Security, Risk Management and Compliance

2010 Track Kickoff

Pulse2010

The Premier Service Management Event

Scott Henley
IBM WW Security Tiger Team

Agenda

- Welcome
- State of security on the Smarter Planet
- A closer look at
  - Identity and Access Assurance
  - Data and Application Security
  - Data Center and Operational Security
- Security, Risk and Compliance at Pulse 2010

Security at Pulse 2010

- 29 security focused sessions across multiple tracks (security, midmarket, cloud, hot topics…)
- 30 of your peers – IBM customer speakers on security
- 8 security focused demos in the Expo Hall
- 45+ experts on hand to answer your questions
- 18 hands on labs

Since we last met at Pulse 2009…

500

Customers acquired through Ounce Labs and Guardium acquisitions

162

New client references with hundreds of new customers

2

Major security blueprints and guidance documents introduced to customer acclaim

126B

More events managed for customers annually

95

New product and services announcements and integrations

4924

New vulnerabilities protected against for customers

Why IBM?
IBM has a unique perspective on security.

Trusted Advisor	Security Company	Solution Provider	The Company
Helping customers build smarter cities, smarter grids, new data centers, trusted passport systems and more	A leading provider of software and services across a vast array of security product and services segments	A leading provider of software and hardware solutions around the world	400,000 employees across 130 countries with private data to protect

IBM Security Solutions

State of security on the smarter planet

The planet is getting
instrumented, interconnected and intelligent.

New possibilities.
New complexities.
New risks...

"We have seen more change in the last 10 years than in the previous 90."

Ad J. Scheepbouwer, CEO, KPN Telecom

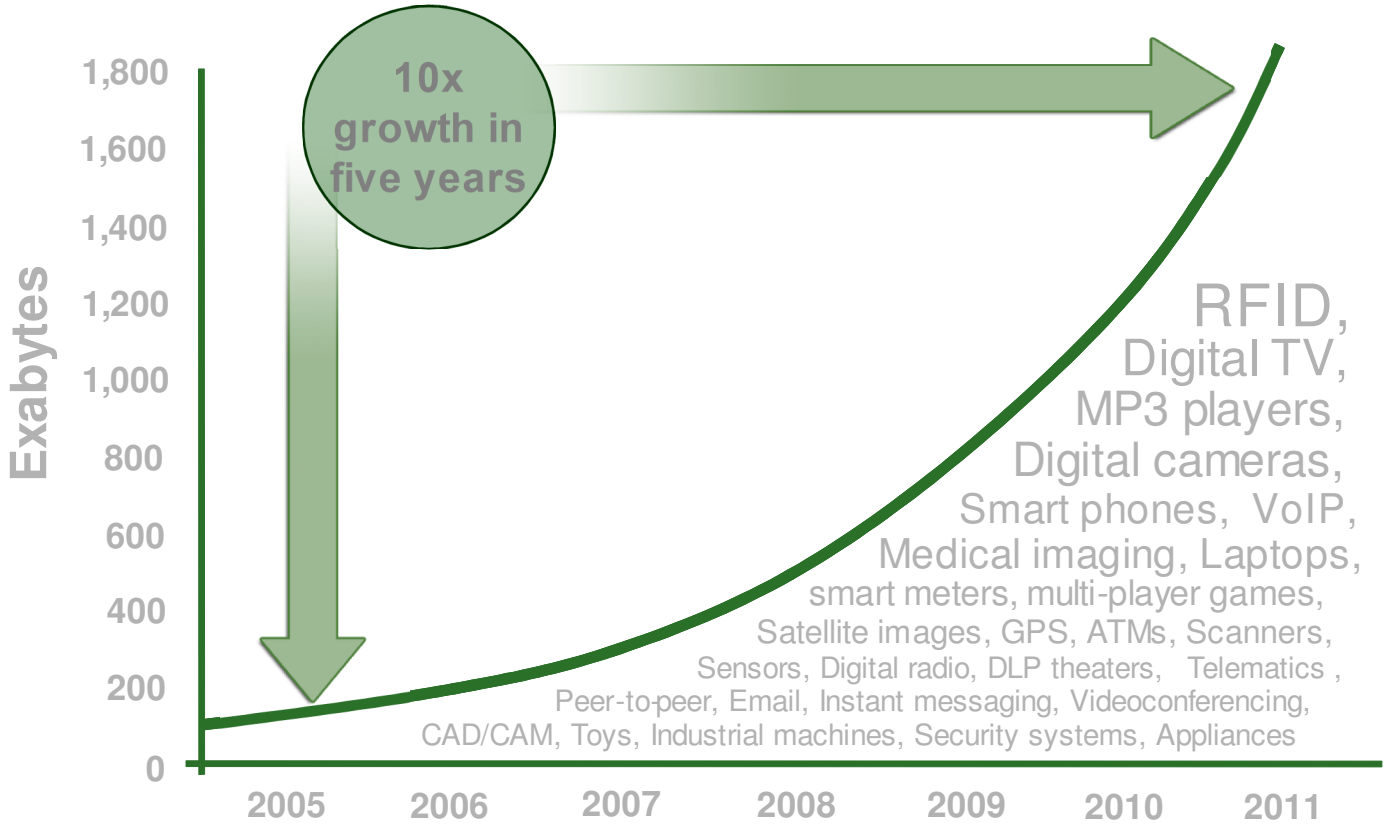
Critical Infrastructure Protection

Privacy and Identity

New and Emerging Threats

Cloud Security

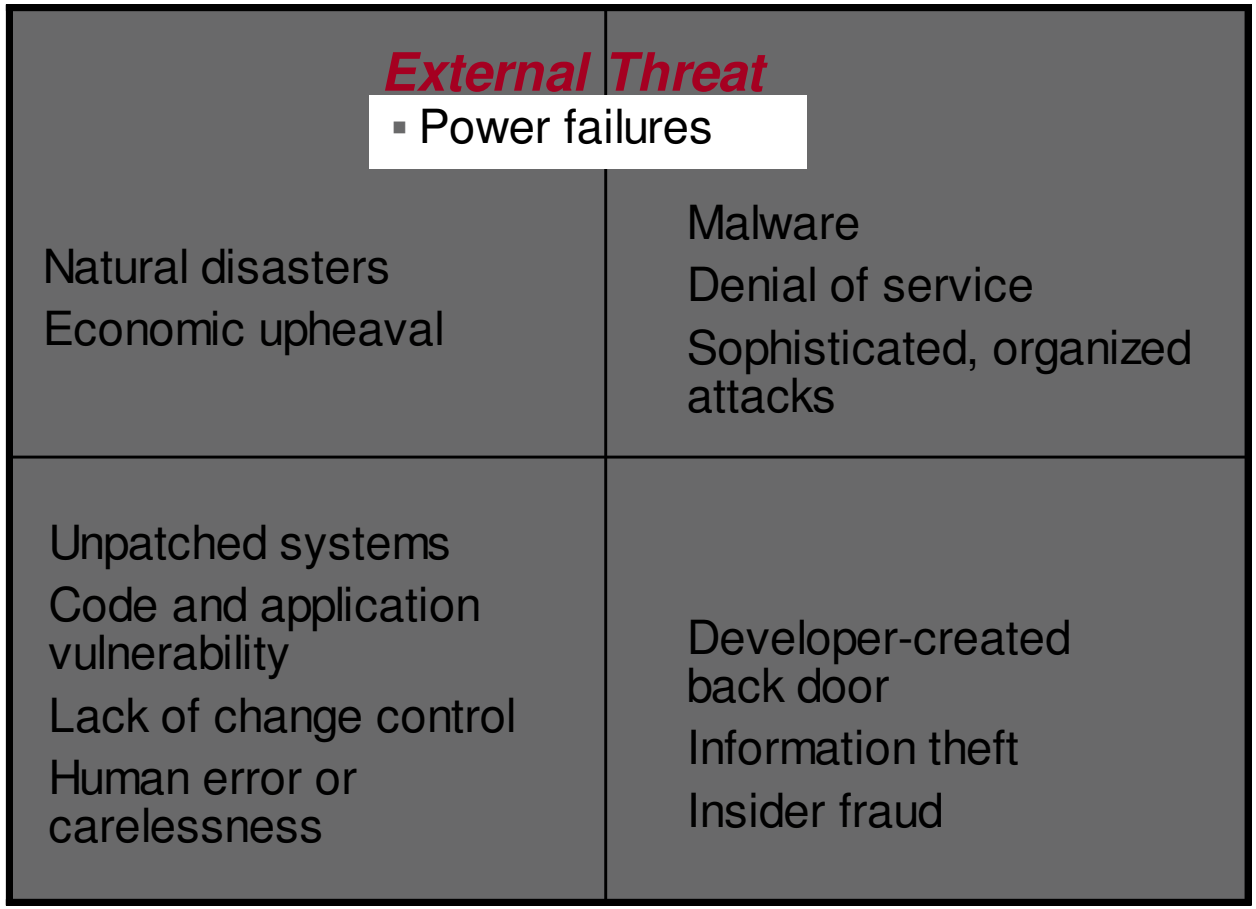
In just 5 years, the world will be 10x more instrumented. Internet connected devices will leap from 500M to 1 Trillion



