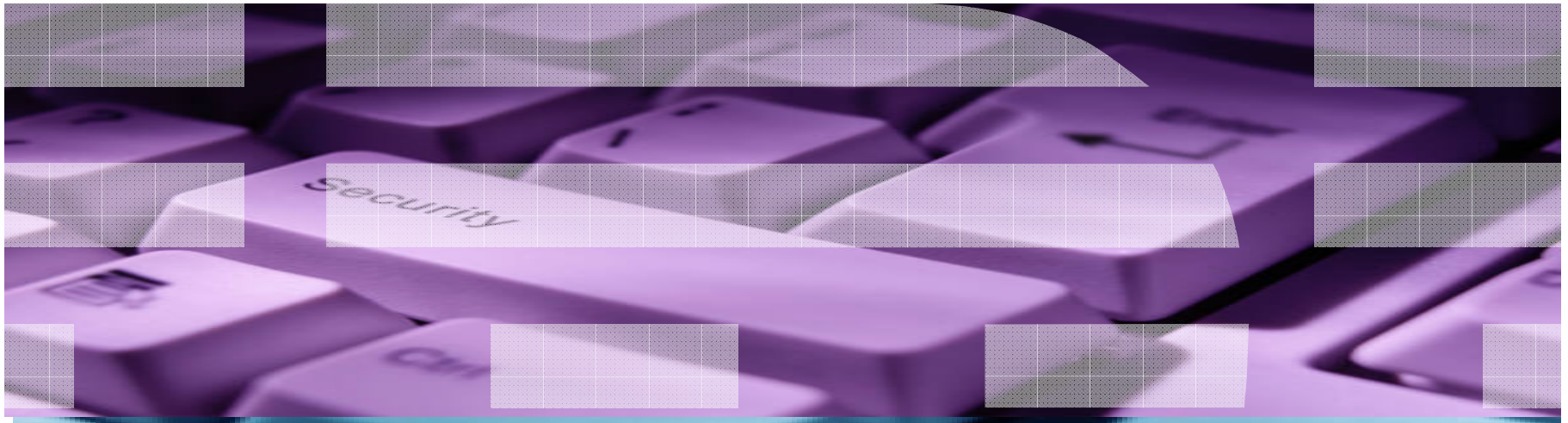


IBM Security Services

Foundational Security Solutions for Managing the Changing Security Threat Landscape and for Meeting Complex Compliance Requirements



Presentation Objectives

Our clients tell us that are having challenges meeting the compliance and audit demands. Moreover, the pervasiveness of mobile devices and cloud computing adds more complexity and challenges.

During this presentation we present you with three solutions that will provide a sustainable, effective and cost-efficient approach to achieving improved security and long term compliance.

Agenda

- The Changing Threat Landscape
- How IBM helps clients meet the security challenges
- Three Foundational Security Solutions/Best Practices
 - Data Protection
 - Key and Certificate Management
 - Mobile Security

PCI-DSS HIPAA
GLBA FISMA
SOX J-SOX
Basel II
ITAR ISO 27000



The impact of security breaches is becoming more apparent...



\$226 Billion

Economic impact of cyber attacks on businesses has grown to over \$226 billion annually.

Source: Congressional Research Service study

33%

A third of healthcare workers keep confidential information on portable devices without adequate security.

Source: "Healthcare workers putting patient data at risk"

158% increase

Security breaches are on the increase: cyber attacks have increased 158% since 2006¹, and worldwide cyberattacks increased 30% over the second half of 2008².

Sources: ¹US Department of Homeland Security, ²IBM Internet Security Systems X-Force

52%

Private-sector statistics show that the insider threat is up more than 52% in the past year.

Conventional Approaches Fail



New Threat = New Product, Vendor

Force Business Process to Change

User Productivity Impacted

Numerous Control Panels, Interfaces

Multiple disparate Policies, Reports

Expensive Deployments, Support

Increasing Complexity, Cost and Risk

Countrywide Insider Steals 2 Million People's Information

Posted on August 4th, 2008

by Ed Dickson in All News, Blogosphere News, Breaking News, California News, Economic News

Probe Targets Archives' Handling of Data on 70 Million Vets

By Ryan Singel  October 1, 2009 | 8:05 am | Categories: Breaches, Fed Blotter, politics

T-Mobile: Employee Data Theft Leads To U.K.'s Largest Data Breach

Employee sold millions of customer records to data brokers, reports say

Nov 18, 2009 | 05:51 PM

AvMed: Data of 208,000 at risk after Gainesville theft

Date: Mon, 8 Feb 2010 13:30:12 -0500

Gainesville Times

Clients today are facing new pressures to improve risk management

Risk Management-related pains

- “Threats are growing and changing. How do I stay current and assess their impact on the business?”
- “How can I be sure that my security policies are up-to-date and meeting the organization’s risk management objectives?”
- “I need a dashboard that not only provides business management a view of the risks, but also enables IT to pinpoint its source.”
- “How should I allocate security spending to maximize risk reduction?”
- “Which security tools would help me best lower my IT risk?”



Compliance-related pains

- “Regulatory mandates are growing and impacting more areas of the business.”
- “I need a map that shows if a control will address multiple regulations.”
- “These regulations are a moving target. How can I be sure my controls are kept current?”
- “Privacy laws are more strict in Europe. Are my US-defined controls sufficient?”
- “How can I assess that my vendors and partners are also in compliance?”
- “How can IT help my Compliance Officer demonstrate to examiners that we are in compliance?”

A smarter planet introduces several security challenges.

Key drivers for security projects

Increasing complexity



Soon, there will be **one trillion** connected devices in the world, constituting an “Internet of things”

Rising costs



Spending by U.S. companies on governance, risk and compliance will grow to **US\$29.8 billion** in 2010

