



Un pianeta intelligente è anche più sicuro

Cesare Radaelli

IBM Software

PCTY2010



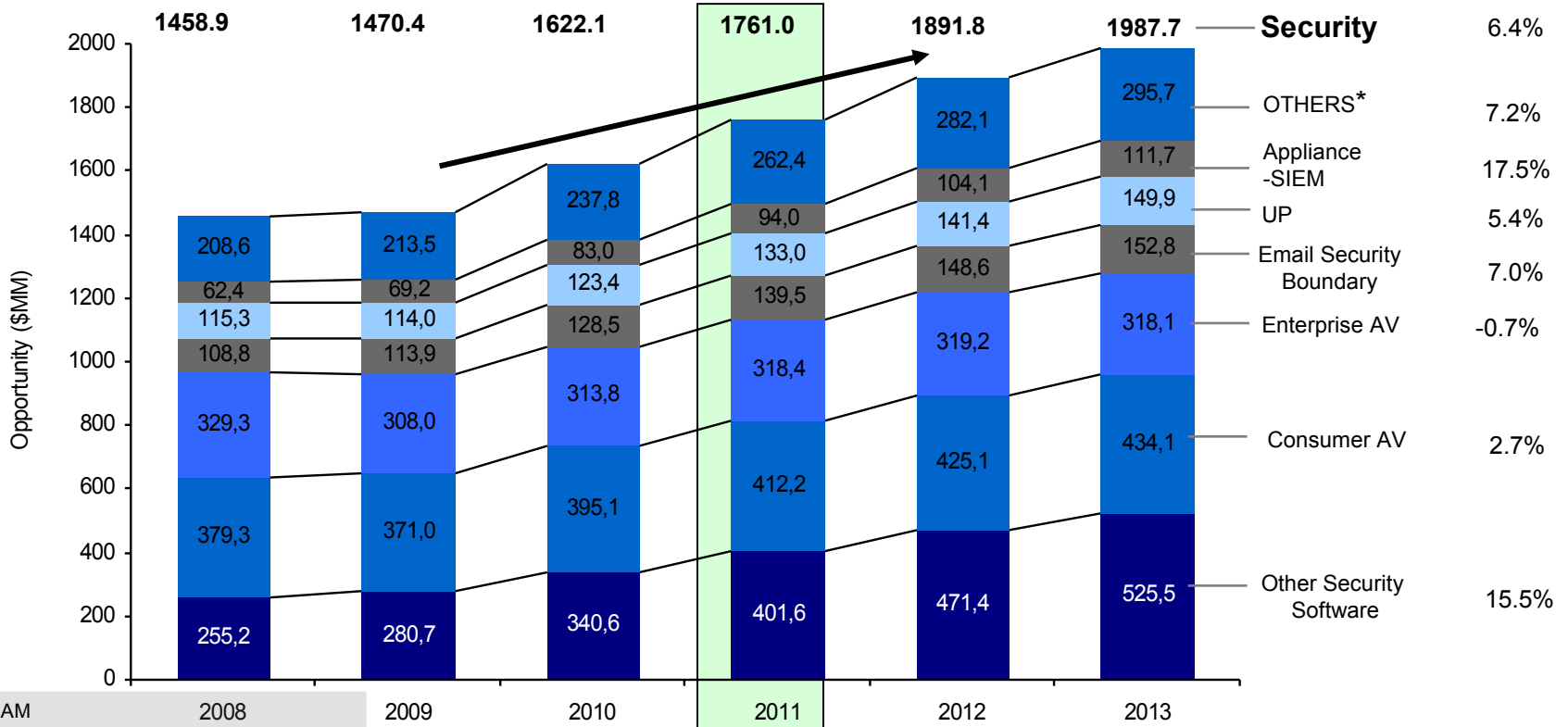
Pulse Comes to You

23 Novembre, Milano

According to Gartner, the Software Security market opportunity is forecasted to grow at a CAGR('08-'13) of 6.4% ; Appliance E-mail security is the fastest growing segment where as Enterprise Anti-Virus is projected for a negative growth

Security Solutions market opportunity trend '08 – '13 SWIOT (\$M)