Approximately 70% of the digital universe is created by individuals, **but enterprises are responsible for 85%** of the security, privacy, reliability, and compliance.*

* *"As the Economy Contracts, the Digital Universe Expands", IDC, May 2009*

There are simply too many scenarios to plan for…



Meanwhile, security is no longer an option, but a requirement…


Safety Belt Devised For Car

DESIGNED to hold passengers firmly in their seats in event of a crash so that they will not be thrown violently against the car interior, a newly developed safety belt for automobiles may eliminate injuries attributed to this cause.

"Modern Mechanix", Circa 1930s


Baby Goes for Car Rides in Homemade Armchair

NO CONVENTIONAL sling-type infant's chair for automobile use would satisfy the baby son of Lester Bresson, of Torrington, Conn., so Father constructed the armchair shown at the left. Made from odd bits of wood, strap iron, and discarded upholstery fabric, the chair rests on a column extending to the floor between the car's two front seats.

Chair rests on a column fastened to

- In 2010, regulations increasingly require "security by design"
- Analogous to the evolution of the safety standards within the automobile industry

Integrated Service Management provides Visibility. Control. Automation.™ across business infrastructure ….

Integrated Service Management

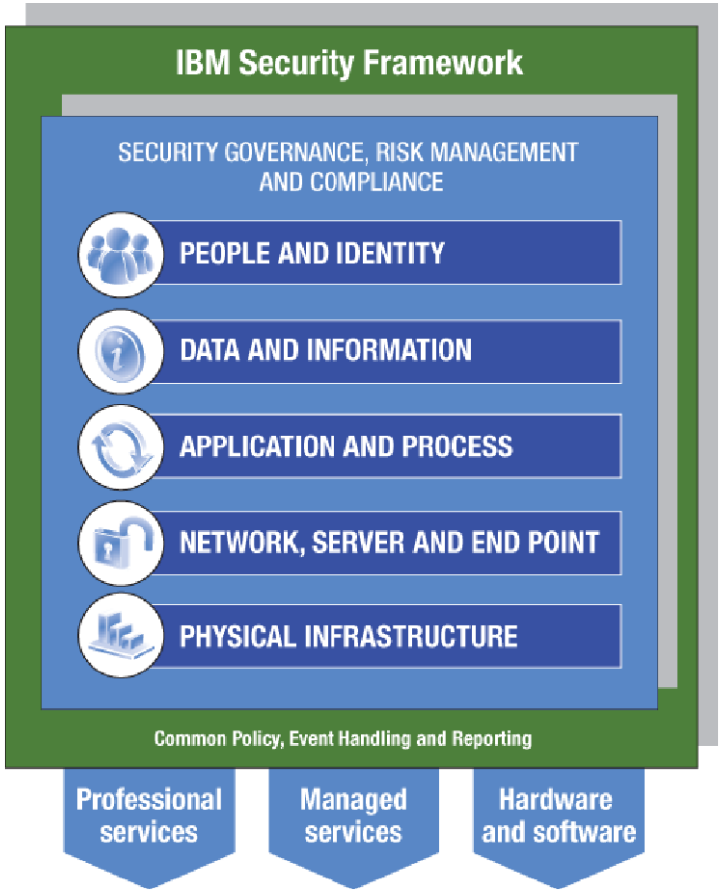
for Data Centers

Expertise and capabilities to assist clients with improving efficiency of IT Operations while improving effectiveness of the business services delivered and managed by IT from the next generation of data centers.

….to deliver innovative products and services to customers.

IBM takes a holistic approach to security **with** *end-to-end coverage* **of the security foundation.**

Improving service, managing risk and reducing cost



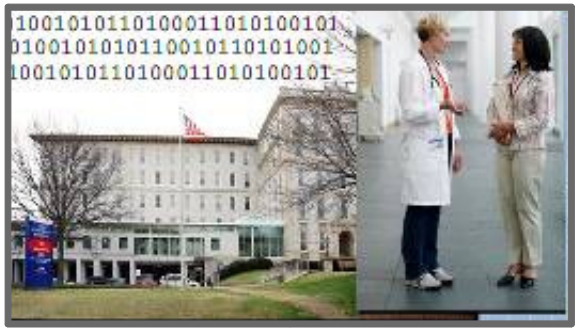
Smarter security: enabling client innovation

SMART is

Gruppo Intergea:

Reduced and prevented network downtime and improved continuity. Identified and blocked new, un-cataloged threats for superior performance

SMART is



Northwest Hospital and Medical Center:

Introduced RFID badge for physical and computer access for significant savings and increased efficiencies across hospital areas and departments. Eliminated the need to share passwords and leave machines and applications permanently logged on… meeting HIPAA requirements

SMART is

Reducing time to market for new secure services

DTCC:

Security features are designed and built into more than 225 new applications per year. Application developer productivity is improved and time to market for each new service is reduced

Why IBM?
IBM Research, X-Force

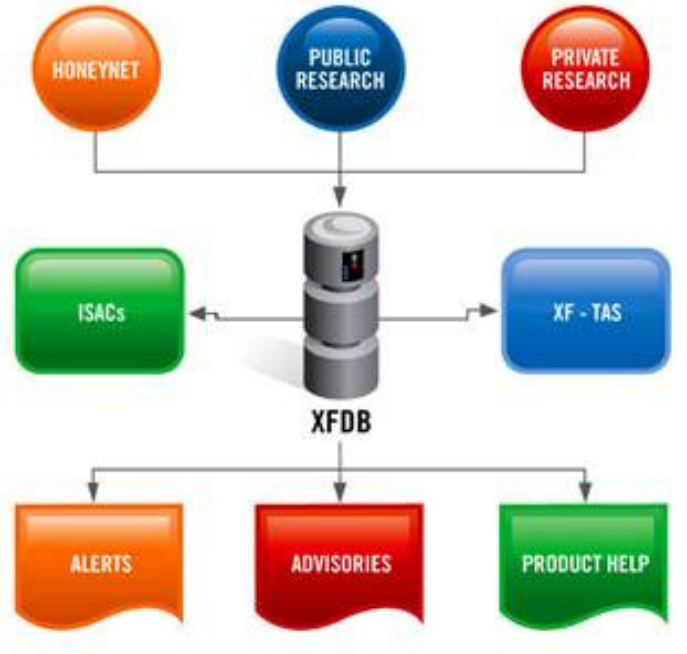
IBM Security Research

Provides Specific Analysis of:

