



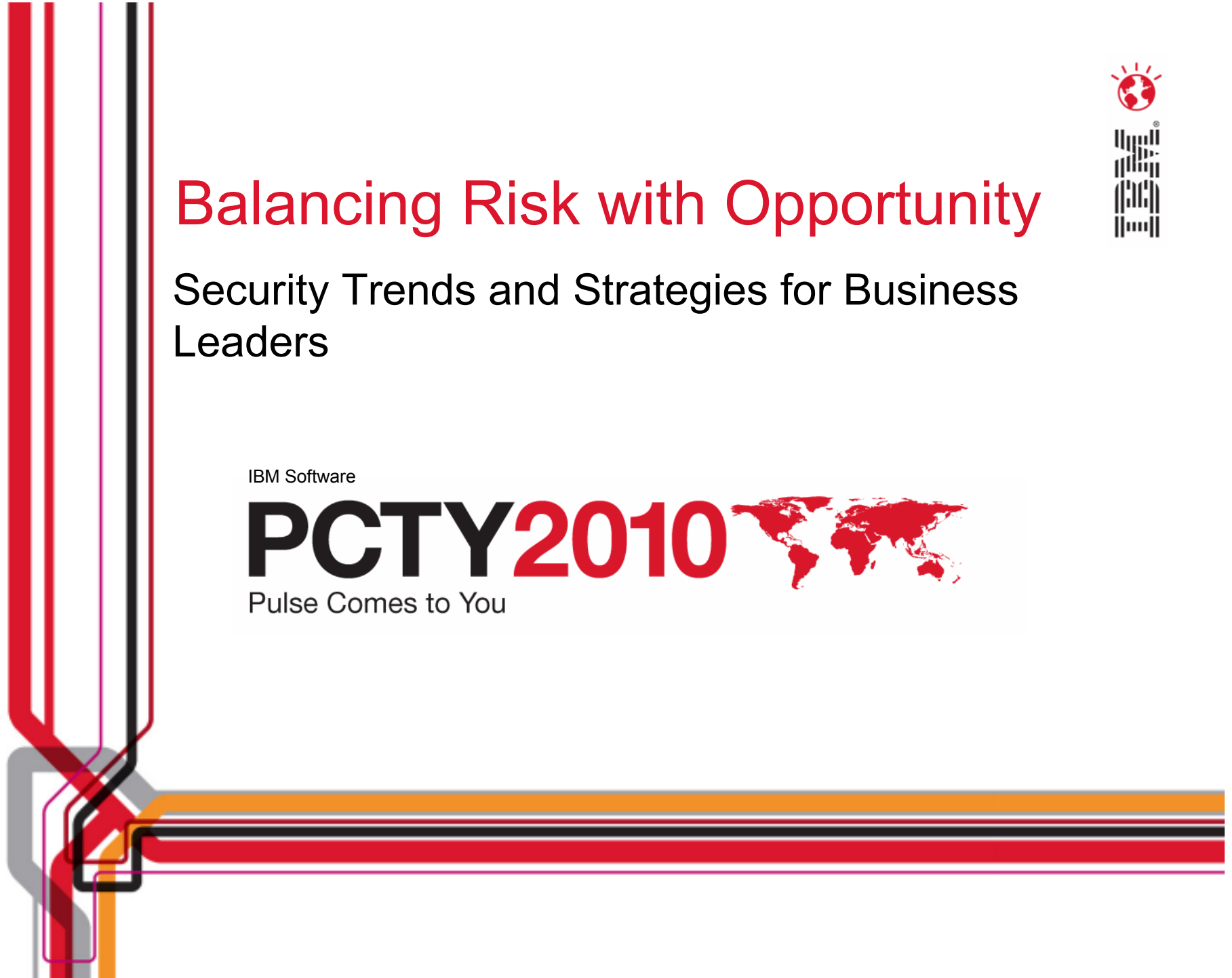
Balancing Risk with Opportunity

Security Trends and Strategies for Business Leaders

IBM Software

PCTY2010 

Pulse Comes to You





Agenda

- Typical security challenges
- Foundational Controls
- IBM Security Solutions
- Customer Casestudies
- Why IBM