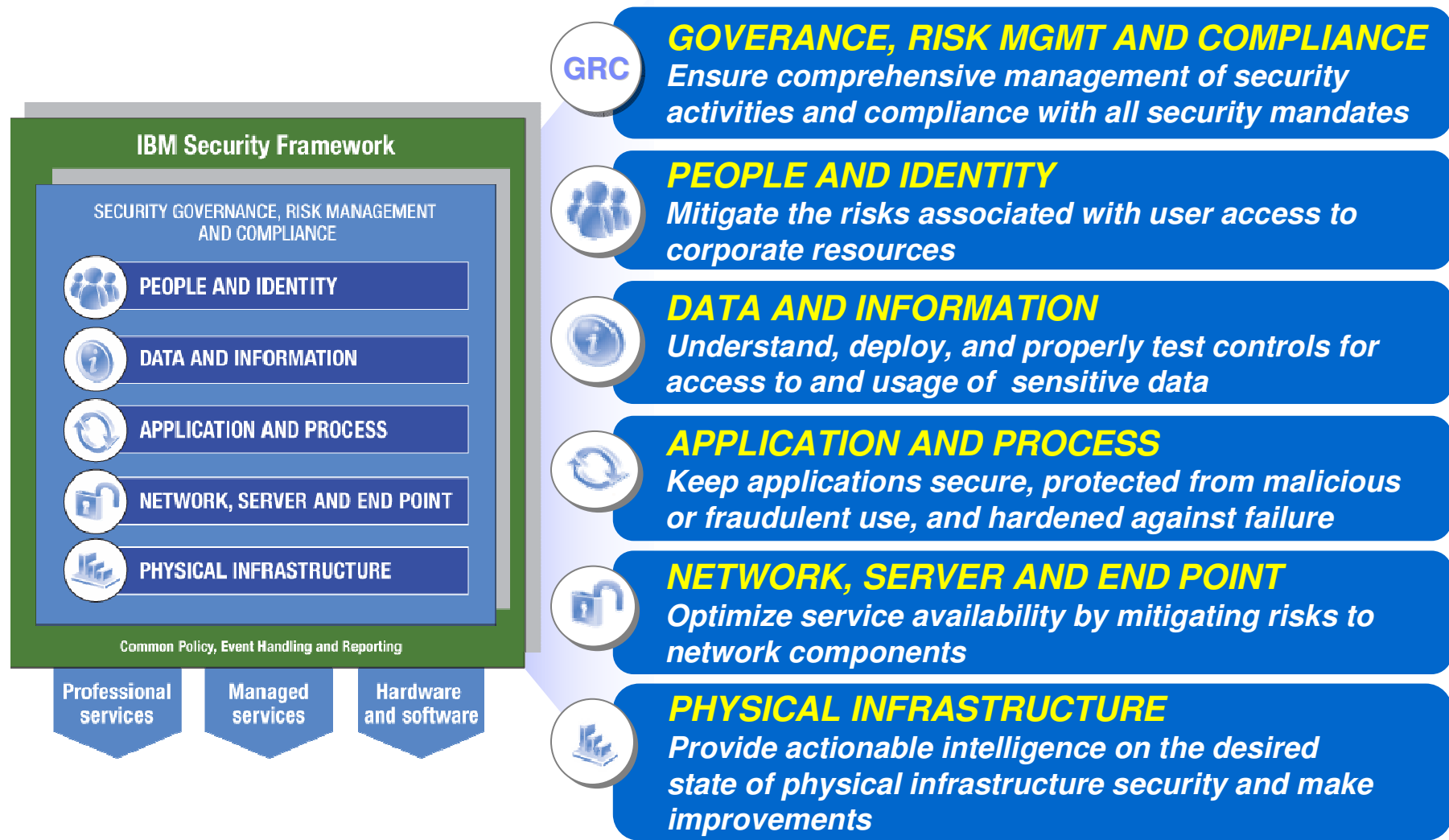
Ensuring compliance



The cost of a data breach increased to **US\$204** per compromised customer record

Source: Compliance Management News: Governance, risk and compliance spending to grow in 2010, by Linda Tucci, Senior News Writer, December, 2009
http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html

A Security Framework supports Integrated Service Management helping you assess and manage risk



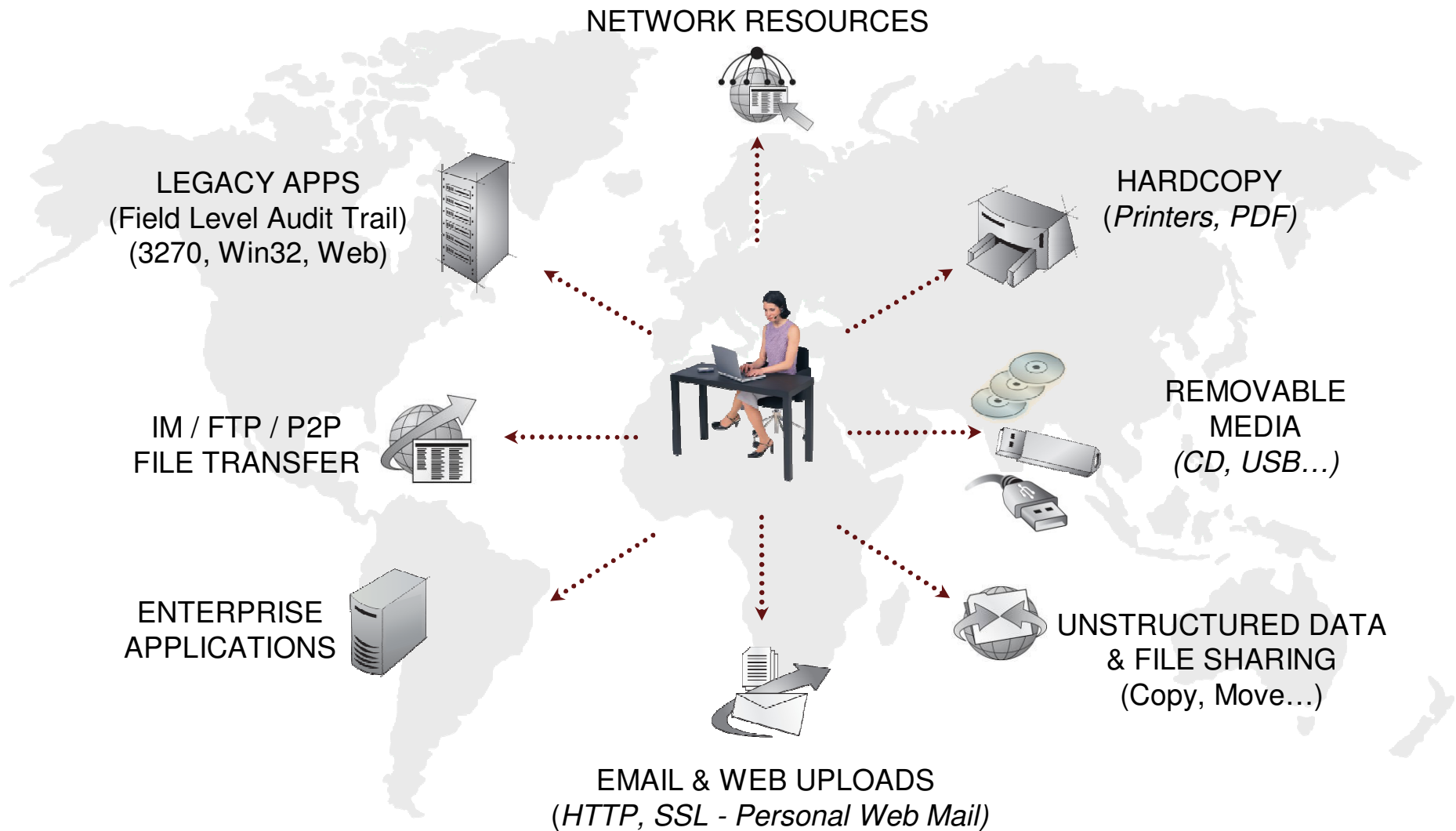
Three smart security solutions to manage threat, improve operational efficiency

Data Protection

Key and Certificate Management

Mobile Security

Data, Data, DataEverywhere



Endpoint Information Protection vs Data Loss Prevention

EIP

DLP

Network Monitoring & Control
Data Discovery
Email Monitoring & Control
Host Monitoring & Control

Unified Encryption (file, email, disk)
Removable Media / Device Mgt
VDI controls
Logical Network Segmentation
Secure Collaboration
Export Controls
Application Vaulting
Application Data Management
eDiscovery & Forensics
Host Based Network Control
Distributed Data Discovery
Application Based Email Monitoring & Control
Host Content & Context Monitoring & Control
Information Policy Awareness & Training
Legacy Application Remediation
Automated Classification & Tagging
Process Compliance Auditing
Transactional Security