CAGR
2013/08



Security

OTHERS*

Appliance -SIEM

UP

Email Security Boundary

Enterprise AV

Consumer AV

Other Security Software

6.4%

7.2%

17.5%

5.4%

7.0%

-0.7%

2.7%

15.5%

WAM
URL Filtering
SIEM
Appliance-E-mail Security Boundary
OTHERS*

Source: Gartner Security Market EMEA 2009

Hybrid Security platforms and Cloud security are driving the WW trends in 2010

Key Trend	Guidance
1. Hybrid security will diversify	The mix of security platforms (HW, appliances, SW, security SaaS, and virtualization) and possibly PSS and MSS will continue to diversify
2. Cloud security will move toward solutions	Concerns about cloud security cause solutions to emerge that focus on authenticating users, controlling admin privileges, managing encryption keys, etc
3. SaaS will become a standard security platform	Customers are demanding more flexibility, thus vendors will offer SaaS as an alternative to HW/SW. SaaS will include messaging, Web, vulnerability and identity management.
4. DLP will disappear	DLP will disappear into messaging, Web, and IAM security suites. It will only remain an independent product for large enterprise customers.
5. Vertical integration will return	Vertically integrated vendors will embed security functions into all infrastructure management functions. This will help alleviate the many licensing fees associated with various platforms, users, etc.
6. Physical security information management will increase	Demand for intelligent management that links data from multiple surveillance systems, track critical situations in real time, filter alerts, determine appropriate responses, and delegate administration.
7. Endpoint security will move to the cloud	Because malware signature files are growing too large for PC storage and processing, suspicious files will increasingly be sent to cloud-based applications for confirmation and fixes.
8. Mobile security will finally take off	The rising use of mobile devices will drive mobile security functions that are handled from a consolidated Web-based console
9. Telecom will become a major developer and reseller of security	The growth of IP networks, telcos are moving beyond traditional MSS to provide cloud-based MSS (including DOS defense, DPI, network security, messaging security, and Web security).



Key drivers for Smart Security

Increasing Complexity



Soon, there will be **1 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 **\$29.8 billion** in 2010

Ensuring Compliance



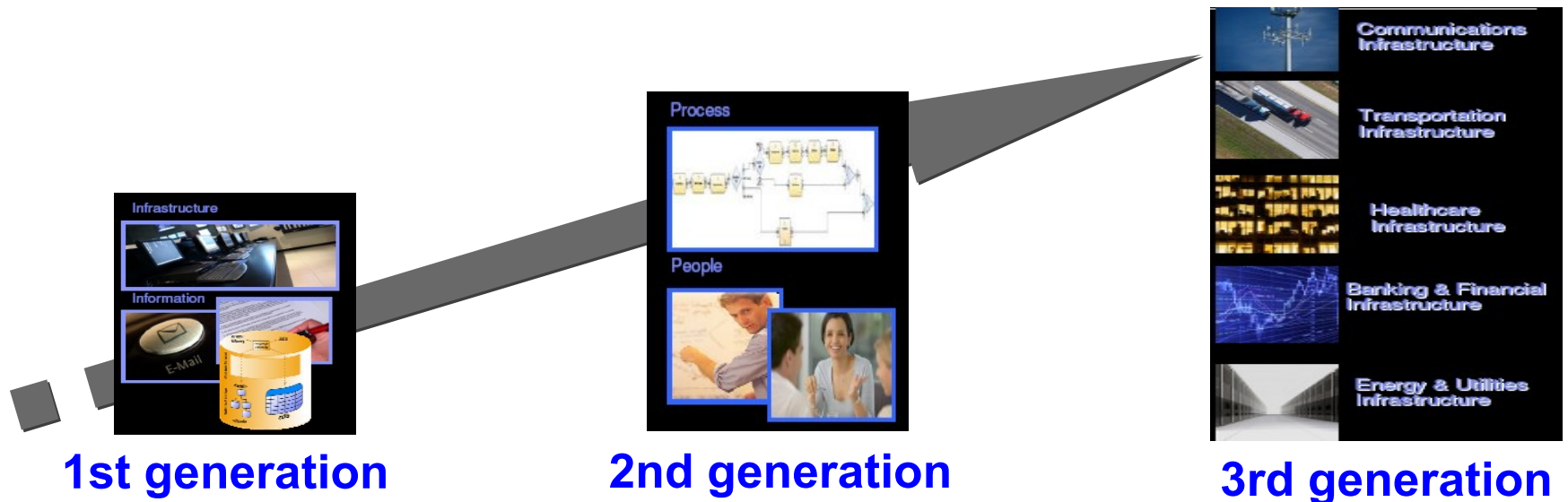
The cost of a data breach increased to **\$204** per compromised customer record

People are becoming more and more reliant on security

What are the Risks?