Typical Challenges

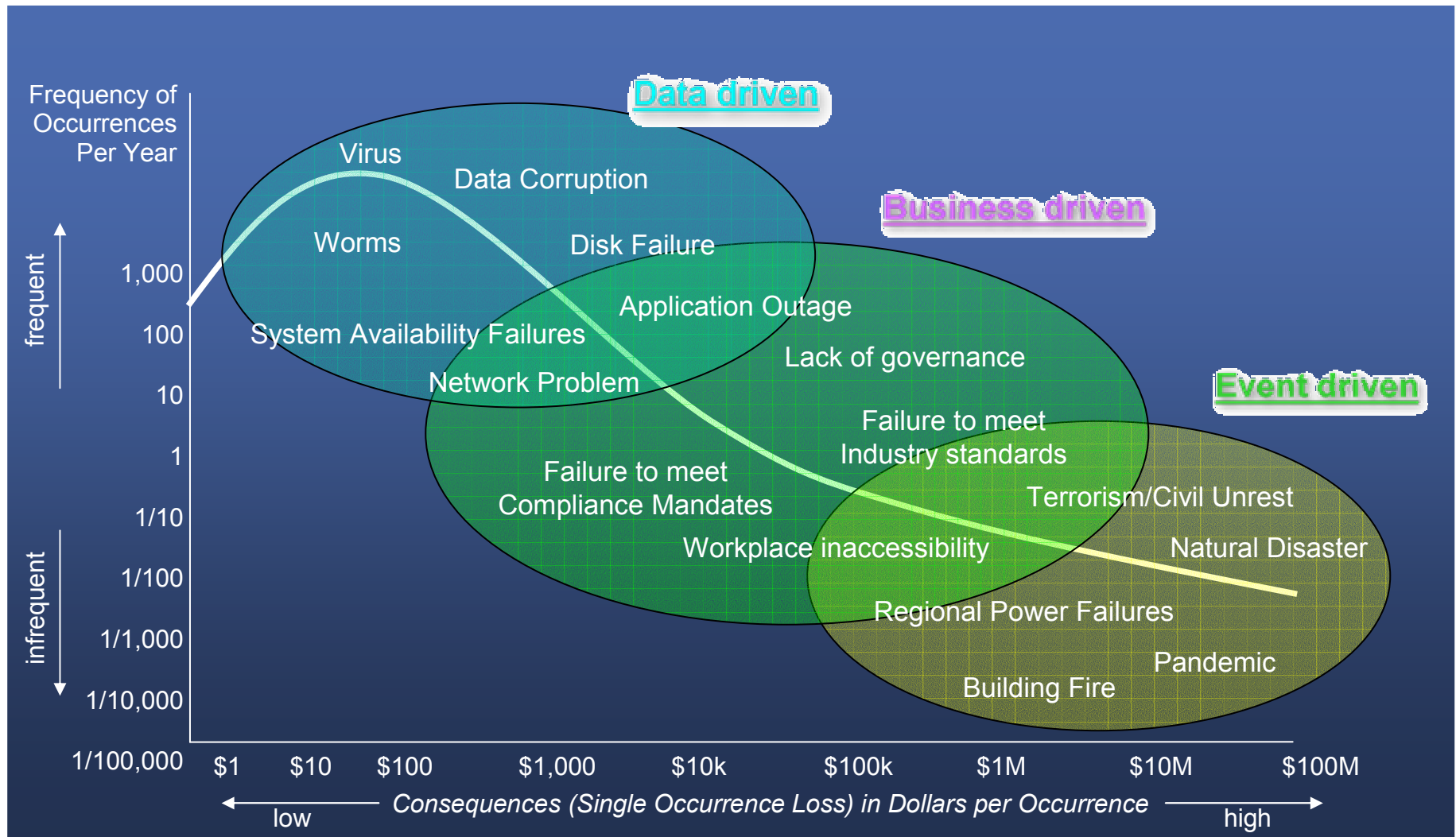


- **Data Security**
 - Can I ensure that sensitive data will not be compromised, exposed, or leak outside the company?
- **Identity & Access Management**
 - Can I certify that the system access controls work and only employees that should gain access to key systems are entitled?
- **Financial & Intellectual Property Theft**
 - Can the systems be safeguarded to prevent either financial abuses or intellectual property from being stolen?
- **Intrusion Detection & Prevention**
 - Are we vulnerable to hackers who may be mounting a denial of service or other type of intrusive attack?
- **Viruses & Worms**
 - Are all systems patched and protected against virus and other vulnerabilities to prevent an outbreak that will shut us down?
- **Regulatory Compliance**
 - Can I meet all the industry regulatory requirements and prevent a significant financial setback prevent the internal staff from if there is a security exposure?
- **Resilience, Recovery and Redundancy**
 - Can the company and the systems continue to operate in the event of a major catastrophe?
- **Application Security**
 - Can I compromise systems and prevent insider theft?
- **Physical Security**
 - Is the workplace safe and secure for employees & clients?