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

Source: IBM X-Force Database

IBM X-Force® Database



Most comprehensive vulnerability database in the world

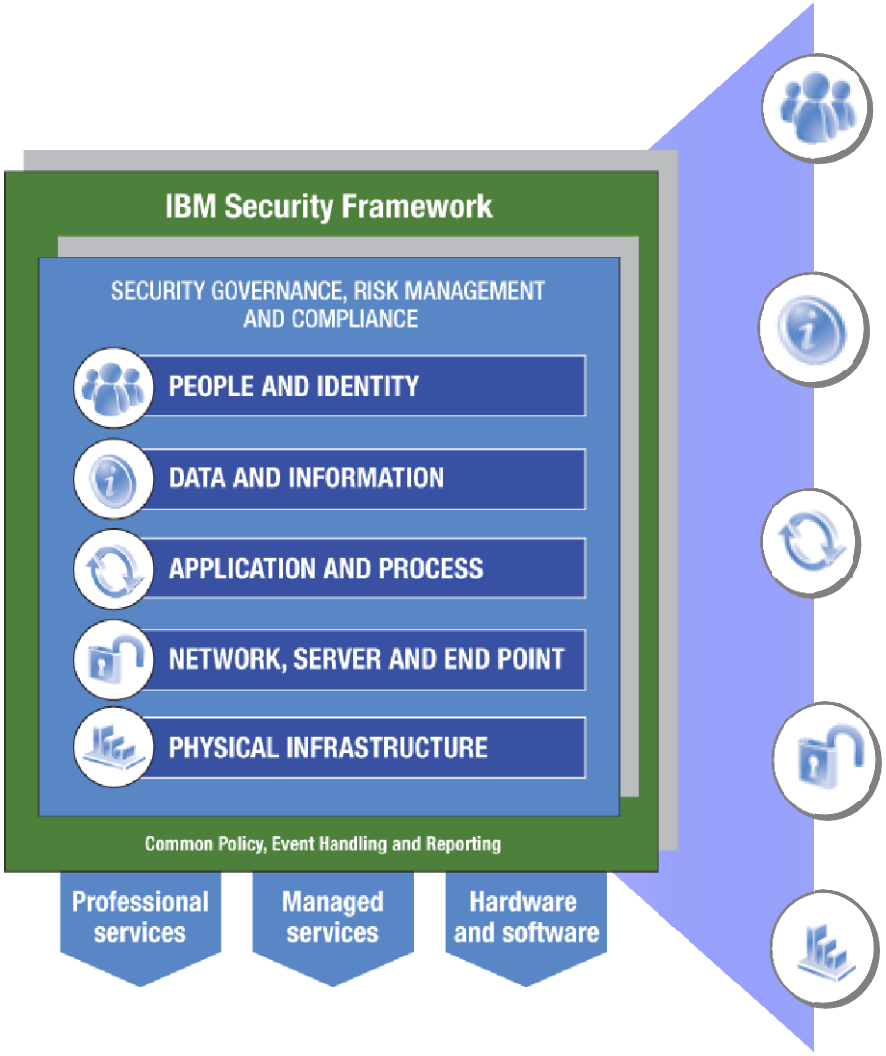
- Entries date back to the 1990's

Updated daily by a dedicated research team currently tracks over:

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

Meet the X-Force: Join the Birds of a Feather session Tuesday, 6pm in room 109!

IBM Security framework



Give the right users access to the right resources at the right time

Protect sensitive business data

Keep applications available and protected from malicious or fraudulent use.

Optimize service availability by mitigating risks

Provide actionable intelligence and improve effectiveness of physical infrastructure security

IBM Security portfolio

= Services

= Products

Security Governance and Compliance Services

Identity and Access Mgmt. Services

Identity Management

Access Management

Data Security Services

Data Loss Prevention

Messaging Security

E-mail Security

Encryption and Key Lifecycle Mgmt.

Database Monitoring and Protection

Data Masking

SIEM and Log Mgmt

Application Security Services

App Vulnerability Scanning

Web App Firewall

App Source Code Scanning

Access and Entitlement Mgmt.

SOA Security

Threat Assessment, Mitigation, and Mgmt. Services

Mainframe Security

Virtual System Security

Security Events and Logs

IPS

Physical Security Services

IBM Security Solutions

Improving service, managing risk and reducing cost of security without compromise

nd Access *t access for right people*

Applicatior *ty of business data and*

nd Operati *ating risks while optimizi*

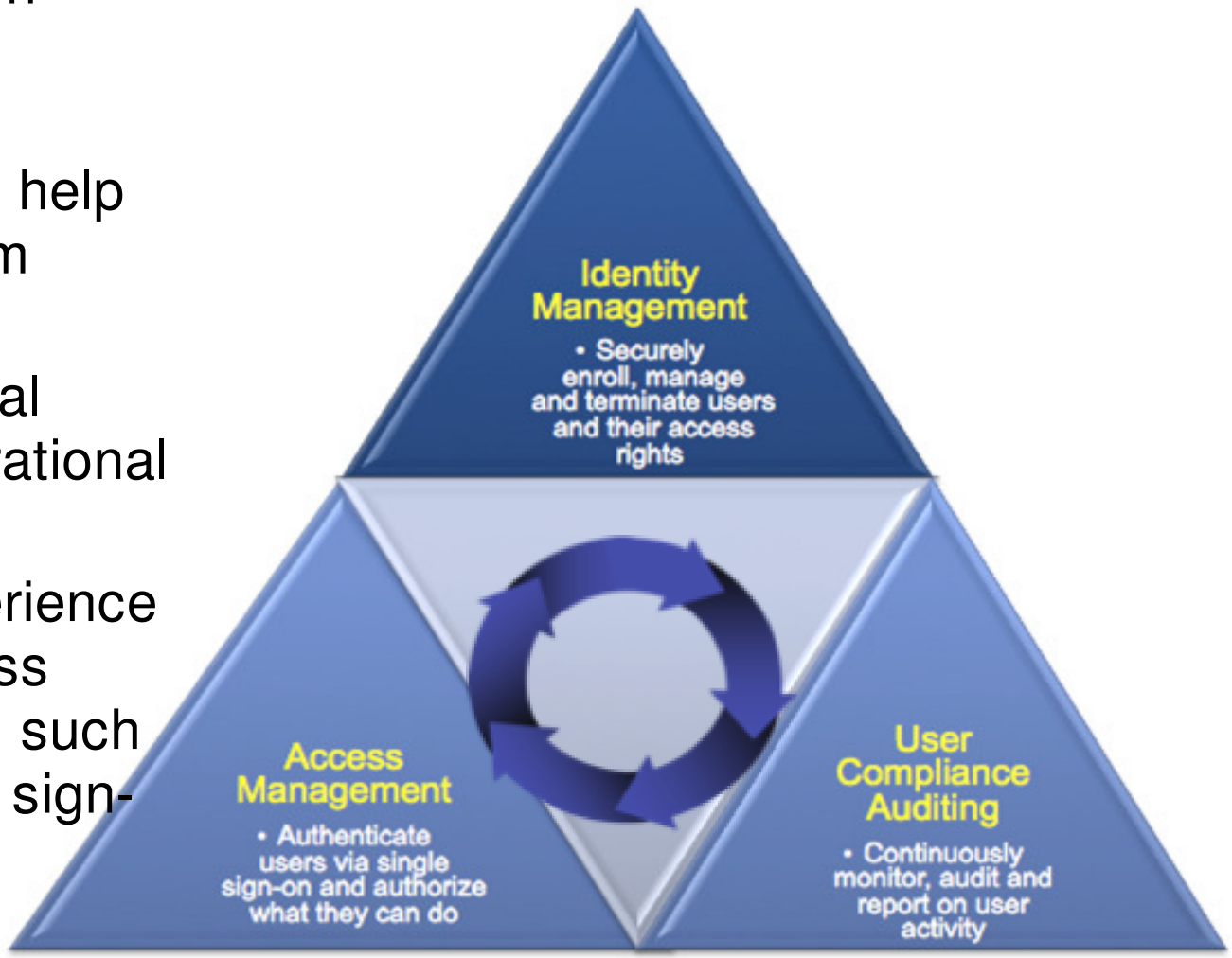
Information on new products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. Information on the new product is for informational purposes only and may not be incorporated into any contract. The information on new products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

The challenges of managing digital identities

- Dormant IDs or shared identities being used to inappropriately access resources
- Cost of administering users and identities in-house
- Privileged user activity unmonitored
- Meeting compliance requirements, responding to audits