IT Control Cases

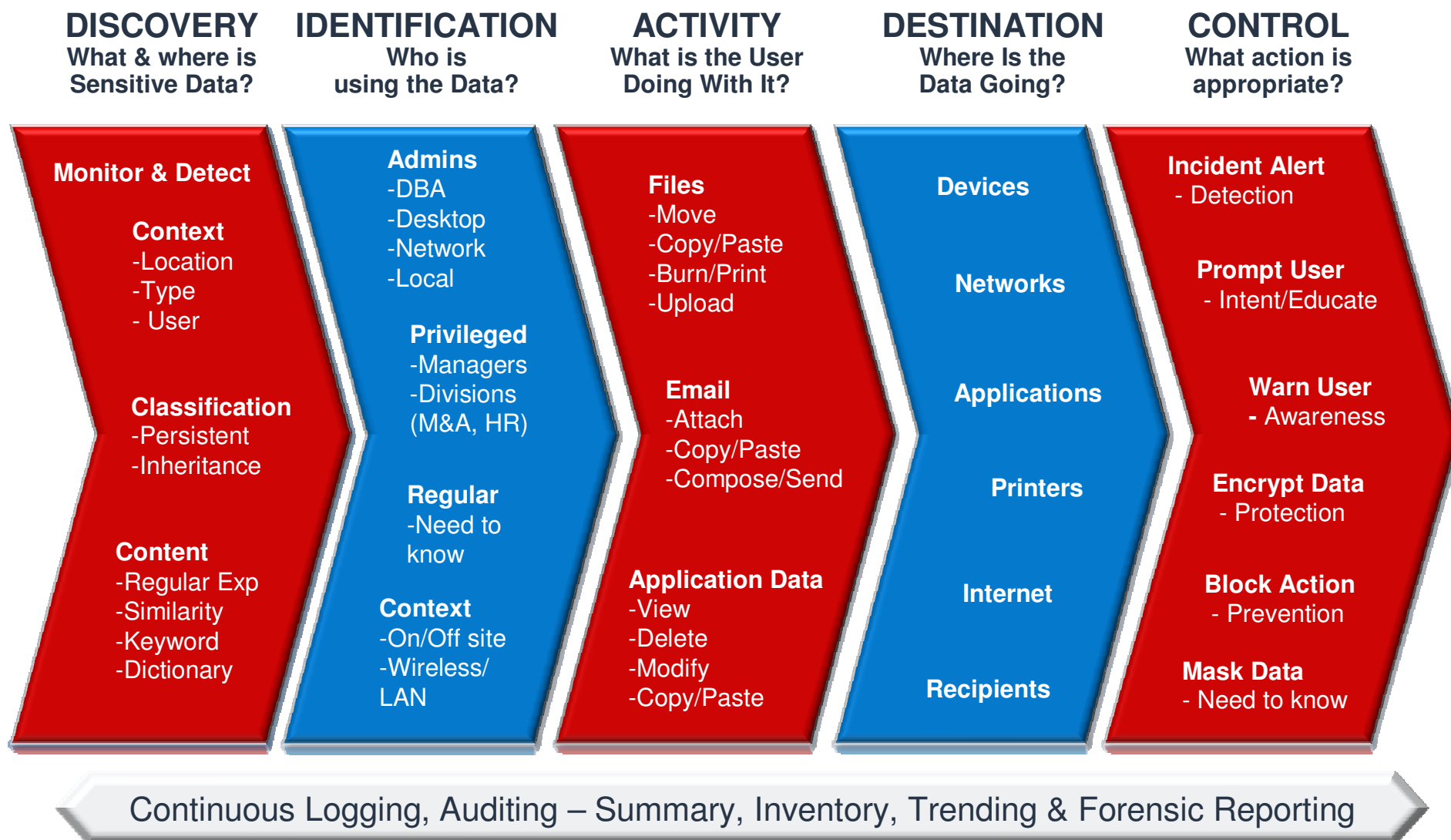
Value

Business Use Cases

Value Proposition

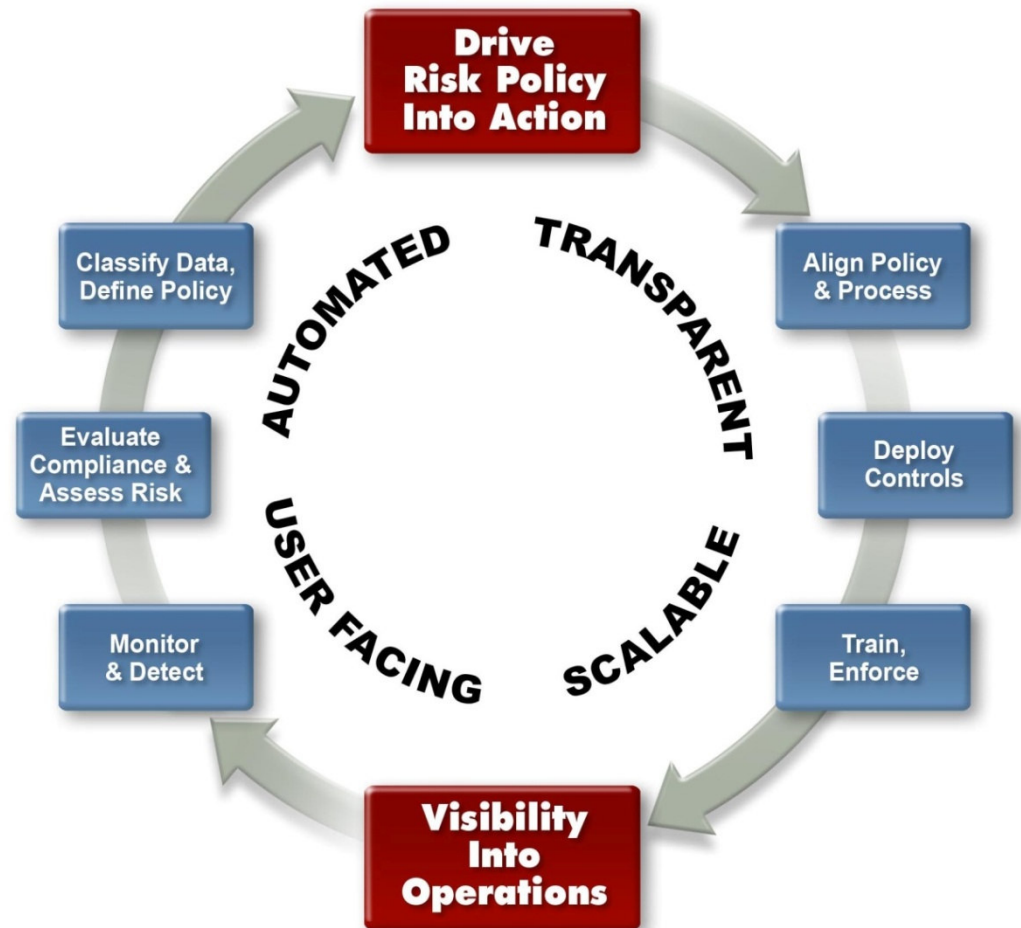
- **Enable the enforcement of the usage policy based on the classification of the data**
- **Monitor and control employee behavior at the endpoint egress points for data leakage on network and off for (Call Centres, 3rd party, Partners, Dealers, M&A)**
 - Content inspection of files, buffers and streams usage visibility and efficient control capabilities
- **File transformation/encryption will propagate the file labels**
- **Managing data loss to business by guiding the end user to apply the risk appropriate remediation controls**
- **Where controls have not been applied, inform the data owner/business on data breaches and usage reports by classification**