- Complex “system of systems”
- No perimeter – vast number of User “touch points”
- Interdependence on Digital Systems (Internal and external providers)
- Inconsistent application of Security Engineering



X-Force R&D Drives IBM ISS Security Innovation

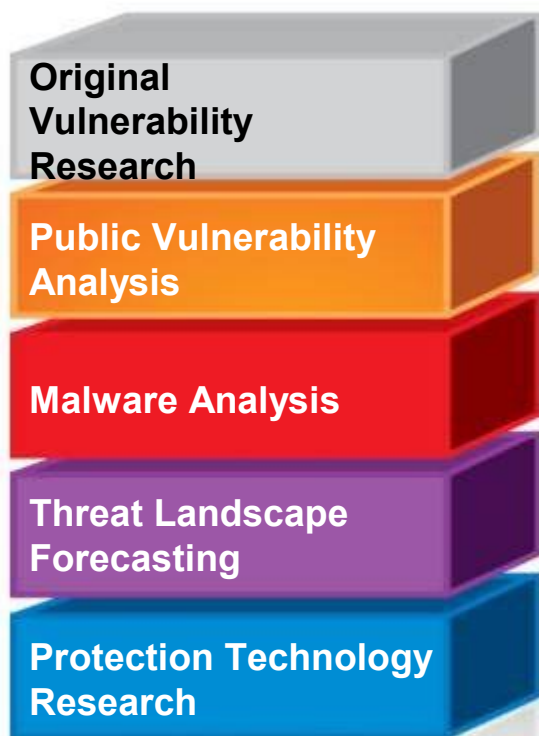
Research



Technology



Solutions



X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

X-Force XPU's

- Security Content Update Development
- Security Content Update QA

X-Force Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing

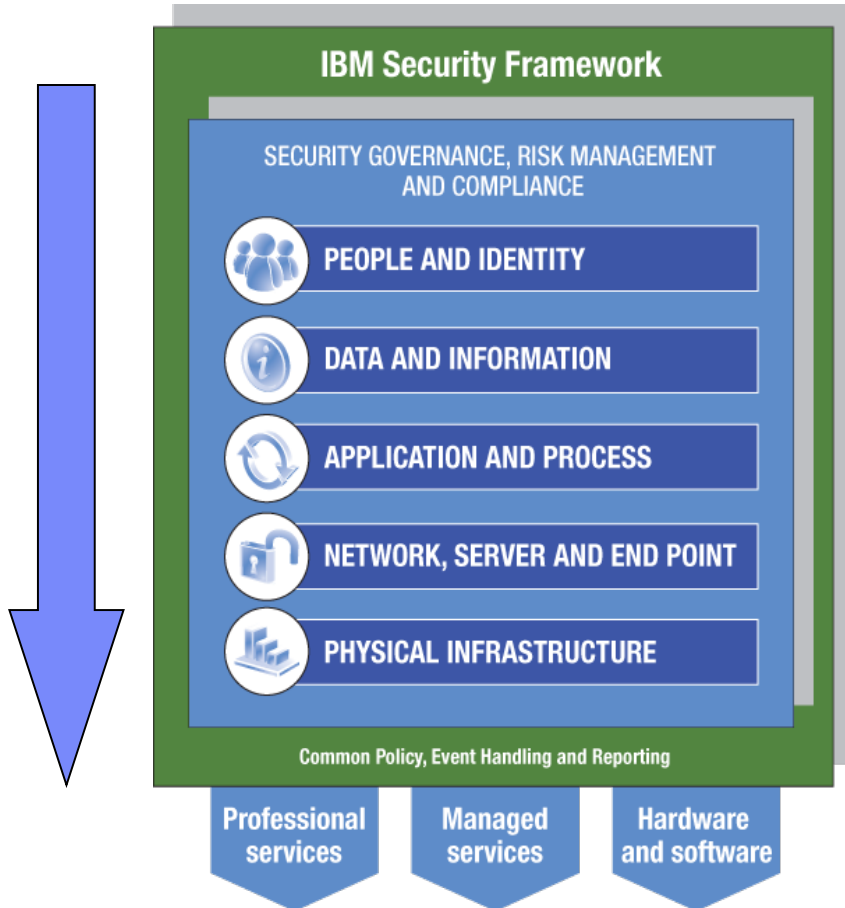