Implementing identity and access management can address these challenges and drive positive results

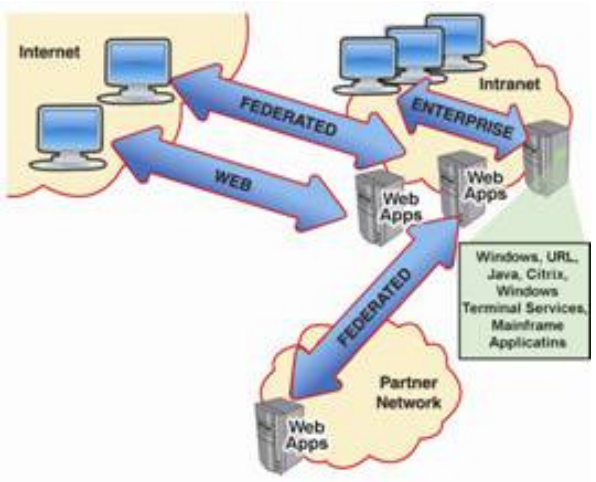
- Can reduce the time to onboard and de-provision identities from weeks to minutes
- Can significantly reduce help desk costs resulting from password reset calls
- Decreases risk of internal fraud, data leak, or operational outage
- Improves end-user experience with Web-based business applications by enabling such activities such as single sign-on



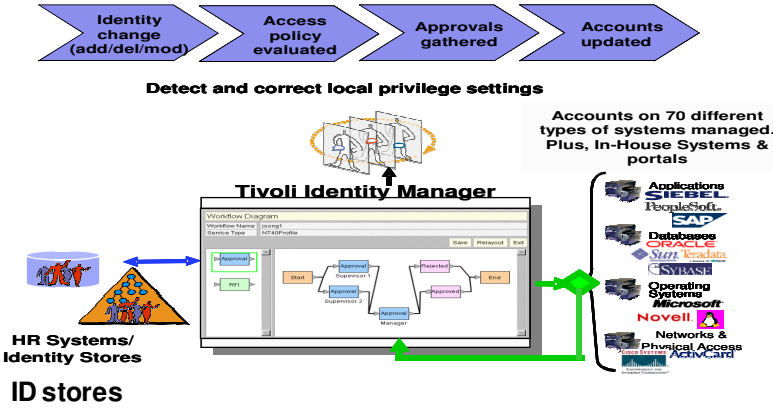
Getting started with Identity and Access Assurance

Single Sign On

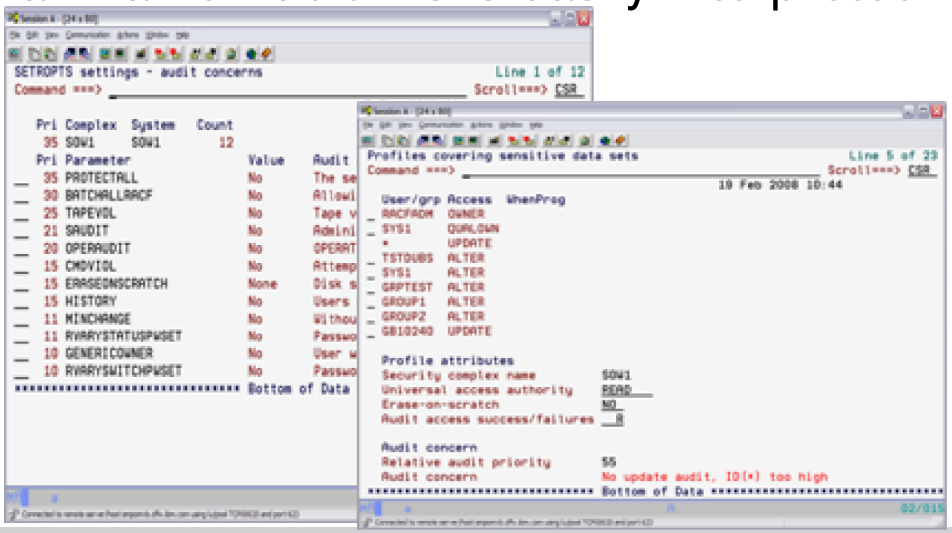
& Password Management



User Provisioning / Role Management



Mainframe Audit Risks easily interpreted



Security log management storage & reporting

IBM Identity and Access Assurance

Strategy:

Increase the value that customers realize by extending the identity context to application, data and threat management

Innovation and Integration Focus Areas

- Expand IAM Governance Capabilities
- Decreased operational costs
- Further enable System z to serve as the enterprise security hub

Market Drivers

- Simplification
- Compliance
- Virtualization
- Application and Data Protection

Challenges of protecting data and applications

- Data disclosure and privacy compliance
- Number and complexity of controls that need to be integrated within the enterprise
- Costs of data breaches, notification, brand value
- Managing data availability to the right people, at the right time
- Application security and agility
- Protecting Intellectual Property, data-in-use
- Securing data-at-rest

A solid data and application security strategy will span people, processes and technology

Centralized key management

- Inter-organization data collaboration
- Centralized, fine-grained access control to information
- Audit and reporting of data usage
- Security log management
- Centralized server administration integrity, including virtual servers
- Application and database security

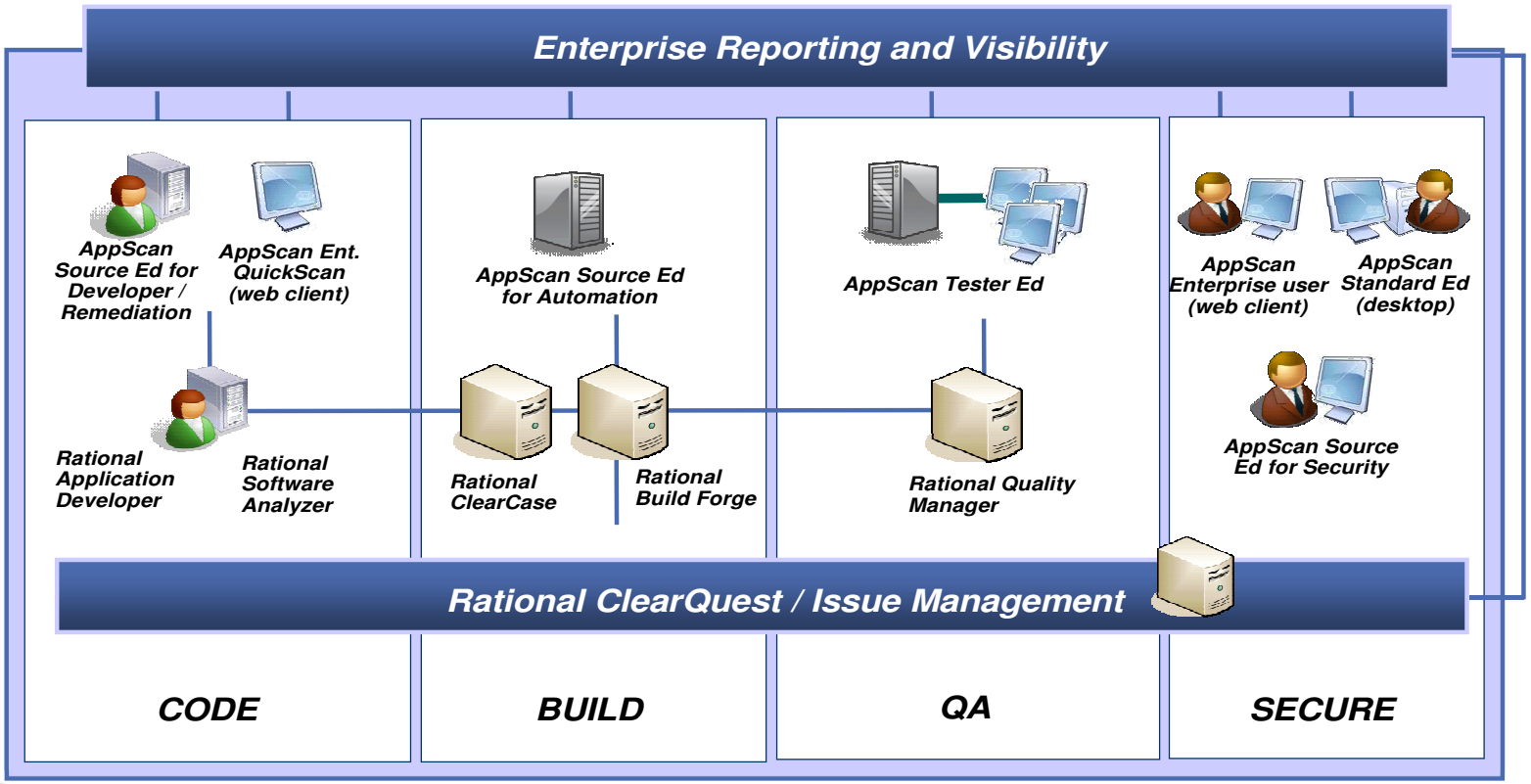
IBM has acquired Guardium a market leader in safeguarding databases and protecting critical enterprise data.