Data-Centric Information Understanding and Protection

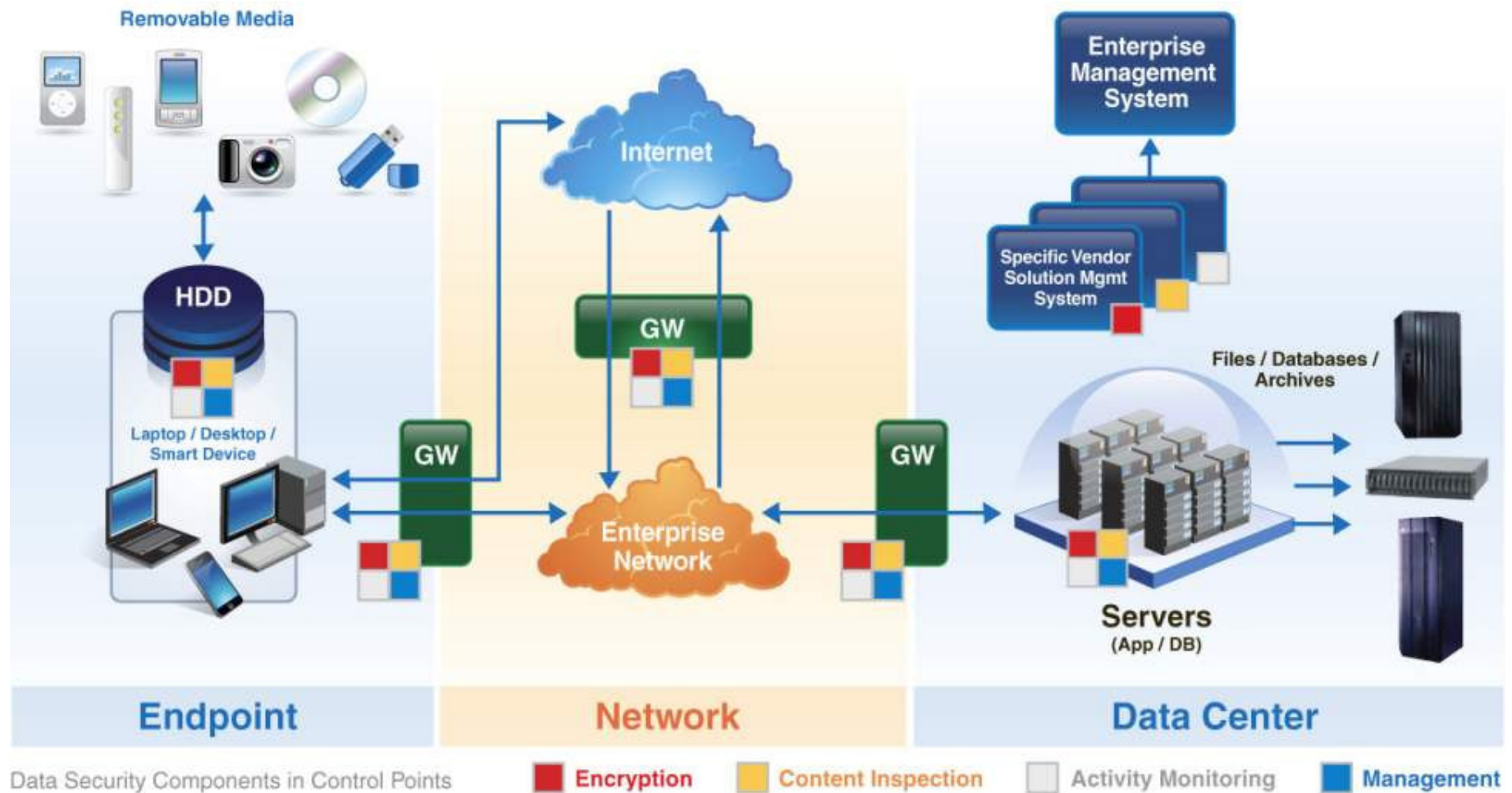


Continuous Strategic Information Protection

- Complete data level Visibility
- Perform risk-based evaluation of data location & usage
- Define actionable data classification & information protection policies
- Drive policies into action
- Align information protection policies & business processes
- Train and drive accountability to end users in real time
- As change occurs, monitor and detect and repeat the process



Solution Context: Create a holistic framework to unify the who, what, when, where, and how to protect data every step of the way



Three smart security solutions to manage threat, improve operational efficiency

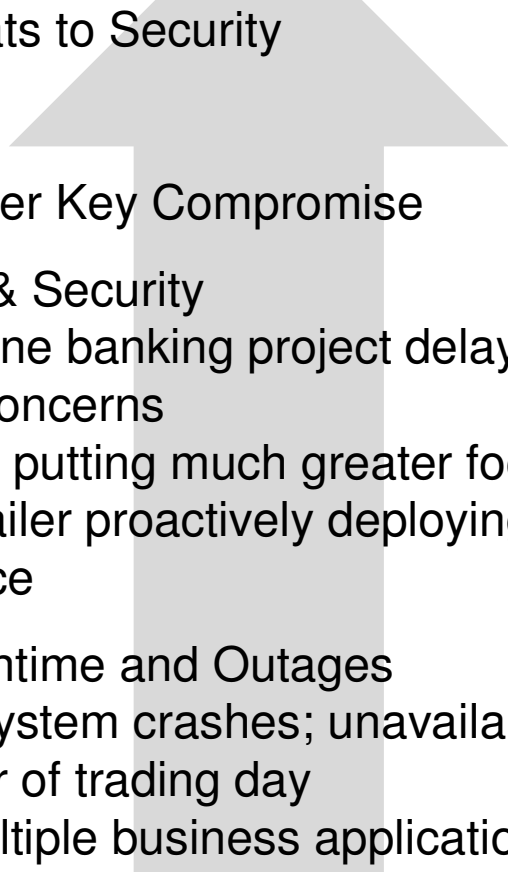
Data Protection

Key and Certificate Management

Mobile Security

Unquantified and Unmanaged Risk

An Evolution

- 
- Market Threats to Security
 - Stuxnet
 - Wikileaks
 - PS3 Master Key Compromise
 - Compliance & Security
 - Major online banking project delayed nearly two years due to private key security concerns
 - PCI 2.0 is putting much greater focus on private key security in audits
 - Major retailer proactively deploying 10s of 1000s of certificates for PCI compliance
 - System Downtime and Outages
 - Trading system crashes; unavailable to customers and brokers through remainder of trading day
 - Loses multiple business applications simultaneously; DSL provisioning down for nearly 24 hours
 - Production line down for several hours

Is Your Organization at Risk?

- How would you answer these questions?
 - 1.Key & certificate vulnerability?**
 - a) Can you account for all of the digital certificates and encryption keys in your environment?
 - b) Do you know who owns the keys and certificates?
 - c) Do you know which keys/certs will expire/rotate in the next 10 days?
 - d) Do you know the issuing source & physical location of the keys and certificates?
 - 2.Do your administrators have direct access to private keys?**
 - a) Are key and certificate management processes manual?
 - b) Do separation of duties and access controls exist?
 - c) Are key operations logged?
 - 3.Do keys & certificates protect sensitive regulatory data and communications?**
 - a) What types?
 - b) How valuable is this data? How valuable are the communications?

Do you have Unquantified and Unmanaged Risk?

Case Study

	Before			After		
		Installed	Not Installed		Installed	Not Installed
Known	On Radar	1,255 In 3 XLS's	40 In 2 CA's	On Radar	2,457 1 Data Base Backed Up	5 In 2 CA's 1 Int/1 Ext
Unknown	Off Radar	1,202 Not Recorded	55 In 2 CA's			

▪ Net Results

– Confirmed Unquantified Risk

- 95% Larger Population than expected
- 110% More Unused Certs than expected
- Risk is Managed

Reduced # of CA's:

Before: 4 CA's: 2 known & 2 unknown

After: 2 CA's: 1 internal & 1 external

- Reduced scattered data:
- Before: 3 separate spreadsheets with no backup
- After: Single database with production backup
- Proactive Discovery every 24 hours automated
- Proactive Notification automated

Notify every 60, 45, 30, 15, 5 days until renewed

Best Practices For Key and Certificate Management

Practice	Description
Downtime Avoidance	Ensure certificates and keys do not expire in-place: <ol style="list-style-type: none"> 1. Build a complete and accurate encryption asset inventory 2. Validate accuracy of inventory & update regularly 3. Determine responsible parties for each asset 4. Monitor for expirations 5. Notify responsible parties and escalate as necessary
Enhanced Security / Risk Reduction	Improve key and data security: <ol style="list-style-type: none"> 1. Determine current key access chain 2. Ensure key protection standards are in place 3. Reduce exposure to absolute minimum 4. Minimize validity periods 5. Track parties and rotate keys immediately in response to changes
Demonstrable Compliance	Show clear evidence of policy compliance: <ol style="list-style-type: none"> 1. Establish concise policy guidelines (dual control, separation of duties, logging, policy) 2. Reconcile inventory with applicable policies 3. Show timeline for demonstrable adherence 4. Establish audit response process 5. Establish response plan for out-of-policy items
Operational Cost Reduction	Reduce encryption asset management costs: <ol style="list-style-type: none"> 1. Minimize repetitive and error-prone manual processes 2. Leverage appropriate sourcing for encryption assets

Venafi Key & Certificate Mgmt Solution



Discover & Monitor

- Locate certificates and keys
 - Published or unpublished
- Create Book of Assets
 - Asset Type
 - Expiration/Rotation Dates
- Notify admins of expiring assets
- Provide reporting/export



Enroll

- Provide simple, common process for new/renewal
 - Multiple Certificate Authorities
- Reduce admin time to minutes with consistent quality results
- Engage & educate distributed admin users
- Policy driven workflow processes



Provision

- Eliminate business interruption risk
 - 100% verification
- Control the complete process
 - Human check points with automation
- Automated enforcement of all policies
- Full history logging

Infrastructure Management

Unified Enterprise Policies | External System Interfaces | Granular Controls | Workflow Driven