IBM: gli approcci alla Sicurezza Integrata

**Top-Down:
Business Driven**

**Enterprise Security
Governance**

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






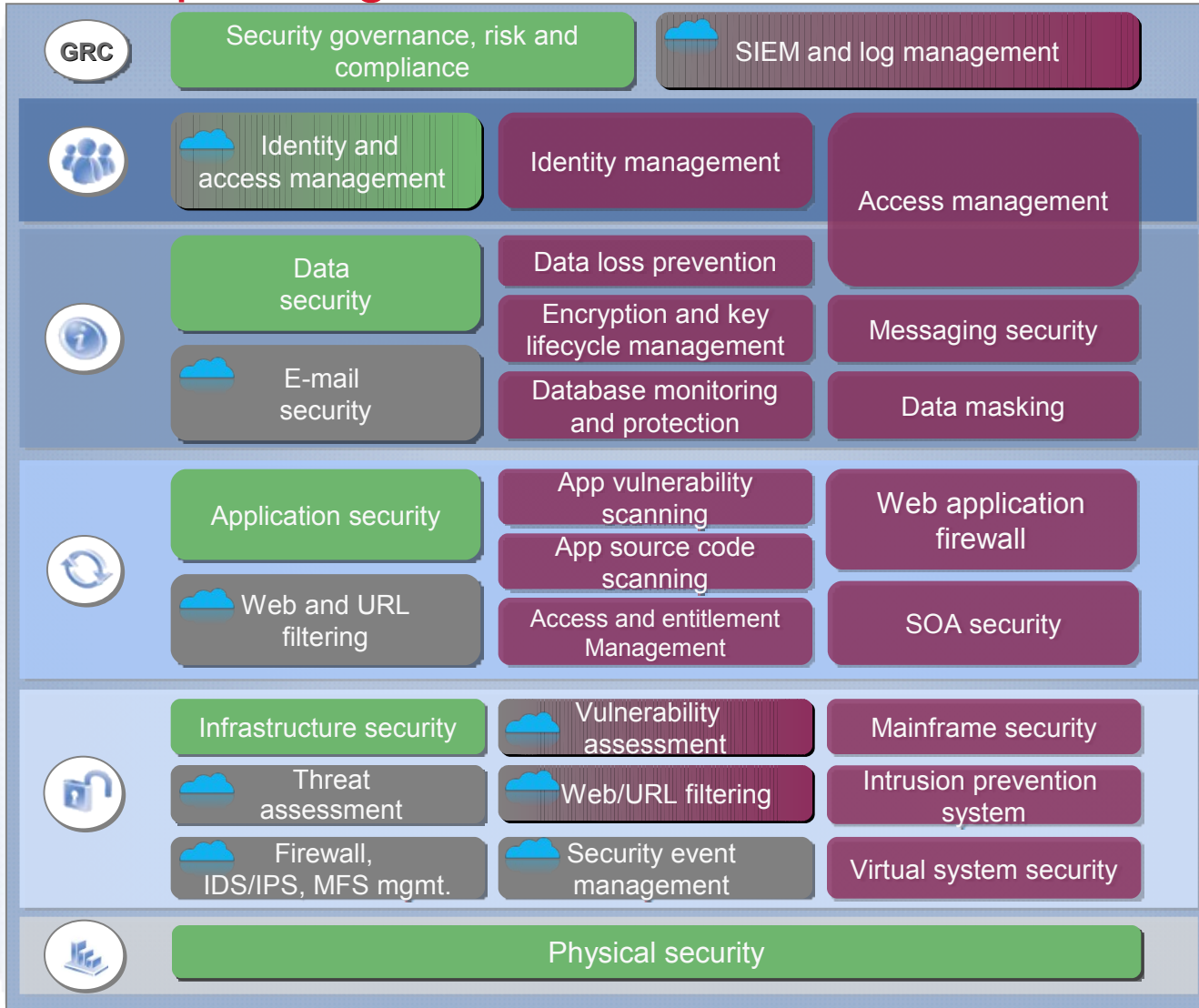
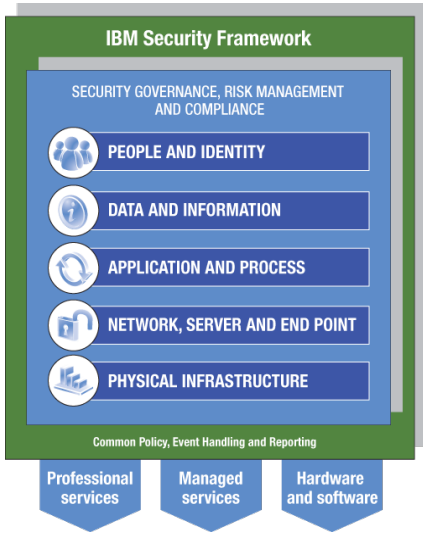
**Bottom-Up:
Technology
Driven**

**Design and
Implementation of
Security Solution**

*How can I design
and implement
Security Solutions
that address my
organizational and
technical
requirements?*

IBM Security Framework: portafoglio offerta

-  Professional Security Services
-  Cloud-based and managed services
-  Products