- IBM's acquisition of Guardium enables our clients to maintain trusted information infrastructures by monitoring and protecting high-value enterprise databases.

- Solution: Guardium Real-Time Database Monitoring Platform
  - Real-time, automated, cross-DBMS, monitoring and auditing platform
  - Secures and protects high-value databases, identifies application-layer fraud
  - Enables consistent enforcement of governance policies; demonstrates compliance
  - Lowers compliance costs and effort compared to traditional DBMS-resident auditing, with no impact on existing business processes

Ounce Labs acquisition expands the operationalization of security testing

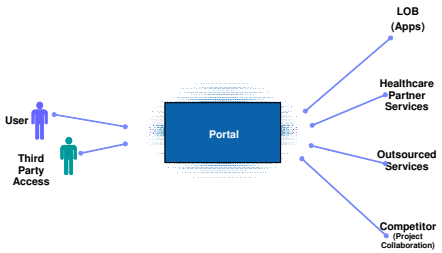
- By combining Ounce Labs source code testing with IBM Rational AppScan's application security testing IBM is the only provider of a true end-to-end application security solution for managing security compliance across all stages of the development process – from coding to production.



Getting started with Data and Application Security

Portal Security and Federation

- New revenue from partner services
- Rapid post-merger integration
- Cloud access control
- Unify J2EE and .Net

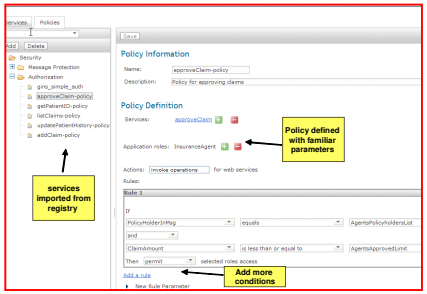


Data Privacy Compliance

- Detect PII leakage in your network
- Block inappropriate Web and mail content
- Protect against known/ *unknown* Web attacks

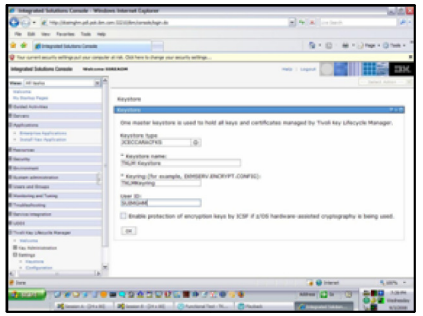
SharePoint / DataPower Management

- Essential when multiple DataPower / SharePoint installs per client
- Centralized, consistent policy management
- Supports compliance and app availability



Storage Encryption Key Management

- Cost effective, low OPEX solution for PCI and encryption laws
- Ensure availability of keys through lifecycle
- Manage Tape & Disk



How can you protect data access from your business critical applications and services?

The business *requirement* is to protect access and disclosure of client and customer PII
(e.g. Credit cards, SSNs, Patient)Records, Financial Results

Security Officer
Corporate Intranet

Security Architect
Internal Tool

Translates it as need to encrypt that information in all services using message security *policy*

App Owner
Eclipse

Translates and code it as application specific data entitlement *policy*

IT Operations
IAM Console

Translates and code it as configurations and tool-specific access *policy*

How can customers demonstrate compliance back to the business?

You can centrally manage and enforce data access using Tivoli Security Policy Manager without having to modify the applications

The business *requirement* is to protect access and disclosure of client and customer PII
(e.g. Credit cards, SSNs, Patient)Records, Financial Results

Security Officer
Corporate Intranet

Security Architect

App Owner

IT Operations

Policy Design Tool

Tivoli Security Policy Manager

Databases (DB2, Oracle)

Java, .NET Apps (e.g. Portal)

Content Managers (e.g. FileNet, SharePoint)

Demonstrate Compliance and Drive Data & Application Security

Demo of Tivoli Security Policy Manager

And if you like what you see here…

come see us in the Expo Hall in the Security Zone to learn more!

IBM Data and Application Security

Strategy:

Deliver innovative, integrated new solutions to address critical compliance and data protection challenges

Innovation and Integration Focus Areas

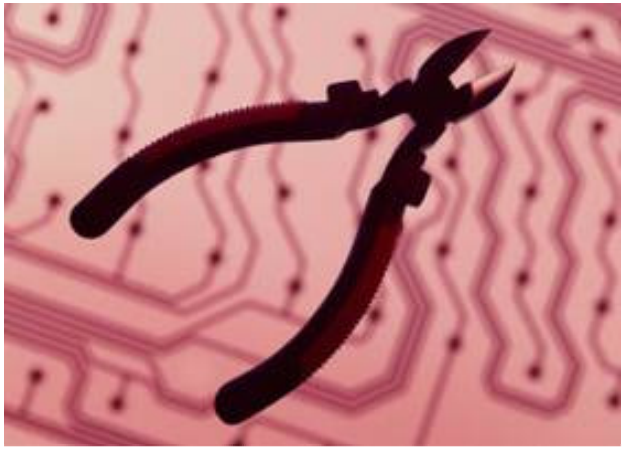
- Content Aware Access Control
- Application Security / Content Control
- End-to-End Compliance Visibility
- Standards Leadership

Market Drivers

Simplification	Compliance	Cloud / Web 2.0	Application and Data Protection

The threat landscape is continuously evolving. It is a challenge for an enterprise to keep up…

- Poor understanding of risks in new technologies and applications, including virtualization and cloud
- Parasitic, stealthier damaging attacks
- Inability to establish forensic evidence
- Undetected breaches due to privilege access misuse and downtime from incidents
- Compounding cost of managing an ever increasing array of security technologies



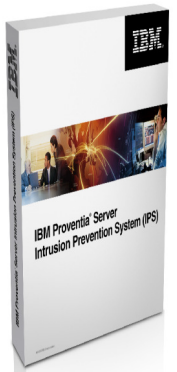
Data Center and Operational Security

- Improves service availability and supports performance against SLAs
- Reduces cost of ongoing management of security operations
- Increases productivity by decreasing risk of virus, worm, malcode, spam infestation
- Drill down on specific violations to quickly address resolution

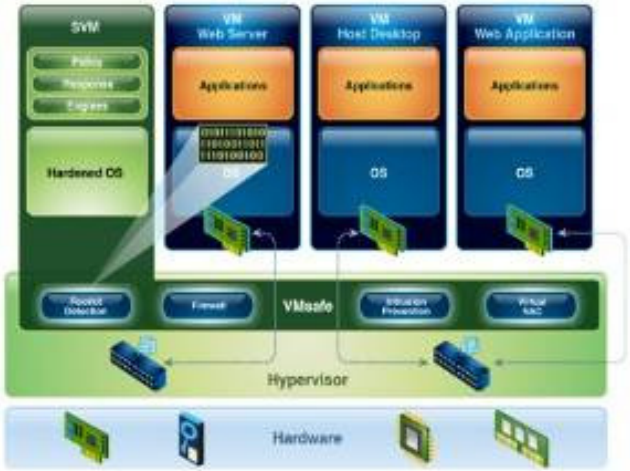
Getting started with Data Center and Operational Security