Not all risks are created equally





Increasing complexity



Death by
point
products



Interconnect, share
and protect
magnitude of data

15 petabytes of new information
are being generated every day. This
is **8x** more than the information in all
U.S. libraries



Confusion on
approach
Where to start?



Rapidly
changing
threat
environment

508% increase in the number of
new malicious Web links discovered
in the first half of 2009



Disruptive
technologies like
Virtualization and
Cloud Computing

80% Of enterprises consider security
the **#1** inhibitor to cloud adoptions

Source: IBM X-Force 2009 Mid-year Tre...



Rising costs

Today's CIOs spend 55% of their time on activities that spur innovation. The remaining 45% is spent primarily on cost reduction, managing risk and automation.*

Skills to deploy new technologies like Virtualization and Cloud computing are costly



IT departments have:

- Increasing responsibilities
- Time pressures
- Do more with less



Bulk of security budget is spent firefighting rather than innovating



Administrators and help desk resources are strained to support increasing base of users



Source: IBM Global CIO Study, 2009



Cost, complexity and compliance



Death by point products



Rising Costs: Do more with less



Regulation/Compliance fatigue

People are becoming more and more reliant on security

IBM believes that security is progressively viewed as every individual's right





“Foundational Controls” =

- Find a balance between effective security and **cost**
 - The axiom... never spend \$100 dollars on a fence to protect a \$10 horse
- Studies show the Pareto Principle (the 80-20 rule) applies to IT security*
 - 87% of breaches were considered avoidable through reasonable controls
- Small set of security controls provide a disproportionately high amount of coverage
 - Critical controls address risk at every layer of the enterprise
 - Organizations that use security controls have significantly higher performance*
- **Focus on building security into the fabric of the business**
 - “Bolt on” approaches after the fact are less effective and more expensive



*Sources: W.H. Baker, C.D. Hylender, J.A. Valentine, 2008 Data Breach Investigations Report, Verizon Business, June 2008
ITPI: IT Process Institute, EMA December 2008



The IBM security strategy: Make security, by design, an enabler of innovative change

Trusted Partner

*Delivering secure
products and services*

- **15,000** researchers, developers and SMEs on security initiatives
 - Data Security Steering Committee
 - Security Architecture Board
 - Secure Engineering Framework
- **3,000+** security & risk management patents
- Implemented **1000s** of security projects
- **40+** years of proven success securing the zSeries environment
- Managing **over 7 Billion** security events per day for clients
- **200+** security customer references and more than 50 published case studies

Trusted Security Vendor

*Providing end-to-end coverage
across all security domains*





Physical infrastructure



BUSINESS VALUE

Provide actionable intelligence and improve effectiveness of physical infrastructure security



	Video Surveillance	Video Analytics	Command and Control
Business challenge	Legacy analog video systems with proprietary interfaces are hard to integrate with IT infrastructure	Video information from many cameras present an information overload to human security personnel, detection is often after the fact and response management is problematic	IT and physical security operate in silos and do not integrate. It is increasingly difficult and expensive to consolidate security information across locations for effectiveness and compliance
Software	IT infrastructure, Logical Security products, and DVS partner products	Smart Vision Suite	Command Control Center Solution
Professional Services	Base Digital Video Surveillance Infrastructure services	Design, Implementation, Optimization services	Command Control Center Solution Services

This is not intended to be a comprehensive list of all IBM products and services



People and identity

BUSINESS VALUE

Lower costs and mitigate the risks associated with managing user access to corporate resources