IBM investe in continue acquisizioni per arricchire il proprio portfolio

- **Netezza** [Announced September 20, 2010] leading creator of analytic data warehousing appliances
- **OpenPages** [Announced September 15, 2010] automates the process of identifying, measuring and monitoring all the different areas in an organization that risks will impact
- **BigFix** [Closed on July 19, 2010] provides an integrated architecture for endpoint management that will enhance existing capabilities in the IBM Integrated Service Management portfolio
- **Initiate** [closed March 1, 2010] a privately held data integrity firm based in Chicago
- **Guardium** [Closed November 30, 2009] market leader in real-time enterprise database monitoring and protection
- **SPSS Inc.** [Closed October 2, 2009] leading global provider of predictive analytics software and solutions
- **Ounce Labs Inc.** [Acquired July 28, 2009] provides source code (static) security testing tools that help companies identify and resolve security vulnerabilities in applications
- **Encentuate, Inc.** [Closed March 11, 2008] leading provider of identity and access management (IAM) software focused on enterprise single sign-on and strong authentication.
- **Cognos** [Closed January 31, 2008] a leading provider of Business Intelligence and performance management technologies
- **Princeton Softech, Inc.** [Closed September 10, 2007] protects data privacy in vulnerable development and testing environments and validating test results
- **Watchfire Corporation** [Closed July 20, 2007] provides web application security software that pinpoints critical vulnerabilities and helps manage the process of fixing them
- **Consul Risk Management, Inc.** [Closed January 22, 2007] leading provider of compliance and audit management solutions for distributed and mainframe systems
- **ISS** [Closed October 20, 2006] is at the leading edge of security research and innovation, including the invention of vulnerability assessment, intrusion detection and prevention technologies
- **DataPower Technology, Inc.** [Closed October 14, 2005] provider of technology that helps simplify, accelerate and increase the security of SOA deployments.
- ...

IBM Security Framework in action



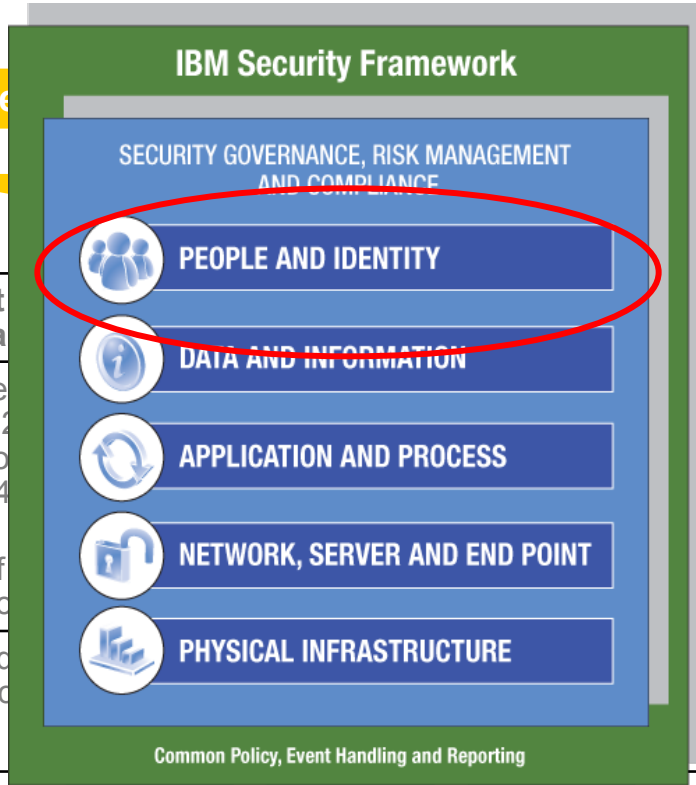
People and identity



BUSINESS VALUE

Lower costs and mitigate the

access to corporate resources



	Cost Management			Auditing, reporting and managing access to resources
Business Challenge	<ul style="list-style-type: none"> On average, users spend 20% of their time on about 40% of invalid logins. 30% of passwords are expired. 			<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 Assurance			Tivoli Identity and Access Assurance, Tivoli Security Information and Event Manager
Professional Services	Identity and Access Management Services	Professional services	Managed 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

IBM Tivoli Identity Manager v5.1 enhances enterprise IAM governance

IBM Tivoli Identity Manager v5.1	
Feature	Benefit
Role hierarchy	Simplify and improve visibility of user access
Separation of duties	Strengthen security and compliance by preventing business process conflicts
Access recertification	Drive compliance while minimizing end user impact
Group management	Simplify and reduce cost of user administration
Compliance Reporting	Proof for audit purposes



C-Level officers receive improved visibility, control and automation of critical resource access

Operational role management is a fundamental, embedded capability within the TIM platform