Network

Server



Virtualization



Security event, log mgmt and reporting

Data Center and Operational Security

Network Protection

IBM Security Network IPS
IBM Security Network IPS Virtual Appliance

Unified Threat Management

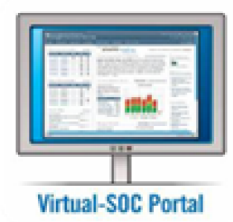
IBM Security Network Multi-Function

Virtual Infrastructure Protection

IBM Security Virtual Server Protection for VMware

Server Protection

IBM Security Server and Server Sensor



Security Management

Managed Security Services

IBM Security SiteProtector

Products
Value add for Cloud Providers

Network Threat Protection

Prevent unauthorized intrusions from internal and external sources

Vulnerability Management

Reduce risks by accurately identifying, prioritizing, tracking and reporting cloud infrastructure vulnerabilities

Server and Virtualization Security

Multi-layered protection designed to keep cloud data and applications secure

Managed Security Services

Real-time security management including system monitoring, emergency response and 24/7 guaranteed protection

Network Intrusion Prevention

Strategy:

Network Intrusion Prevention System (IPS) remains a key "anchor point" for the IBM security portfolio. Use this control point to deliver new capabilities.

Innovation and Integration Focus areas

- Development Of High Performance / Extended Feature Set
- Datacenter Content Expansion

Market Drivers

- Simplification
- More Security Functions
- Threat Protection
- Application and Data Protection

Endpoint (Server) Intrusion Prevention

Strategy:

Server security is a key “anchor point” for IBM security. IBM will deliver a converged Server agent for compliance, configuration management and threat protection

Innovation and Integration Focus Areas

- **Data Center Security**
- **Product Integration and Broad Platform Support**
- **Virtualization**

Market Drivers

- Compliance
- Threat & Operations Coverage
- Broad Platform Support

IBM Security Virtual Server Protection

Strategy:

Use virtual server security to address the security and compliance barriers that prevent clients from adopting virtualization and cloud computing

Innovation and Integration Focus Areas

- Expand Feature Set of Virtual Server Protection for Vmware®
- Virtual Environments, Servers and Applications are an "Anchor Point" for Security

Market Drivers

- Threat & Operations Unification
- Server Lifecycle Management
- Threat Protection
- Compliance

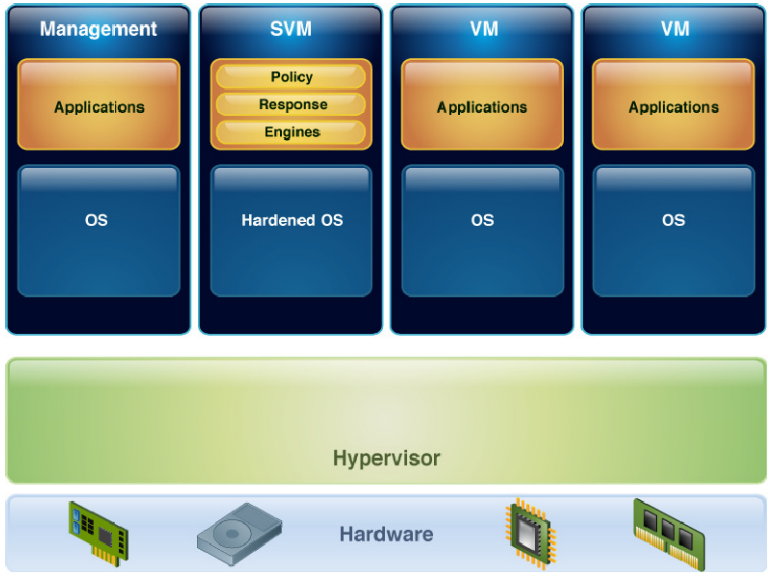
Security Challenges with Virtualization: New Complexities

- **New complexities**
  - Dynamic relocation of VMs
  - Increased infrastructure layers to manage and protect
  - Multiple operating systems and applications per server
  - Elimination of physical boundaries between systems
  - Manually tracking software and configurations of VMs

Before Virtualization

- 1:1 ratio of OSs and applications per server

After Virtualization



- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure

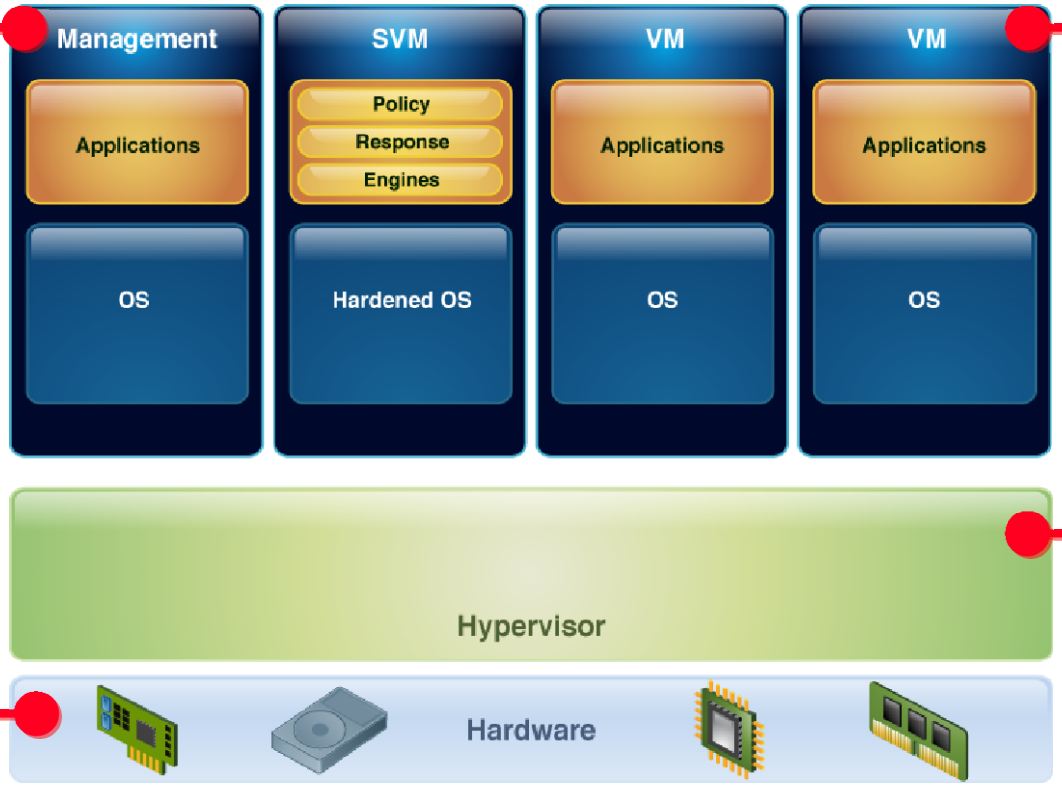
Three reasons why virtualization infrastructure protection is important

Need	How IBM Security Virtual Server Protection for VMware® helps	
Mitigate new risks and complexities introduced by Virtualization		Provides dynamic protection for every layer of the virtual infrastructure
Maintain compliance standards and regulations		Helps meet regulatory compliance by providing security and reporting functionality customized for the virtual infrastructure
Drive operational efficiency		Increases ROI of the virtual infrastructure