	Cost and Complexity of Managing Identities	Providing Access to Applications	Auditing, reporting and managing access to resources
Business Challenge	<ul style="list-style-type: none"> On average, enterprises spend 2 weeks to setup new users on all systems and about 40% of accounts are invalid 30% of help desk calls are for password resets, at \$20 per call 	<p>“We would need to spend \$60k on each of our 400 applications to implement security access rules”</p> <p>– Global financial services firm</p>	<ul style="list-style-type: none"> Privileged users cause 87% of internal security incidents, while firms cannot effectively monitor thousands of security events generated each day Role management, recertification, etc.
Software	Tivoli® Identity and Access Assurance, Tivoli zSecure suite	Tivoli Access Manager, Tivoli Federated Identity Manager	Tivoli Identity and Access Assurance, Tivoli Security Information and Event Manager
Professional Services	Identity and Access Management Professional Services	Identity and Access Management Professional Services	Compliance Assessment Services, Privileged Identity Management
Managed Services	Managed Identity and Access Management	Managed Identity and Access Management	Managed User Monitoring and Log Management

This is not intended to be a comprehensive list of all IBM products and services



Data and information

BUSINESS VALUE

Understand, deploy and properly test controls for access to and usage of sensitive business data



	Protecting Critical Databases	Messaging Security and Content Filtering	Managing Data Access and Encryption	Monitoring Data Access and Preventing Data Loss
Business Challenge	Mitigate threats against databases from external attacks and internal privileged users	Spam and inappropriate Web sites pose major productivity drains, resource capacity strains, and leading attack vector for malware	Over 82% of firms have had more than one data breach in the past year involving loss or theft of 1,000+ records with personal information; cost of a data breach increased to \$204 per compromised customer record*	42% of all cases involved third-party mistakes and flubs... magnitude of breach events ranged from about 5,000 to 101,000 lost or stolen customer records*
Software	Guardium Database Monitoring & Protection	Multi-Function Security appliance, Lotus Protector	Tivoli® Key Lifecycle Manager, Tivoli Security Policy Manager, Tivoli Federated Identity Manager	Data Loss Prevention; Tivoli Security Information and Event Manager
Professional Services	Data Security Assessment Services	Data Security Assessment Services	Data Security, Compliance Assessment Services	Data Security, Compliance Assessment Services

This is not intended to be a comprehensive list of all IBM products and services

* "Fifth Annual U.S. Cost of Data Breach Study", Ponemon Institute, Jan 2010



Application and process

BUSINESS VALUE

Keep applications secure, protected from malicious or fraudulent use, and hardened against failure



	Security in App Development	Discovering App Vulnerabilities	Embedding App Access Controls	Providing SOA Security
Business Challenge	Vulnerabilities caught early in the development process are orders of magnitude cheaper to fix versus after the application is released	<ul style="list-style-type: none"> •74% of vulnerabilities in applications have no patch available today* •80% of development costs are spent identifying and correcting defects, costing \$25 during coding phase vs. \$16,000 in post-production** 	According to customers, up to 20% of their application development costs can be for coding custom access controls and their corresponding infrastructure	Establishing trust and high performance for services that span corporate boundaries is a top priority for SOA-based deployments
Software	Rational® AppScan®; Ounce	Rational AppScan; Ounce	Tivoli® Identity and Access Assurance	WebSphere® DataPower®; Tivoli Security Policy Manager
Professional Services	Secure App Dev Process Enablement, App Vulnerability and Source Code Scanning	App Vulnerability and Source Code Scanning	Application Access Services	
Managed Services		Managed Vulnerability Scanning	Managed Access Control	