Data and information

BUSINESS VALUE

Understand, deploy and properly

of sensitive business data



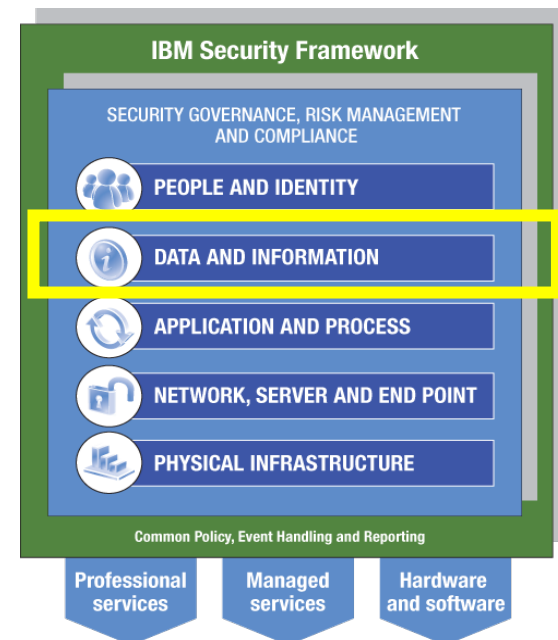
	Protecting Critical Databases				
Business Challenge	Mitigate threats against databases from external attacks and internal privileged users				had each in the or theft of personal data breach record*
Software	Guardium Database Monitoring & Protection				42% of all cases involved third-party mistakes and flubs... magnitude of breach events ranged from about 5,000 to 101,000 lost or stolen customer records*
Professional Services	Data Security Assessment Services	Professional services	Managed services	Hardware and software	Data Loss Prevention; Tivoli Security Information and Event Manager
					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

How Does Guardium Complement Tivoli?

- Integrates with Tivoli Security & Information Event Manager (TSIEM) for sharing policy violation alerts & selected log information
- Use TSIEM for:
 - Collecting logs & events from range of systems (UNIX, Windows, z/OS, firewalls, applications, etc.)
 - Enterprise-wide dashboard
 - Compliance reporting
 - Correlation & forensics across all types of systems
- Use Guardium for all database security & compliance:
 - Real-time monitoring & granular auditing (including privileged user monitoring) with minimal performance overhead
 - VA & configuration auditing for databases
 - Sensitive data discovery in databases
 - Compliance reporting & workflow automation
 - Feeding policy violations & selected audit logs to TSIEM