Three smart security solutions to manage threat, improve operational efficiency

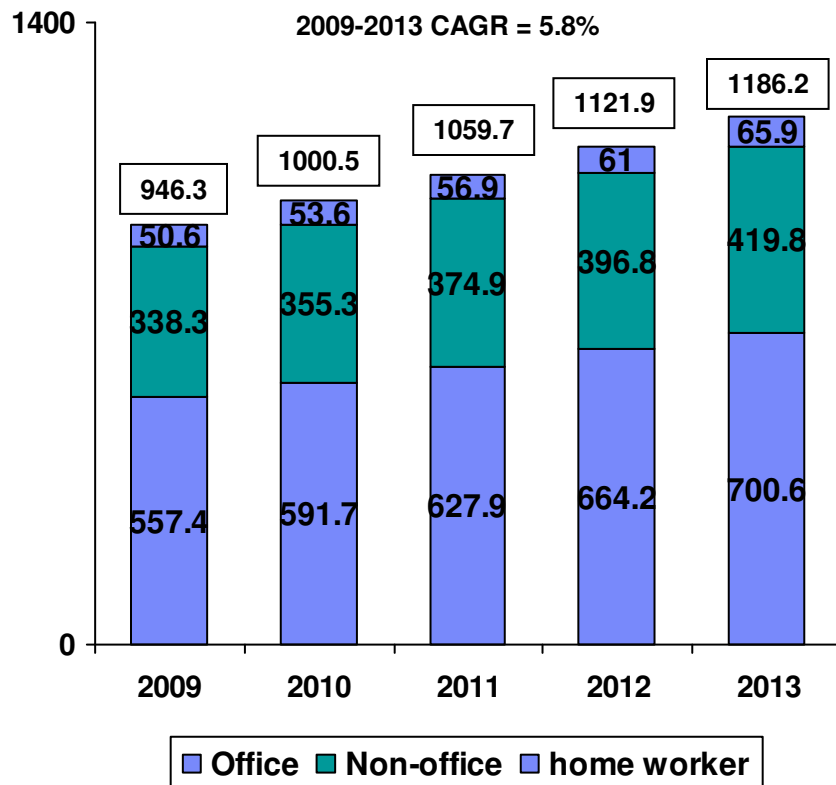
Data Protection

Key and Certificate Management

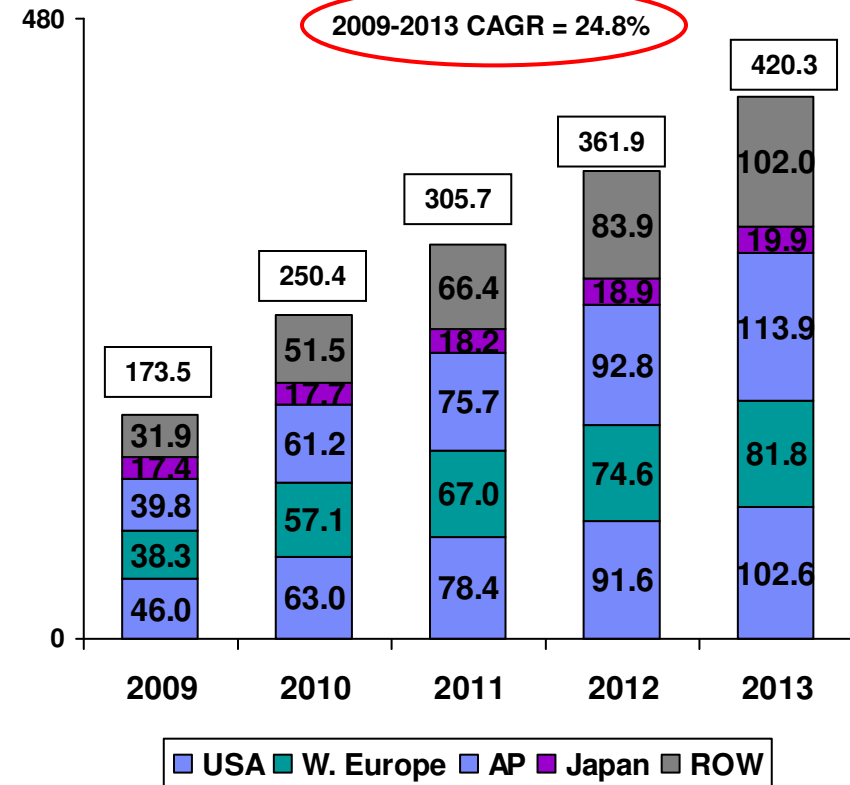
Mobile Security

The mobile worker population grew to 1 billion in 2010, with the increasing proliferation of smartphones and other smart devices becoming a notable management challenge

WW Mobile Worker Population (M)



WW Smartphone Shipments (M)



Sources: "WW Mobile Worker Population 2009-2013 Forecast," IDC, December 2009. "WW Smartphone 2010-2014 Forecast Update: June 2010," IDC, June 2010.

Mobility solutions enable organizations to improve information access, enhance productivity and provide better client service

Mobile devices bring enterprises great benefits:

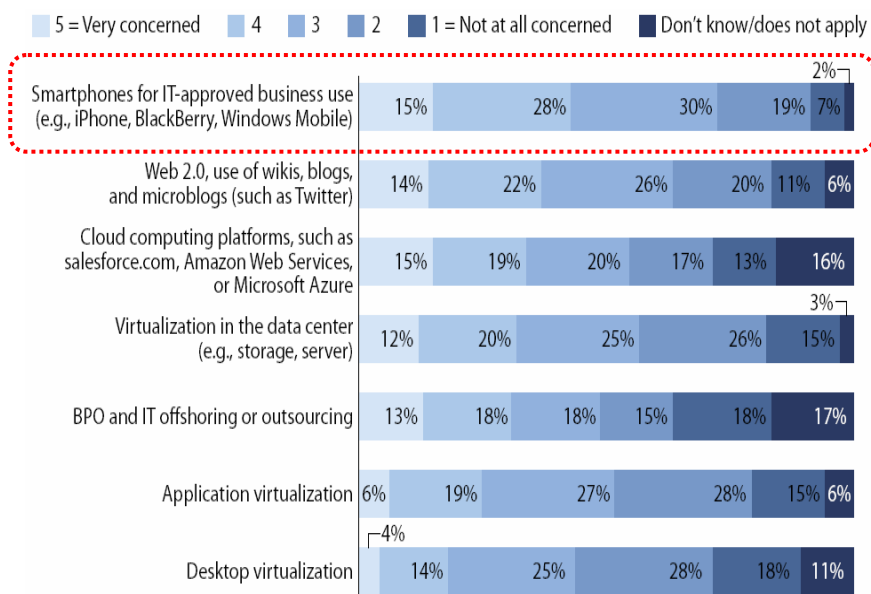
- Allow employees to access business information anywhere, anytime
- Improve worker effectiveness and productivity through better connectivity
- Provide mobile work locations for employees
- Increase business communication and collaboration
- Improve responsiveness to clients' needs
- Reduce telecommunication and network ownership costs

But they also present significant challenges:

- Support for a variety of mobile device types, platforms, and service providers
- Management of devices not necessarily owned by enterprises
- Mix of business and personal information on the same device
- Dissemination of enterprise confidential information on insecure device
- Lack of control on applications that can exist on devices
- Short of skills for mobile technology

Smartphones cause the most security concerns among IT executives, as 44% of users purchase their own devices

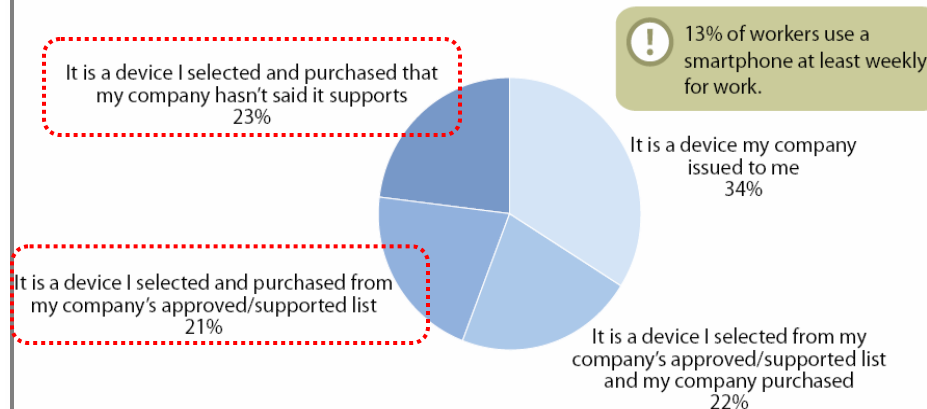
“How concerned is your firm about the level of security or IT risk in adopting the following technologies or technology initiatives?”