* IBM X-Force Annual Report, Feb 2009

** Applied Software Measurement, Caper Jones, 1996

This is not intended to be a comprehensive list of all IBM products and services

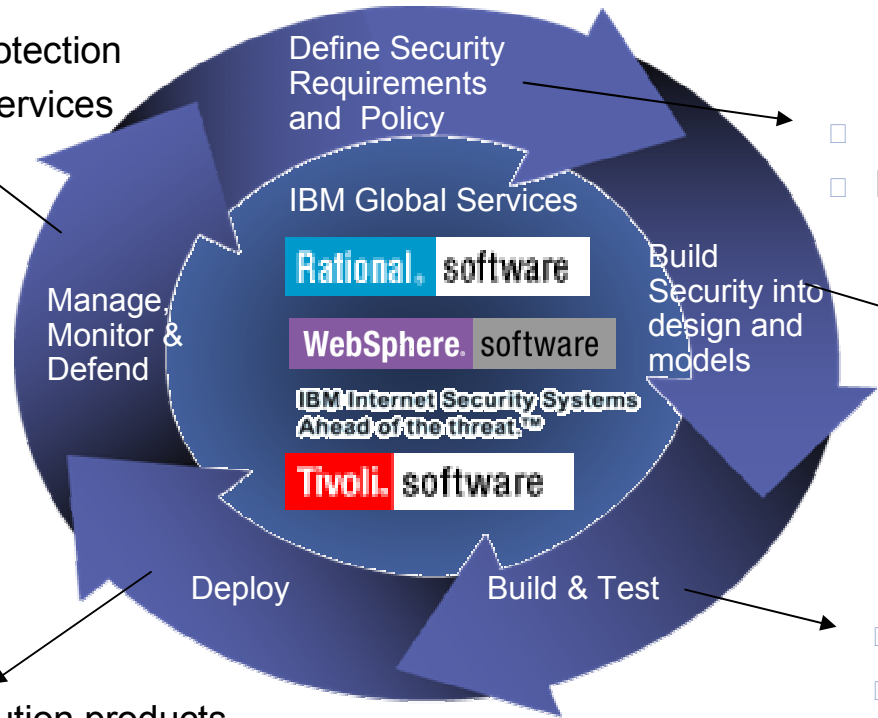


Application and Process

- 54% of all vulnerabilities disclosed in 1st half of 2008 were web-based*
- 75% of attacks are focused on applications**



- IBM ISS Intrusion protection
- IBM ISS Managed Services



- IBM ISS Consulting
- Rational Requirements Management
- Rational Application Developer
- Rational Software Architect
- WebSphere Business Modeller
- Rational Change Management
- Rational BuildForge
- Rational AppScan

- Tivoli distribution products



Integrated Security Throughout the Application Lifecycle



Network, server and end point

BUSINESS VALUE

Optimize service availability by mitigating risks while optimizing expertise, technology and process



	Protecting Servers	Protecting Endpoints	Protecting Networks	Protecting Mainframes
Business Challenge	Mitigate threats against servers; prevent data loss	Effective management can cut total cost of ownership for secured desktops by 42%*	Mitigate network based threats and prevent data loss	Mitigate threats against mainframes; protect against vulnerabilities from configuration; contain the privileged users
Software	Server Protection, Server Protection for VMWare	Desktop security platform; encryption	Network Intrusion Prevention System (IPS)	Tivoli® zSecure suite
Professional Services	Server security, data security assessment services	Desktop security, data security assessment services	Network security assessment services	
Managed Services	Managed IDS, Privileged User Mgmt	Managed Desktop security platform	Managed Network IPS	

* Gartner Desktop Total Cost of Ownership: 2008 Update, Jan 2008

This is not intended to be a comprehensive list of all IBM products and services

Addressing New Threats

Virtualization and Cloud



- Market-leading network protection now available on a virtual appliance
 - World class, vulnerability-based protection powered by X-Force research
 - Integrate virtual security with physical network protection
 - Runs on VMWare
- Segment-based network protection
 - Physical network segments
 - Virtual network segments
 - Cloud-based service providers
- Network protection with the speed of an appliance
 - Replacement for Real Secure Network Sensor
 - Upgrade to full Proventia protection
- Makes virtualized and cloud environments **REAL FOR BUSINESS**



Security governance, risk management and compliance

BUSINESS VALUE

Ensure comprehensive management of security activities and compliance with all security mandates



	Security Strategy Design	Pen Testing & Vuln. Assessment	Sec. Compliance Assessment	Incident Response
Business Challenge	Design and implement secure deployment strategies for advanced technologies such as Cloud, virtualization, etc.	Identify and eliminate security threats that enable attacks against systems, applications and devices	Perform security compliance assessments against PCI, ISO and other standards and regulations	Design and implement policy and processes for security governance, incident response; perform timely response and computer forensics
Software		Rational® AppScan®; Guardium Database Monitoring & Protection	Tivoli Security Information and Event Manager; Guardium Database Monitoring & Protection; Tivoli zSecure suite	Tivoli® Security Information and Event Manager; Tivoli zSecure suite
Professional Services	Consulting Services; Security Design	Ethical hacking and AppSec assessment	Qualified Security Assessors	Policy definition services; CERT team
Managed Services		App Vulnerability and Source Code Scanning OnDemand		Managed Protection Services

This is not intended to be a comprehensive list of all IBM products and services



We know how... Smarter security enabling client innovation



Banco Mercantil do Brasil

Automates access management, reduces the number of help desk calls by 30% with savings of 450K annually