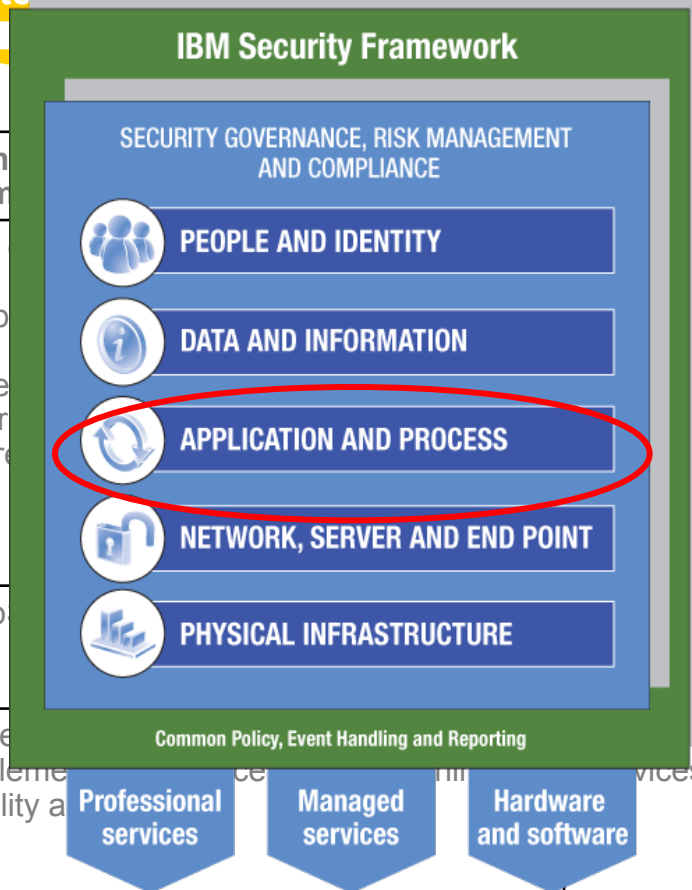


Application and process

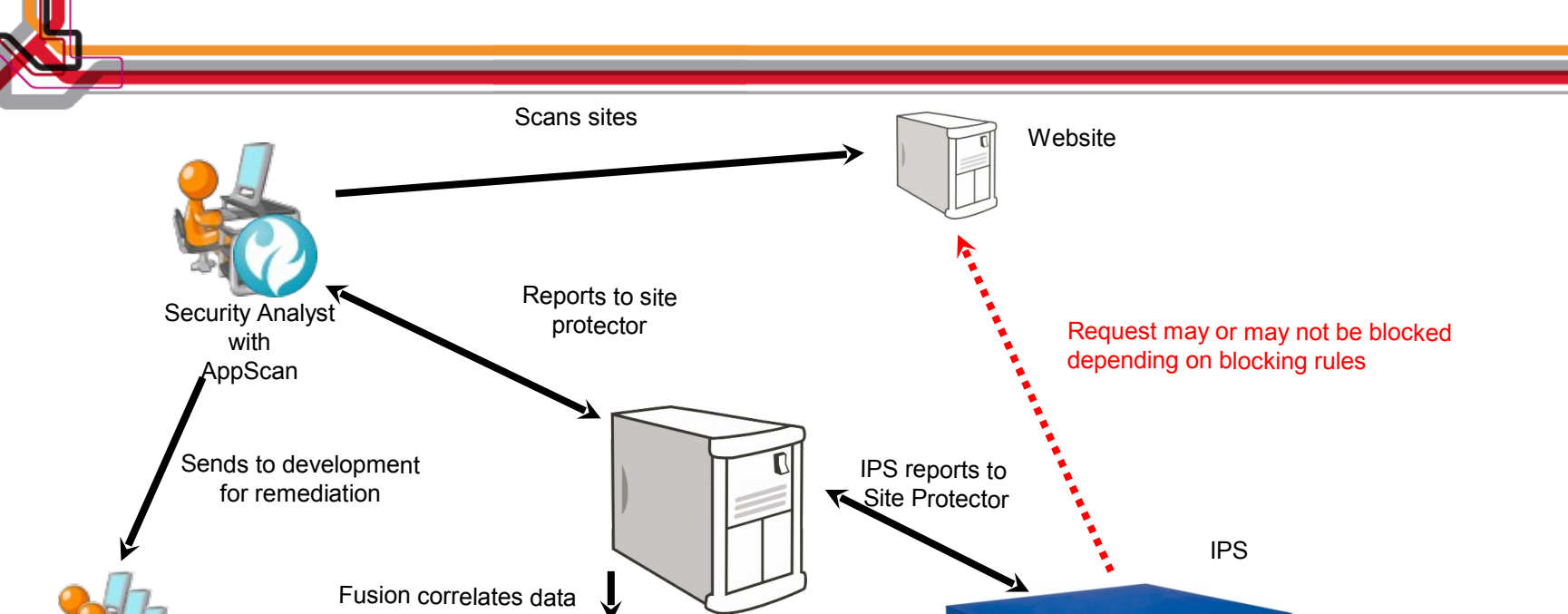
* IBM X-Force Annual Report, Feb 2009
 ** Applied Software Measurement, Caper Jones, 1996

BUSINESS VALUE

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



	Security in Development		Adding App Controls	Providing SOA Security
Business Challenge	Vulnerabilities early in the development process are orders of magnitude cheaper to fix versus after application is released		g to s, up to their on ment costs or coding ccess and their nding cture	Establishing trust and high performance for services that span corporate boundaries is a top priority for SOA-based deployments
Software	Rational® App Ounce		Identity and Assurance	WebSphere® DataPower®; Tivoli Security Policy Manager
Professional Services	Secure App Development Process Enablement App Vulnerability and Source Code Scanning	Professional services	Access	
Managed Services		Managed Vulnerability Scanning	Managed Access Control	



Developers fix issues

SiteProtector

Analysis : 65.196.147.50 : G-Series

My Sites

- 65.196.147.50
 - SP2001
 - Geographical
 - Organizational
 - Protection Solutions
 - ES-Series
 - G-Series
 - M-Series
 - PSL
 - Rational AppScan
 - SiteProtector
 - Test
 - Test-P
 - Ungrouped Assets
 - 1.1.1.1 - 255.255.255.254
 - 192.168.1.0 - 192.168.1.255
 - localhost

Event Analysis - Event Name (Agent) Load View Save View

Data Filters (3 applied)