Base: 1,959 North American and European enterprise and SMB IT security decision-makers (percentages may not total 100 because of rounding)

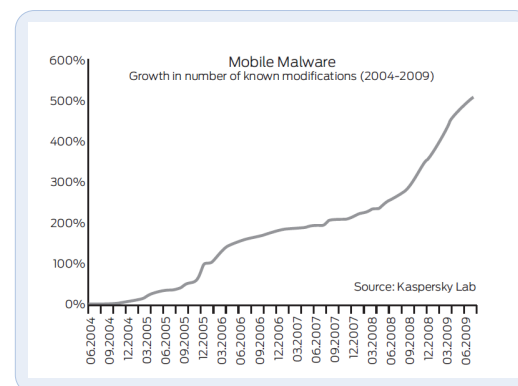
Sources: “Understanding Information Worker Smartphone Usage,” Forrester, November 2009 and Kaspersky Lab

“Which of the following statements describes the primary smartphone you use for work?”



Base: 503 US, Canadian, and UK information workers at companies with 100 or more employees


Growth in number of known malware modifications (2004 – 2009)



The security threats to mobile devices have evolved to all the threats applicable to desktops plus new ones unique to mobile devices

The threat profile to mobile handheld devices is actually a superset of the profile for desktops:

- *Malware - viruses, worms, Trojans, spyware*
- *Spam – voice, SMS, email based*
- *Device loss or theft - losing sensitive data*
- *Application installed without permission*
- *Eavesdropping - sniffing data as it is transmitted*
- *Access to corporate data from unauthorized devices*
- *Exploitation and Misconduct - online predators, pornography*



Mobile devices are becoming Mobile computers...but are they being protected the same way?

Opportunities exist for potential attackers to eavesdrop and extract personal information from phone directories or just pinpoint a users whereabouts by queuring the phone's GPS system.

Rutgers University

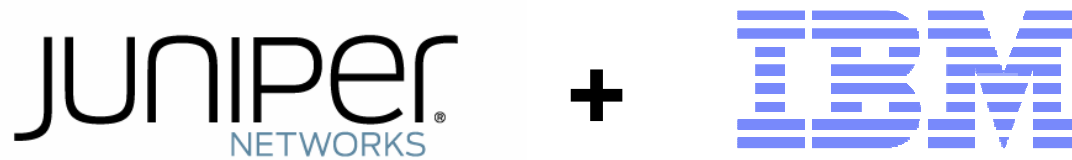
Researchers have demonstrated how they can force certain types of smartphones to visit a malicious URL or install an application without user approval

News.cnet.com

As mobile devices become more ingrained in individuals lives, they tend to contain more financial, medical corporate and personal information, ripe for exploitation. Also we see mobile devices become a conduit for financial transactions, the need for security will grow.

Deloitte

A comprehensive mobile security solution built upon Juniper's industry leading mobile security technology and IBM's world class cloud-based managed security services

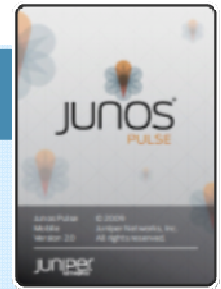


“Juniper is an industry leading networking equipment and technology provider. IBM is the largest IT service provider in the world. Combining the technology innovation, solution delivery capability, and service quality of these two companies gives clients a best guarantee in securing employees’ wireless devices used in the workplace.”

Juniper's Junos Pulse Mobile Security Suite (SMobile) is designed for enterprises to embrace mobile devices with security risks minimized

DESIGNED TO PROVIDE:

- Granular role-based, secure VPN on mobile devices
- Security on a broad range of mobile devices from malware, viruses, & spam
- Ability for enterprise IT to alleviate primary concern on mobile devices and smartphones – loss/theft
- Flexibility and ability for enterprise IT to support employees' personal devices in a zero-touch deployment model



Broad, comprehensive mobile platform support



iPhone



Google Android



Win Mobile



Nokia Symbian



BlackBerry

A comprehensive set of security features is provided to address major security concerns of various customer groups



ANTIVIRUS

- Real-time protection updated automatically
- Scans files received over all network connections
 - SMS, MMS, email, direct download, Bluetooth, infrared, etc.
- On-demand scans of all memory or full device
- Alerts on detection



PERSONAL FIREWALL

- Inbound/Outbound Port +IP Filtering automatically
- Full control of alerts/logging
- Default (high/low) filtering options + customizable



ANTI-SPAM

- Blacklist filtering – blocks voice and SMS spam
 - Block calls, messages or both,
 - Automatic adds contacts to blacklist
- Message settings
 - Save to Inbox, save to spam folder or delete
- Disable alerts for incoming messages
- Automatic denial for unknown or unwanted calls



LOSS/THEFT PROTECTION

- Remote Lock and/or Wipe
- GPS Locate/Track
- Device Backup/Restore
- Remote Alarm/Notification
- SIM Change Notification

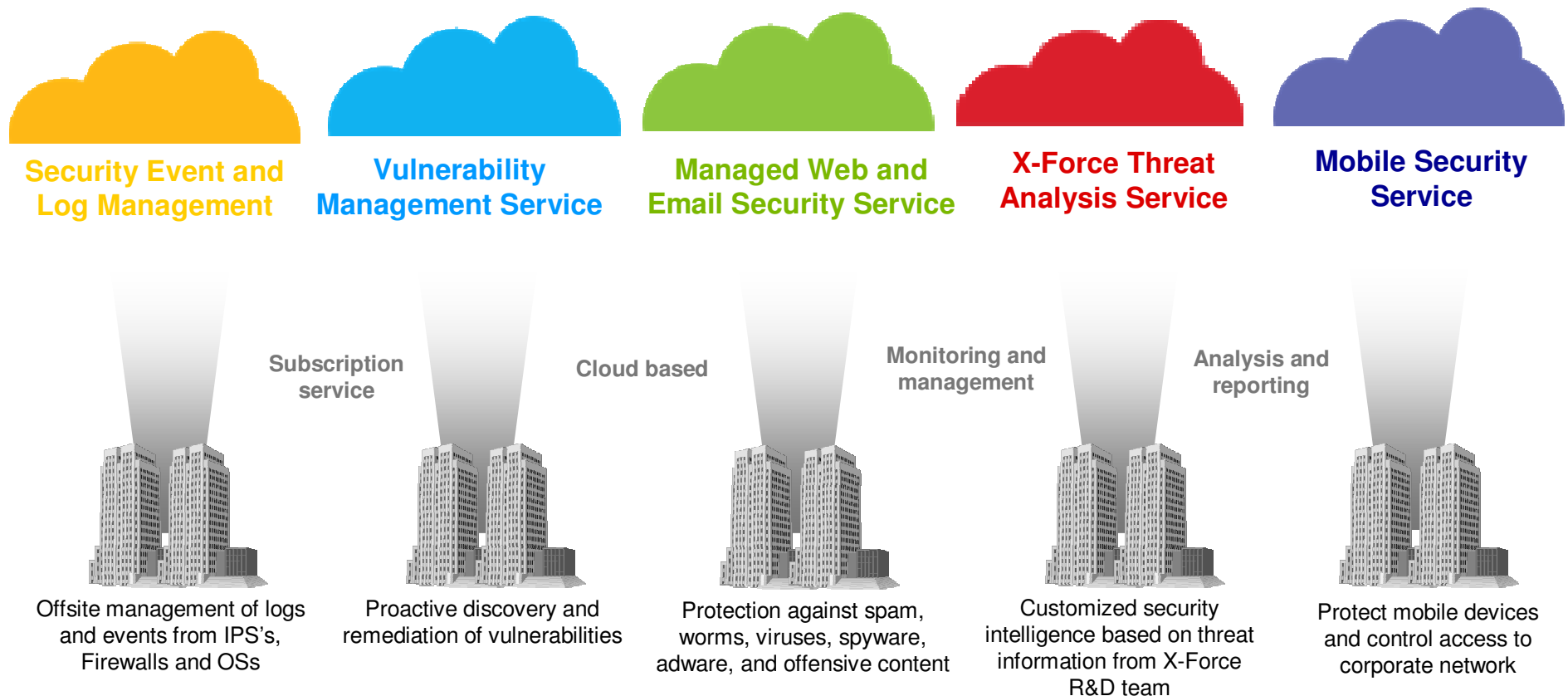


DEVICE MONITORING and CONTROL

- Application inventory and removal
- Monitor SMS, MMS, email message content
- View phone call log and address book/contacts
- View photos stored on device