DTCC

Improves the delivery of new insurance products and services and adds 225 new applications per year



Washington Metro Area Transit Authority

Level 1 merchant with 9 million transactions yearly protects consumer trust by shielding database infrastructure from internal and external threats



Gruppo Interga

Protects its network infrastructure from threats and ensures business continuity



Cognizant

Objectives of the Identity Management Journey @ Cognizant

- Improved user productivity, due to reduced wait for new and updated systems access and fewer authentication problems
- Lower security administration cost, as the bulk of user administration automated or delegated to business users and password resets eliminated or resolved with self-service
- Enhanced security, as inappropriate access terminated quickly and reliably
- Regulatory compliance, from the ability to audit access rights globally, and ensure that only appropriately authorized users have access to sensitive systems and data

na

ge

me

nt

Jo

urn

ey

Business Drivers

- **Cost Containment & Reduction**
 - Reductions in help desk call volumes
 - Reduced manual user intervention
- **Operational Efficiencies / Productivity**
 - Faster access setup for new hires
 - Reduced user down-time waiting for password resets
- **Security Improvements**
 - Immediate access de-activation for terminated / resigned staff
 - Elimination of over provisioning risks
 - Provision new accounts in compliance with standards

Benefits of the Identity Management Initiative at Cognizant

- Improved efficiency of system & application administrators
- Improved employee productivity by self service methodologies
- Improved compliance posture

Implementation Approach

Phase I

- User provisioning
- Password management & self-service
- Accountability

Phase II

- Role-based user-provisioning policies
- Identity management workflows – automated ID management process
- Automation of HRMS integration
- Extension to critical applications like MS Active Directory, MS Exchange, PeopleSoft, and Remedy





Bharti Airtel

bharti



Background

- Largest private-sector telco within ISA region
- Hyper-growth business; more than 100M in subscribers
- Undergoing major transformation in IT infrastructure

Challenges

- Enterprise level security controls across the large user population and heterogeneous application environment
- Scalability and performance to sustain the hyper-growth
- Security overhead for each application; uniformity in audit logging capabilities

IBM Solution

A centralized identity and access management framework for managing identities of Bharti's user community (employees, associates, partners, customers) and their access entitlements to Bharti's 750+ applications.

Benefits

- Secured, scalable, and highly available access management for all applications
- Enhanced employee and IT admin productivity (enhanced on-boarding experience; single login per user; expediated user provisioning from 2 days to 1 hour)
- Automation of IT operations (Automated user provisioning, instantenous password resets, re-certifications, audit logging)
- Uniform security control and audit reporting across the IT infrastructure.

Improving Governance with Password Management at leading telecom service

p

Business Impact	Before SSF	After SSF
Average number of ID's/PW per user	➤ 20 ID/user	1 ID/user Single Sign On
Time required for Password reset or Account Unlock	➤ 2 hour	0.1 hour Self Services/SMS
New employee's Email/User ID creation and Delivery to New employee	➤ 24 hour	1 hour
Time taken for getting account provisioned to each application	➤ 2 Days	1 hour Automatic Provisioning



Smart surveillance helped a large US metropolis to identify safety threats quickly and respond proactively



Value

- Helped increase patrolling of a convention center during a conference event
- Video analytics covered secondary sites, including more than 2 dozen hotels hosting conference attendees
- Surveillance solution identified a van parked by a hotel for more than 24 hours and alerted police to avoid a possible threat

Business Challenge

- Identify public safety threats before they happen
- Quickly respond to events with police, emergency medical services, and fire and rescue when needed

Solution

- IBM Smart Surveillance Solutions
- Delivers a broad set of surveillance tools – including video analytics and centralized monitoring – to help identify threats and quickly alert police, fire and rescue resources.

Physical Infrastructure





Why IBM? “Worldclass Research”



IBM researches and monitors latest threat trends with X-Force

IBM is dedicated to cybersecurity advancement



Institute Focus

- **Engage** in public-private collaboration
- **Address** and mitigate cybersecurity challenges
- **Provide** a forum for clients to better understand how recent IBM Research advances can help

www.ibm.com/federal/security


Provides Specific Analysis of:

- Vulnerabilities and exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

Most comprehensive vulnerability database in the world

- Entries date back to the 1990's

23

Click  for more information

Source: IBM X-Force Database, www.ibm.com/federal/security



Why IBM? Recent accolades

“IDC believes IBM has recognized this trend and has created comprehensive security packages that leverage various products to provide for multiple layers of security to customers.”