Security Challenges with Virtualization: New Risks

Management Vulnerabilities

Secure storage of VMs and the management data



Virtual sprawl

Dynamic relocation

VM stealing

Resource sharing

Single point of failure

Stealth rootkits in hardware now possible

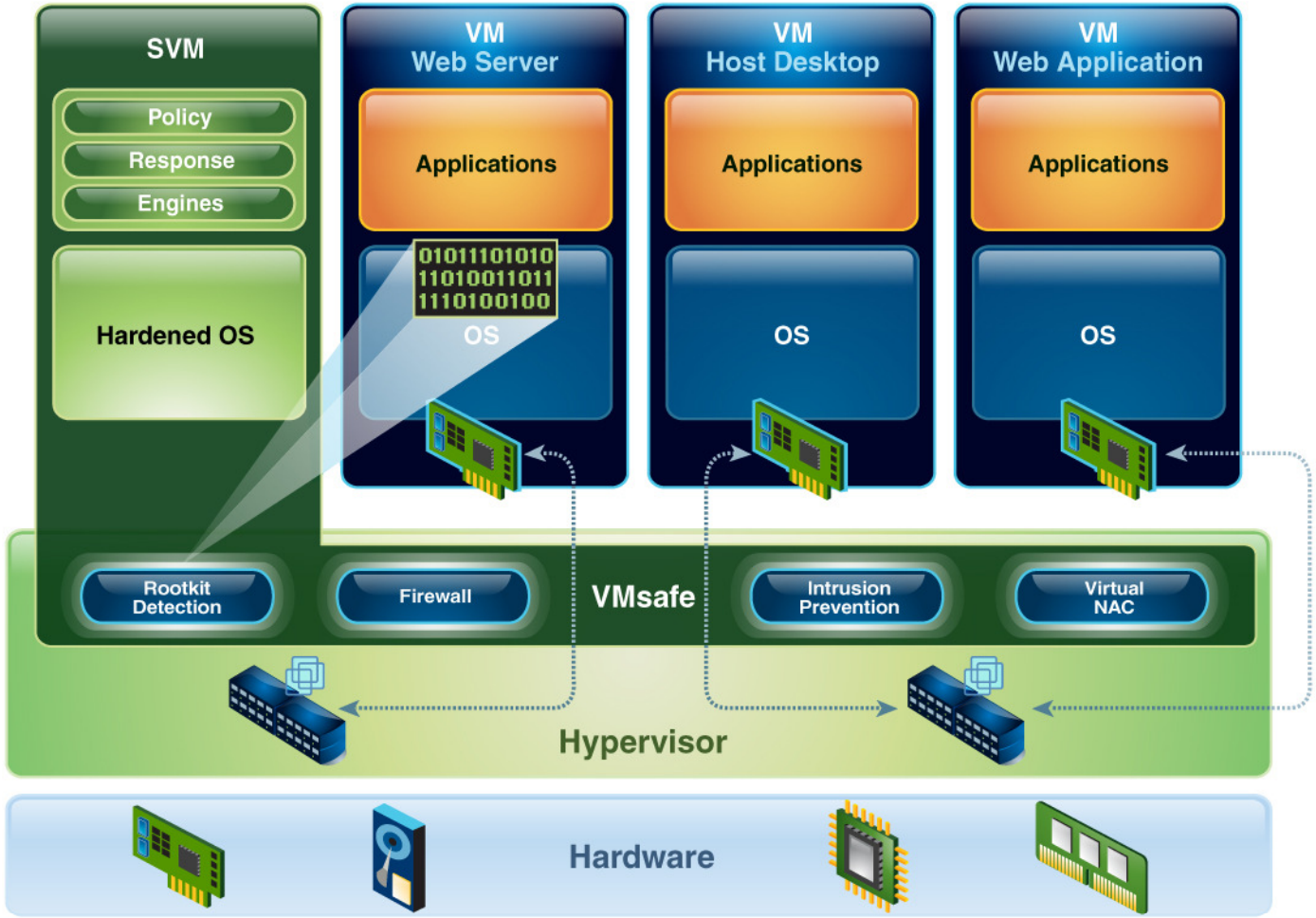
Virtual NICs & Virtual Hardware are targets

40

Introducing IBM Security Virtual Server Protection for VMware

Integrated threat protection for VMware vSphere 4

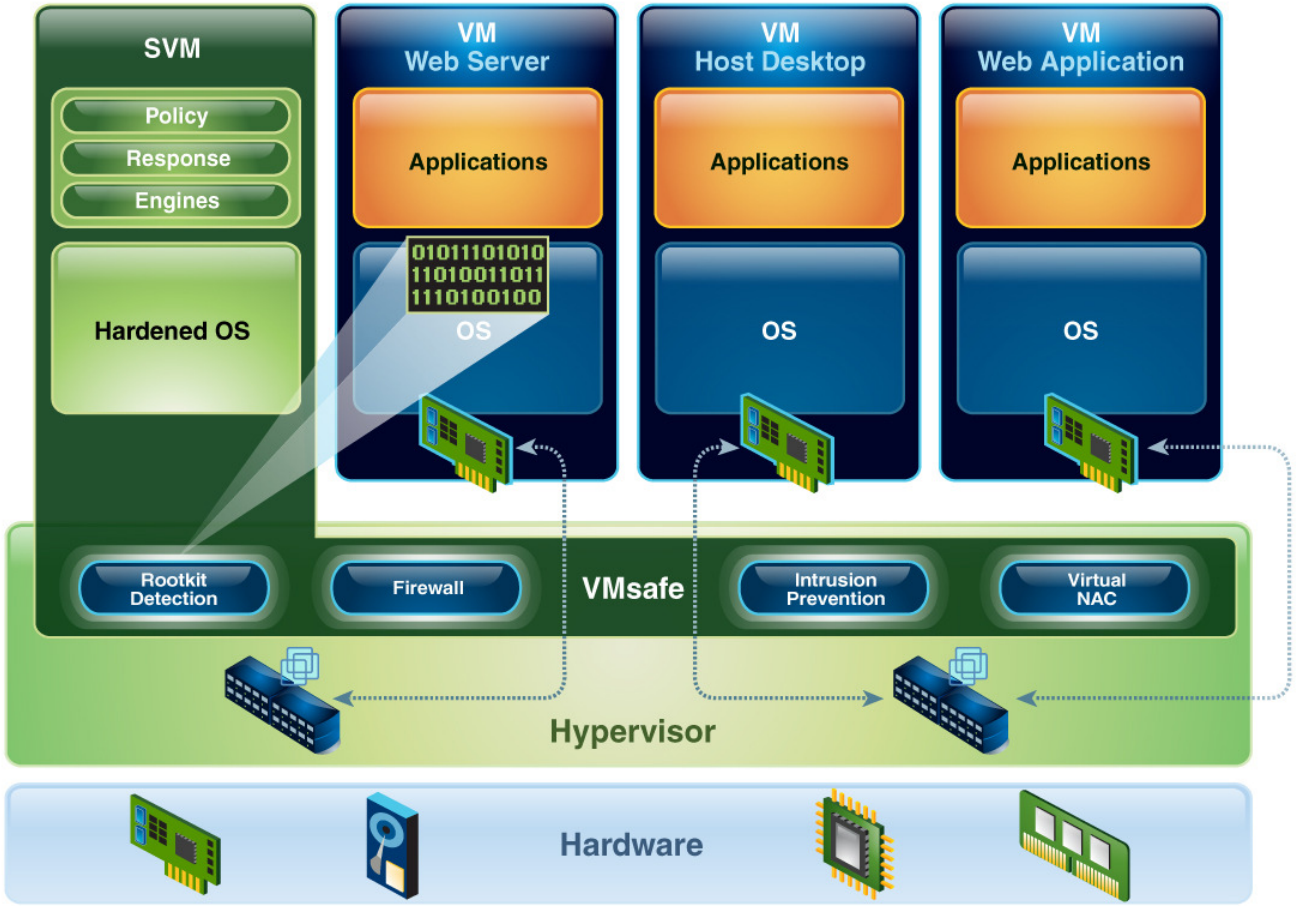
Helps customers to be more secure, compliant and cost-effective by delivering integrated and optimized security for virtual data centers.