Smart Business Security Services delivered from the IBM Cloud

From the Cloud – IBM Security Operations Centers



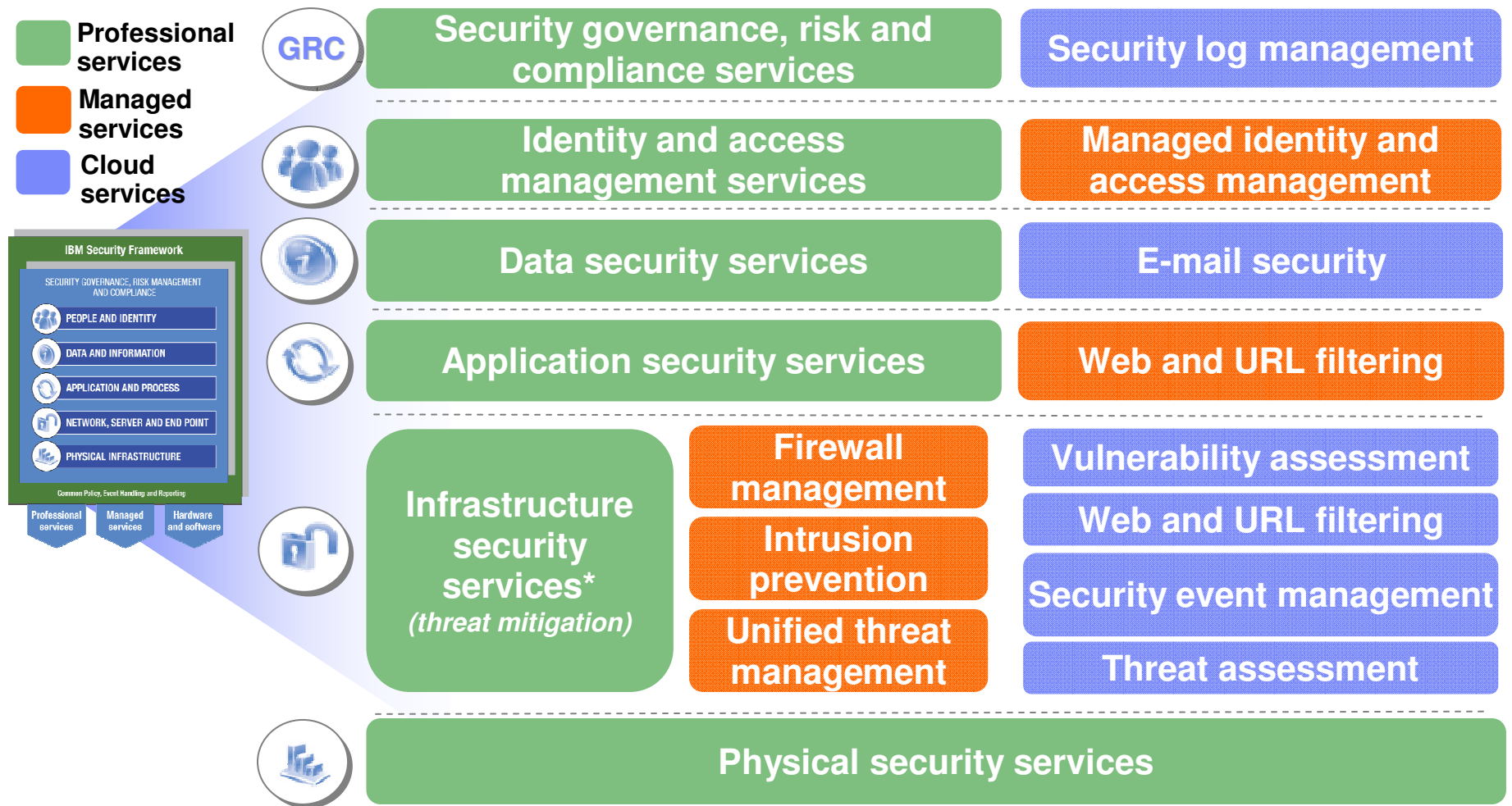
To the customer – Offering Security Tasks off the Ground

We offer a variety of services across all domains of the IBM Security Framework

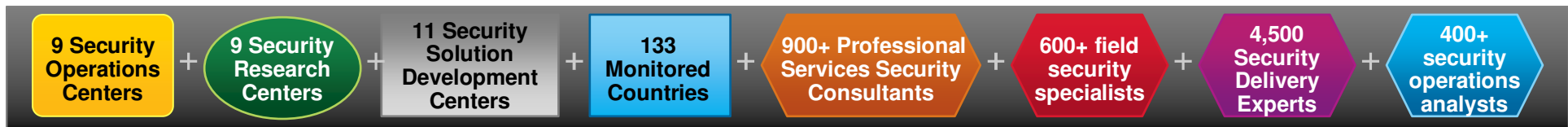
Our portfolio of services – summary view



IBM Security Services provides leading solutions across the IBM Security Framework



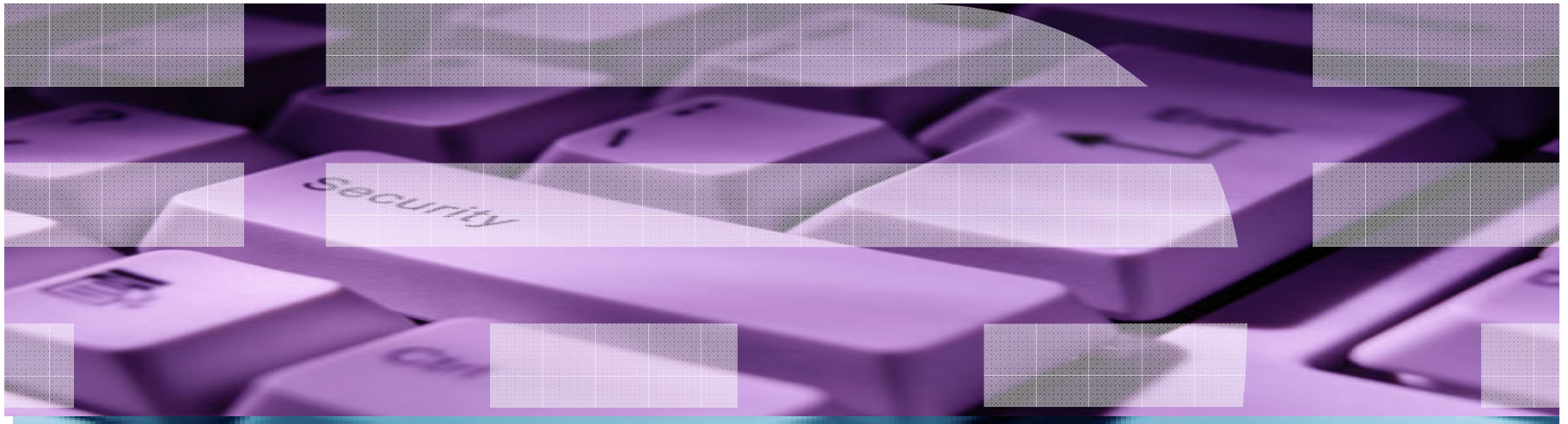
IBM has unmatched global and local expertise to deliver holistic security solutions across our entire portfolio