— Charles Kolodgy, IDC, March 2010

IBM and a few others can help any sized customer with security, regardless of whether they need help securing their business, implementing an enterprise security initiative, or fixing a big security problem.”

— Jon Oltsik, Enterprise Strategy Group, March 2010

In light of IBM’s growing presence in security and compliance, and the weight of its impact on the larger issues of business risk control, these factors should make IBM a primary partner to consider in shaping strategy and evaluating technologies and services that make a difference. Few others have the range of capabilities of today’s IBM for addressing the challenge—fewer still have the resources of an IBM for understanding the nature of business risks and emerging threats, and how best to address them going forward.”

High Performers and Foundational Controls: Building a Strategy for Security and Risk Management - Enterprise Management Associates® (EMA™), Dec 2009



IBM was named the
“Best Security Company”*
by SC Magazine

Source: SC Magazine award, March 2, 2010



Why IBM?

IBM has unmatched global and local expertise in security





IBM is your trusted partner...

Know how to ensure your success



Successfully implemented 1000s of client projects



Deliver value by understanding the big picture

Security across mainframes, desktops, networks, handheld devices



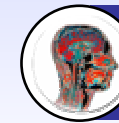
Help you to choose

Create the right solution for you



Ensure success by execution

Manage security for 400,000 IBM employees, 7B events/day for clients



Leverage our skills to meet your goals

1000s of researchers and SMEs



Expertise to meet your industry needs

Tailor solutions to meet your industry challenges



Client success stories to demonstrate results

Provided IT Security for 30+ yrs, 200 client references



Partnership with a huge ecosystem

Large business partner community

Delivering solutions that enable enterprises to be Secure by Design



Thank
You



Back Up Slides

IBM Software

PCTY2010 
Pulse Comes to You



Banco Mercantil do Brasil automates access management processes and increases employee productivity



Value

- Reduced the number of help desk calls by 30%, resulting in savings of at least \$450,000 USD annually
- Enabled HR managers to create and cancel user accounts in just 2 days instead of 7 – improving productivity
- Provided 3,200 employees with a single password, synchronized across several environments in 3 months

Business Challenge

- Automate access management processes for internal applications
- Increase agility
- Manage changes in business and increasing demands

Solution

- IBM's Identity Management solution
- Manages and controls access at a central point
 - Grants access based on roles
 - Ensures security of critical information
 - Increases productivity

People & Identity



MERCANTIL
DO BRASIL



“ We have already reduced from 7 days to 2 days the time it takes to provide employees with access to IT resources, including human resource processes, identifications and passwords. ”

— Jaime Roberto Pérez Herrera,
Technical Support Manager, Banco Mercantil do Brasil.



Community medical center improves patient information security to meet electronic data requirements (HIPAA)



Value

- Client satisfied the mandated electronic data requirements by required deadline (HIPAA)
- Physicians, nurses and administrators are spending less time logging onto and off applications
- Reduced operating costs enabling the medical center to focus more on patient care



People & Identity



Business Challenge

- Meet federal guidelines for HIPAA compliance
- Not impede staff convenience

Solution

- Access Manager for Single Sign On
- Secures access to new and legacy applications
- Delivers single sign on and sign off to users
- Easy to deploy with maximum flexibility

“The solution helped address issues in more than half of the HIPAA security standards, specifically addressing many access control and audit tracking issues.”