- Provides dynamic protection for every layer of the virtual infrastructure
- Helps meet regulatory compliance mandates by providing security and reporting functionality customized for the virtual infrastructure
- Increases ROI over using physical security for virtual data centers
- Increases virtual server uptime with virtual rootkit detection

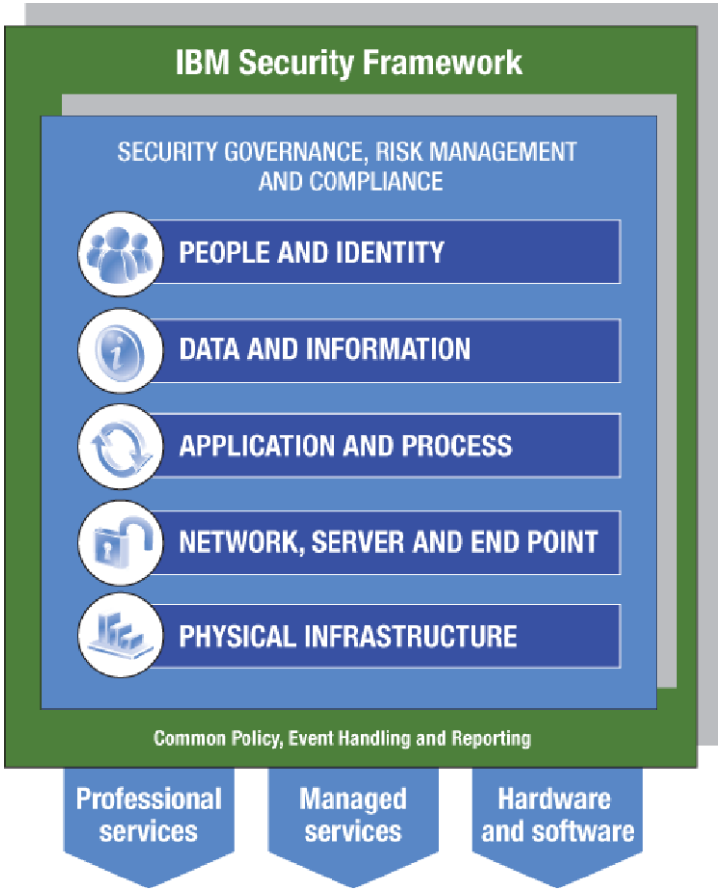
Virtual Server Protection for VMware enables you to realize the benefits of virtualization without reducing your security posture

- Provides dynamic protection for every layer of the virtual infrastructure
  - Hypervisor
  - Operating System
  - Network
  - Applications
  - Virtual machine (VM)
  - Inter-VM traffic



IBM: comprehensive security risk and compliance management

- The ***only security vendor*** in the market with **end-to-end coverage of the security foundation**
- **15,000** researchers, developers and SMEs on security initiatives
- **3,000+** security & risk management patents
- **200+** security customer references and **50+** published case studies
- **40+** years of proven success securing the zSeries environment
- Managing **more than 7 Billion** security events per day for clients



IBM Security: Sum is greater than its parts

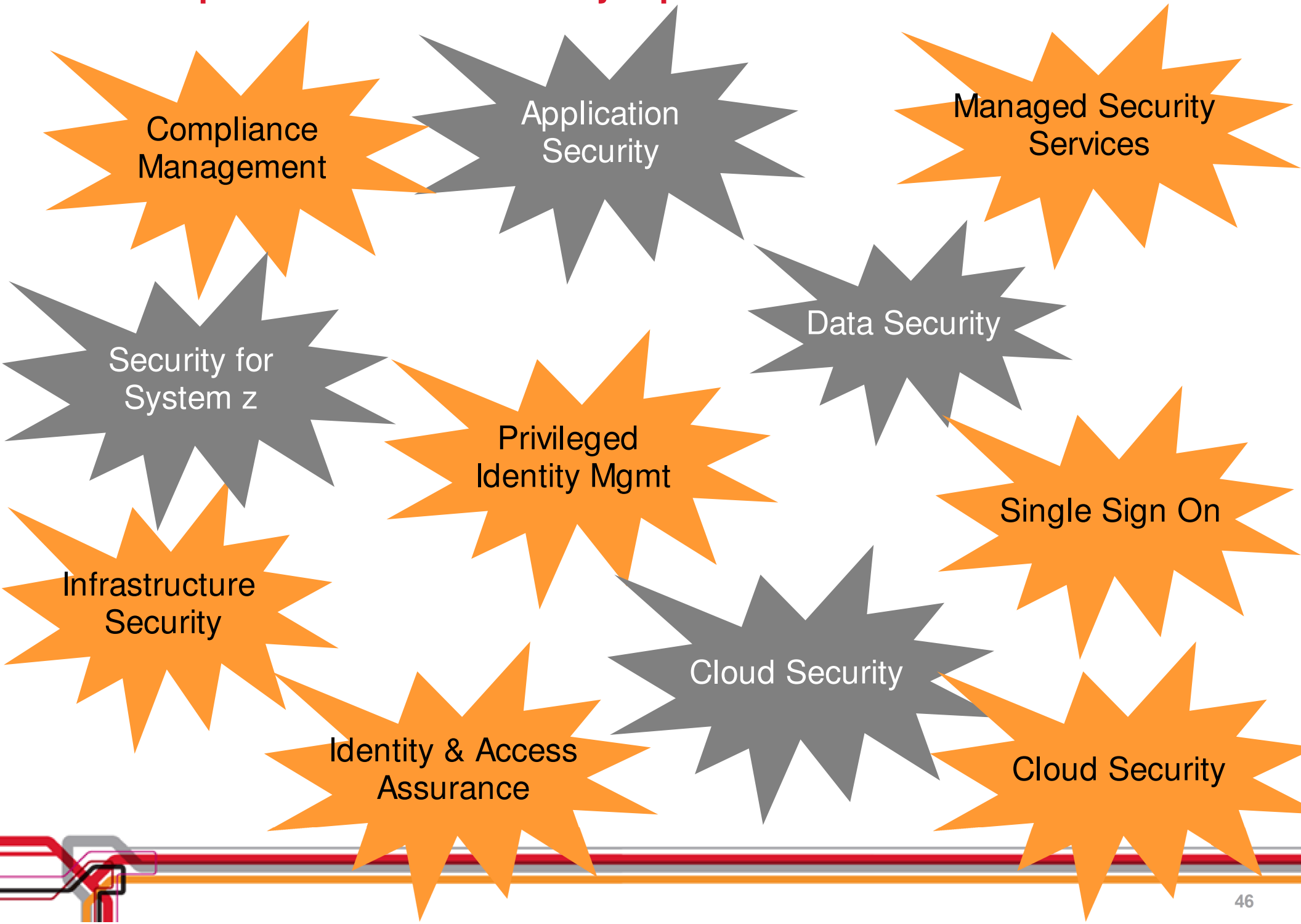
FORRESTER®		Wave: User Account Provisioning (TIM)	Leader
FORRESTER®		Wave: Enterprise Security Information Management	Leader
Gartner		MQ: User Provisioning (TIM)	Leader
Gartner		MQ: Web Access Management (TAM)	Leader
Gartner		MQ: Security Information & Event Management (TSIEM)	Leader
Gartner		ISS Network Security, Firewalls and Managed Services	Leader
Gartner	#1	Marketshare : Web Access Management, Worldwide, 2005 (FIM, TAM)	Ranked #1
Gartner	#1	Marketshare : Application Security Vulnerability Scanning, 2006 (Rational AppScan)	Ranked #1
FROST & SULLIVAN	#1	Identity Management (TIM , TAM, FIM, TDI, TDS,)	Ranked #1
FROST & SULLIVAN	#1	Marketshare: Managed Security Services	Ranked #1
IDC Analyze the Future	#1	Marketshare: Identity and Access Management	Ranked #1
IDC Analyze the Future	#1	Marketshare: Application Vulnerability Assessment (Rational AppScan)	Ranked #1

44

IBM Security: Sum is greater than its parts!

On Tuesday March 2, IBM Corporation was named "Best Security Company" for 2010 by SC Magazine, recognizing IBM's outstanding achievement in risk management and its comprehensive family of security solutions. As the industry's preeminent awards program, the annual SC Awards has recognized security's key contributors and outstanding products for more than a decade.

Visit the expo hall for these security topics and more!




Thank
You

Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at http://www.ibm.com/legal/copytrade.shtml.