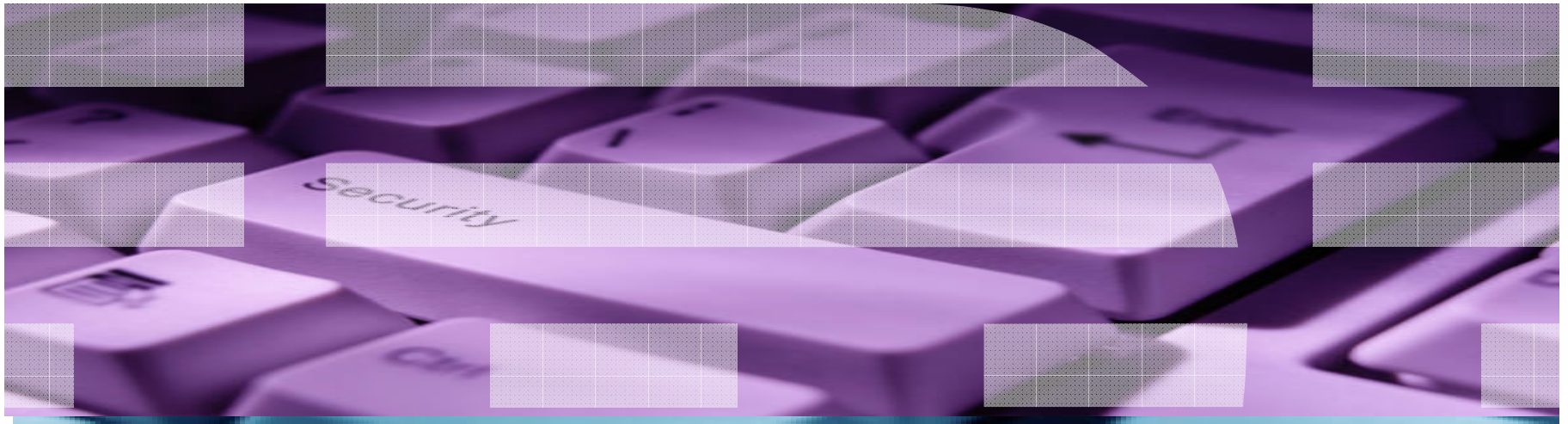
- 16 Acquisitions in security space
- 3,700+ MSS clients worldwide
- 13 Billion+ events managed daily
- World class security research

Question and Answer

Thank You



Standby Slides



Security from the Cloud

Smart Business Security Services delivered from the IBM Cloud

From the Cloud – IBM Security Operations Centers



**Security Event and
Log Management**



**Vulnerability
Management Service**



**Managed Web and
Email Security
Service**



**X-Force Threat
Analysis Service**

**Subscription
service**

Cloud based

**Monitoring and
management**

Offsite management of logs and
events from IPS's, Firewalls and OSs

Proactive discovery and
remediation of vulnerabilities

Protection against spam, worms,
viruses, spyware, adware, and
offensive content

Customized security
intelligence based on threat
information from X-Force
research and development
team

To the Customer – Offloading Security Tasks on the Ground



Secure applications

How can my business keep applications secure, protected from malicious or fraudulent use and hardened against failure?

Business challenges:

Reducing remediation costs	Discovering application vulnerabilities	Embedding application access controls
Vulnerabilities caught during the coding phase are 600x less expensive to fix than those caught after a product is released	The vast majority of new vulnerabilities emerge in applications, and 74% of these vulnerabilities have no patch available today	Up to 20% of application development costs can be for coding custom access controls and their corresponding infrastructure

IBM Services Offerings

- **Application security assessment**
- **Application source code security assessment**
- **Secure Web gateway**



Advantages

- Reduce risk of outage, defacement or data theft associated with web applications
- Assess and monitor enterprise-wide security policy compliance
- Improve compliance with industry standards and regulatory requirements (e.g., PCI, GLBA, HIPAA, FISMA...)
- Improve ability to integrate business critical applications



Manage Infrastructure Security

How can my business optimize service availability while mitigating risks?

Business challenges:

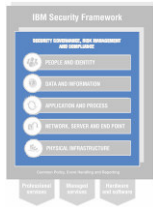
Determining which threats and vulnerabilities pose the most risk to systems and assets	Properly implementing controls at the network, server and endpoint to thwart attacks	Managing security costs
IBM X-Force analyzed over 1,600 vulnerabilities in Q3 2009 alone	Malicious/criminal attacks account for nearly a quarter of data breaches and are the most costly to the enterprise	Despite the economic downturn, 63% of CSOs expect security spending to increase or stay the same

IBM Services Offerings

- Penetration & Assessment
- Emergency Response service
- Deployment and Staff Augmentation
- Firewall Management
- Intrusion Prevention System management
- Managed protection services
- Unified threat management
- Security intelligence analyst
- Hosted e-mail and Web security
- Hosted vulnerability management
- IBM X-Force hosted threat analysis
- Hosted security and event log mgt

Advantages

- Identify and address security risks before they can impact business continuity, company assets or brand
- Establish controls that meet compliance requirements
- Reduce cost of ongoing security operations management
- Increased productivity by decreasing risk, malware infestation and incoming spam
- Simplified management for multiple security device types from many vendors



Managing risk and compliance

How can my business effectively manage risks and ensure compliance with all security regulations?

Business challenges:

Satisfying regulatory compliance requirements	Understanding and managing risk	Implementing appropriate policies and controls
The average enterprise is subject to hundreds of regulations which increasingly have “teeth” and most organizations lack of a single point of ownership and accountability	100% security does not exist – need to make the right trade offs	87% of breaches are avoidable through reasonable controls*

IBM Services Offerings

- Security policy planning and development
- Security risk assessment**
- Security health check**
- Information Security Framework
- Enterprise security architecture
- IBM Privacy services
- Payment Card Industry (PCI) security assessment**

Advantages

- Assesses compliance posture against a wide range of regulatory requirements and/or industry standards
- Makes appropriate trade-offs to align IT security with business objectives
- Enforces appropriate security level in each area in light of business opportunities, threats and vulnerabilities
- Develops the appropriate framework that can fully support the GRC initiative



Manage people and identities

How can my business lower the costs and mitigate the risks associated with managing user access to corporate resources?

Business challenges:

Reducing cost and complexity of managing identities	Providing secure and streamlined application access	Monitoring and reporting on user access
<ul style="list-style-type: none"> “It takes us 2 weeks to get new users set up on all systems” “80% of our helpdesk calls are password resets, at \$20 each” 	<p>“Each of our 400 applications has its own security access rules; it costs a fortune every time we need to change something”</p>	<p>“We are at risk of failing an audit because we can’t verify who has access to what and what our privileged users are doing”</p>

IBM Services Offerings

- **Identity Assessment and Strategy**
- User provisioning
- Web Access Management
- **Enterprise Single Sign-On**
- **User Activity Compliance Management**
- Managed Identity
- Total Authentication Solution

Advantages

- Reduces the cost, increases efficiency and enables audit-ability of user lifecycle management
- Decreases risk of internal fraud, data leakage, or operational outage
- Supports globalization of operations
- Enables shift to on-line services delivery for customers and partners across the globe
- Improves the end-user experience by providing faster access to information



Protect data and information

How can my business enable robust protection of critical data assets across key control points without impacting productivity

Business challenges:

Preventing unauthorized use of data and enforcing corporate security policies at the endpoints	Protecting data at rest, in motion and in use – on a growing number of endpoints	Preventing leakage of sensitive data across networks
82% of organizations in a recent study had more than one data breach in 2009 involving the loss or theft of more than 1,000 records	36% of data breaches are the result of a lost or stolen laptop or other mobile data-bearing device	The average cost of a data breach is \$6.7 million per breach, and the average cost for each compromised record is \$204 ¹

IBM Services Offerings

- Data security assessment
- Design and implementation services for:
 - Encryption
 - Network data loss prevention
 - Endpoint data loss prevention
 - Key and Certificate Management

Advantages

- Identifies key data security risks and assess key gaps in control points
- Protects data both on the network and at the endpoint with leading DLP technologies
- Provides controls to assure that data is not deliberately or inadvertently taken, leaked, or damaged
- Optimizes expenditures on protecting data while meeting audit and compliance mandates
- Improves protection of corporate data assets while not negatively impacting productivity