— George Vasquez



IBM X-Force

IBM Software

PCTY2010



Pulse Comes to You



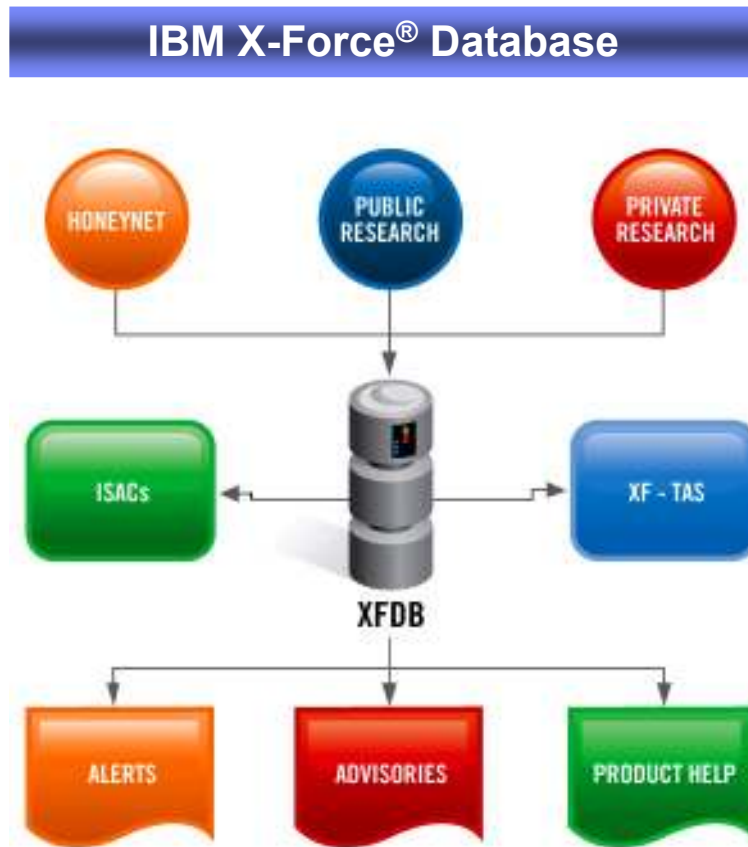
IBM X-Force Research and Development

- **What does it do?**
 - Researches and evaluates vulnerabilities and security issues
 - Develops assessment and countermeasure technology for IBM security offerings
 - Educates the public about emerging Internet threats

- **Why is it differentiating?**
 - One of the best-known commercial security research groups in the world
 - IBM X-Force maintains the most comprehensive vulnerability database in the world—dating back to the 1990s.
 - X-Force develops our Protocol Analysis Module which is the engine inside IBM Security solutions. This technology allows X-Force to regularly and automatically infuse new security intelligence into IBM Security offerings on average 341 days ahead of the latest threats.



IBM X-Force Database



Most comprehensive vulnerability database in the world

- Entries date back to the 1990's

Updated daily by a dedicated research team currently tracks over:

- 7,600 Vendors
- 17,000 Products
- 40,000 Versions



IBM Research

IBM Software

PCTY2010



Pulse Comes to You



Homomorphic Encryption facilitates analysis of encrypted information without sacrificing confidentiality



Analyze confidential electronic client data without seeing any private information

Store data anywhere while it remains completely secure and private



- ✓ *Service providers will be able to easily be able to adopt new models like cloud **Query a search engine without telling the engine what you are looking for!***



IBM continues to research and test new, more robust and more focused approaches to enterprise security



IBM is working with clients worldwide to implement the new **Enterprise Security Architecture**

- Combines:
IBM Methodology for Architecting Secure Solutions
Enterprise architecture framework of IBM Global Services Method
- The new architecture is defined around the concept of six security zones of control
(Boundary control, authentication, authorization, integrity services, audit/monitoring, and cryptographic services)





Advanced Risk Analytics is the key to future of IT Security



- Mine intelligence from logs and audit records from multitude of event sources
- Consolidate and correlate events and data at line speeds and present them to the analyst in a meaningful manner
- Put control back into the hands of decision makers, such as security analysts, by taking over repetitive and manual tasks



Advanced risk calculators to provide faster data processing rates at **15 to 20 times** the scale of today's model

Automatically creates and checks behavioral Models for malware detection at real time

Provides pre-fraud detectors with extremely low false positive rates

With these new opportunities come new risks



Emerging technology

- n Virtualization and cloud computing increase infrastructure complexity.
- n Applications are a vulnerable point for breaches and attack.

Data and information explosion

- n Data volumes are doubling every 18 months.
- n Storage, security, and discovery around information context is becoming increasingly important.

Wireless world

- n Mobile platforms are developing as new means of identification.
- n Security technology is many years behind the security used to protect PCs.

Supply chain

- n The chain is only as strong as the weakest link... partners need to shoulder their fair share of the load for compliance and the responsibility for failure.

Clients expect privacy

- n An assumption or expectation now exists to integrate security into the infrastructure, processes and applications.

Compliance fatigue

- n Organizations are trying to maintain a balance between investing in both the security and compliance postures.