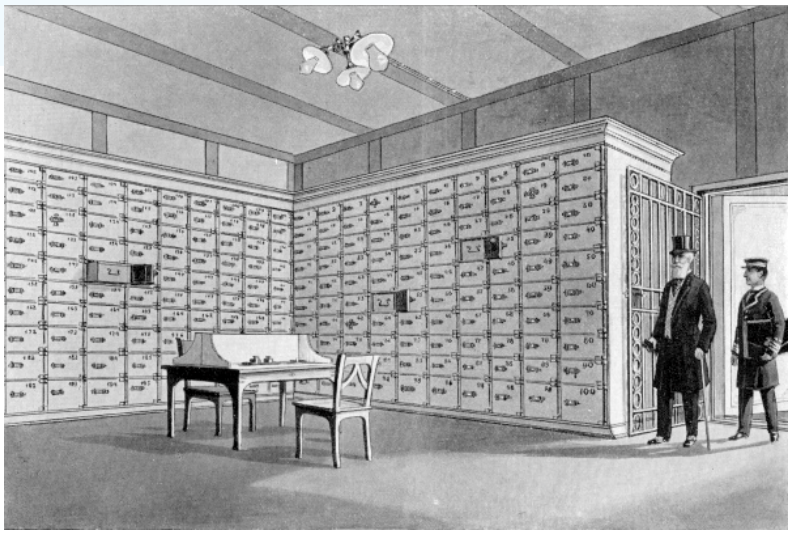


Backup



Best Enterprise Security Practices

Enterprise Security: European Banking Client



Our client needed a

Revamped Security Strategy

to strengthen information classification and protection, answer regulators, and protect the Brand.

Business challenge:

Develop and execute a rapid but phased approach to Transform the Enterprise Security Architecture to Meet Compliance and Regulatory Requirements.

Solution: (IBM Security Services & Products)

- Security Program & Architecture Development Services
- Security Training
- Application Security Products
- Information Discovery & Classification Services
- Database Security Products

Infrastructure (Network): An international commodities exchange analyzes and identifies threats in real time

Maintain system uptimes of over

99.9%

with

0

reported breaches in 3 years

"IBM Network Intrusion Prevention system helps maintain our uptime. In fact, since we put it in place three years ago, we have maintained system uptimes of over 99.9 percent."

– Head of Technology, Middle East Commodities Exchange

Business challenge:

- Help deploy robust security operations
- Help protect against emerging and critical threats
- Move from static to real-time threat protection

Solution: (IBM Network Intrusion Prevention System)

Analyze network traffic and transactions over a worldwide trading platform with over 230 members that connects multiple networks, from terrestrial links and VPNs to public networks

Security Intelligence and Analytics: Growth Markets
Payments Processor Achieves PCI Compliance

Global electronic payments firm operates in

32 Countries

and processes over

2 Billion

Transactions per year

Business challenge:

- Protect client data at the heart of this business
- PCI compliance for processing of >$25 billion in annual transactions
- Rapidly implement proven solution, 0 tolerance for delays or errors

Solution: (QRadar SIEM, IBM Security Network IPS)

- Integrated solution to provide visibility into PCI and data exposure risks
- Expert implementation services based on decades of financial industry experience
- Client passed PCI audit *four weeks* after purchase

Applications: A US Financial Organization creates a Secure Software Factory

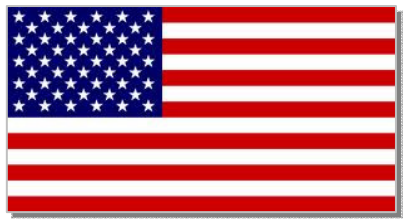
A large financial client needed to improve security for

Hundreds

of applications from internal and external sources. The client required

Consistent & Efficient

security measures.



> "This is the most successful deployment that we have had. A+"
>
> -- CTO, Architecture & Security

Business challenge:

- Client needed to centralized control and leverage a limited team of internal experts
- Solution need to be tightly aligned to their intended processes, but various SDLC's required flexibility

Solution: (IBM AppScan Source Edition)

- Created software"factory"
- Deployed and fully integrated into nightly build process
- Engineering delivered custom components
  - Build Automation server
  - Plug-in for Open Source Maven Project

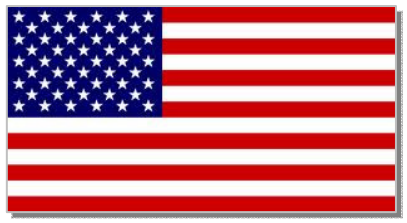
Infrastructure (Endpoint and Server): A regional bank and trust company streamlines endpoint management

A regional bank and trust company installs patches and updates within guidelines

95%

of the time and decreases update and patch cycle time from 2 to 3 weeks to

2 to 3 days



Business challenge:

- A highly distributed environment with nearly 1,800 branch locations
- No local IT resources, making it difficult to provide required patch compliance data

Solution: (IBM EndPoint Manager)

An endpoint management system installed on over 50,000 PC, servers, and mobile computers that, through automation, helps reduce productivity losses and human errors

Infrastructure (Endpoint and Server): IBM efficiently and security manages over 500,000 endpoints (including mobile)

IBM manages well over

500,000

Endpoints with

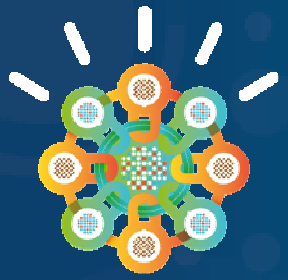
3 FTEs

Business challenge:

- Improve endpoint management & security without impacting employee productivity
- Displace homegrown technology
- Multi-platform environment (Windows, Mac, Linux, iOS, Android)

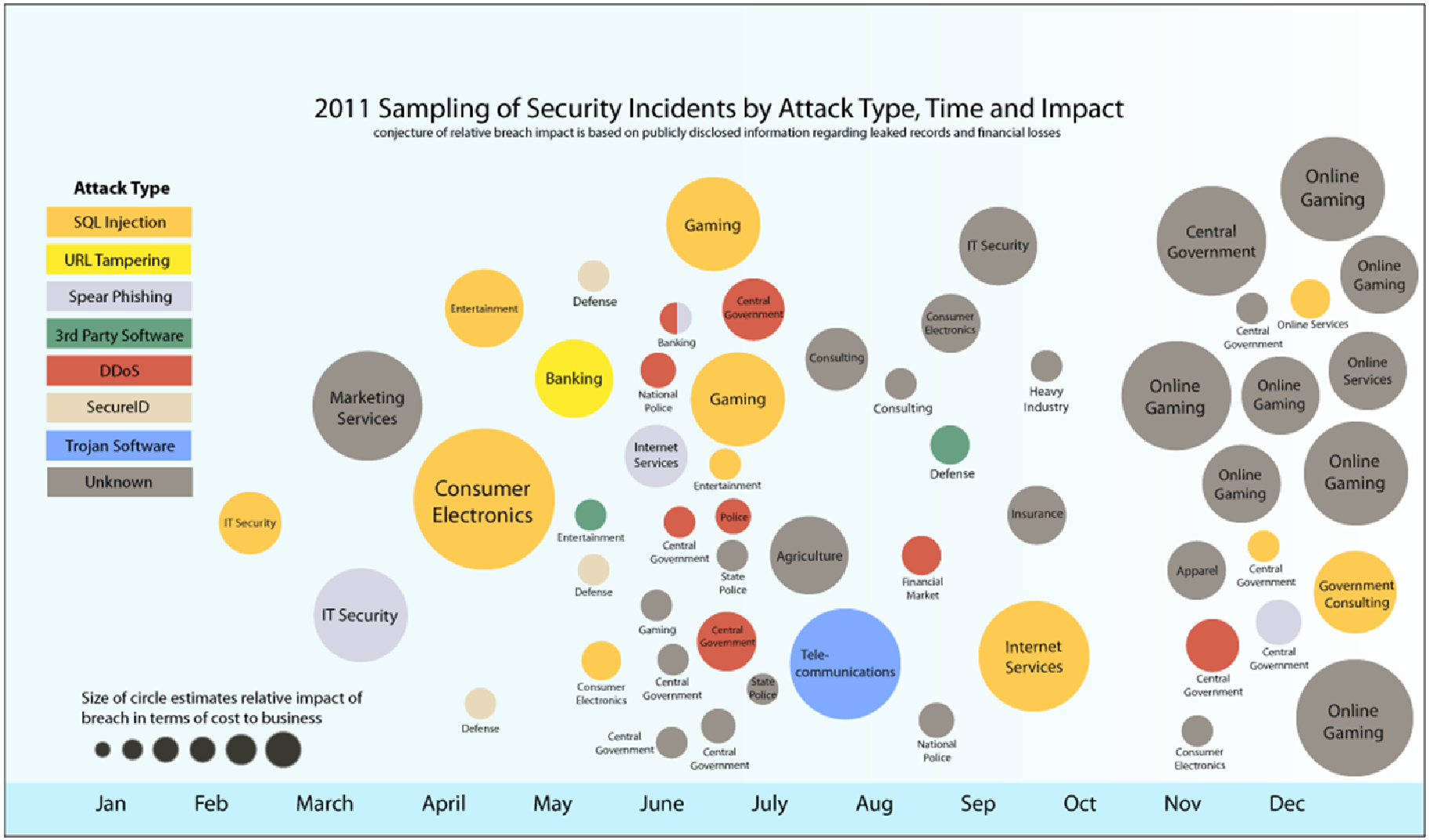
Solution: (IBM EndPoint Manager)

- Fastest client deployment in IBM history - deployed to all Windows clients within 6 months
- 78% decrease in security-related problems since deployment
- >$10M savings in associated cost avoidance
- Migration to persistent compliance model from employee reliant model



Additional Materials

2011: Year of the Targeted Attack



Source: IBM X-Force® Research 2011 Trend and Risk Report

Some Principles for countering advanced, persistent, & sophisticated threats:

- **Get basic stuff right**
  - Doing normal preventative computer security well closes gaps that matter
  - If you can't keep Anonymous out of your network, you can't keep spies out
- **Pay attention to subtle indicators**
  - The APT will avoid being loud
  - Attackers may come baring legitimate credentials
- **Embrace imperfect detection measures**
  - There are no perfect detection methods
  - Every detection is a win
- **Think about the attacker's process – the "Kill Chain"**
  - Reconnaissance
  - Exploitation
  - Infection
  - Command and Control
  - Internal Pivot
  - Data Preparation
  - Data Exfiltration

Expertise: Global coverage and security awareness

IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration

14B analyzed Web pages & images

40M spam & phishing attacks

54K documented vulnerabilities

Billions of intrusion attempts daily

Millions of unique malware samples

X-FORCE

World Wide Managed Security Services Coverage

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 13B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)