Time Filter: Last Week

Tag Name Filter

Source IP Filter

Tag Name	Status
HTTP_POST_SQL_UnionSelect	Detected event
HTTP_POST_SQL_UnionSelect	Attack failure (blocked by Proventia appliance)
HTTP_POST_XP_Cmdshell	Detected event
HTTP_QuikStore	Attack failure (blocked by Proventia appliance)
HTTP_repeated_character	Attack failure (blocked by Proventia appliance)
HTTP_Server_ID	Detected event
HTTP_Share_Point_XSS	Detected attack (vuln not scanned recently)
HTTP_Shells_Perl_Exe	Detected attack (vuln not scanned recently)
HTTP_testcgi	Attack failure (blocked by Proventia appliance)
HTTP_Translate_F_SourceRead	Attack failure (blocked by Proventia appliance)
HTTP_Twiki_Image_Include_CmdExec	Attack failure (blocked by Proventia appliance)
HTTP_Unify_UploadServlet	Attack failure (blocked by Proventia appliance)
HTTP_Unix_Passwords	Detected event
HTTP_BackslashDotDot	Detected attack (vuln not scanned recently)
HTTP_LIRL_dotpath	Detected event
HTTP_LIRL_Many_Slashes	Attack failure (blocked by Proventia appliance)
HTTP_LIRL_repeated_char	Detected event
HTTP_LIRL_Repeated_Dot	Detected attack (vuln not scanned recently)
HTTP_LIRLscan	Detected event
HTTP_Webplus	Attack failure (blocked by Proventia appliance)
HTTP_Windows_Executable	Attack failure (blocked by Proventia appliance)
SQL_Injection	Attack likely successful (vulnerable)
XPath_Injection	Attack likely successful (vulnerable)

Criminal/
Hacker/
Script Kiddie

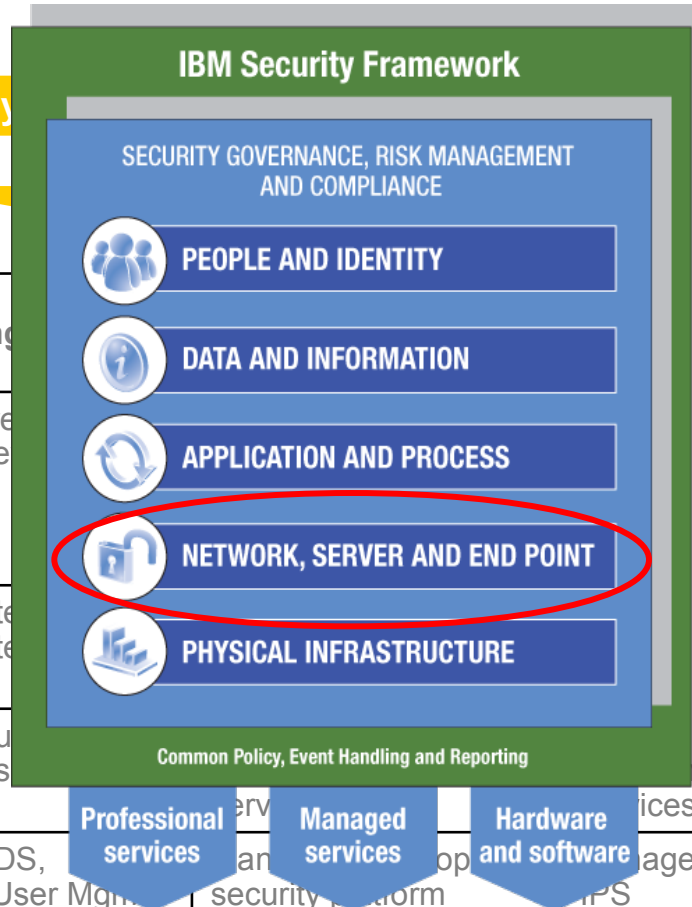
Network, server and end point



BUSINESS VALUE

Optimize service availability by

Optimize, technology and process

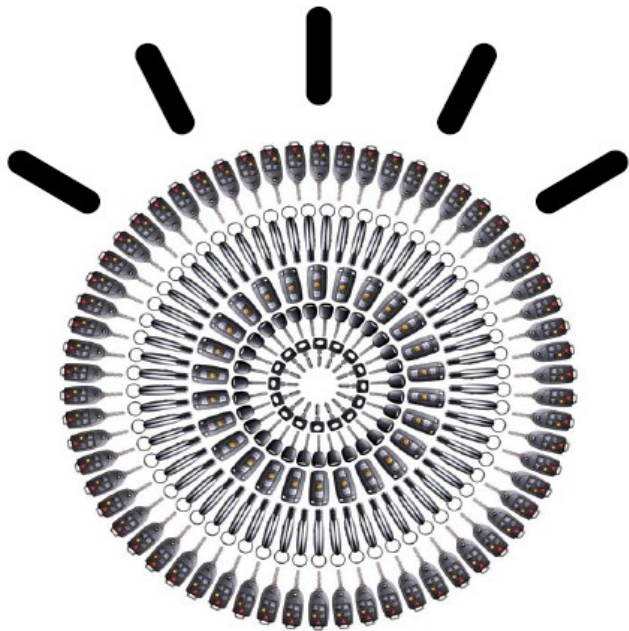


	Protecting Servers	Protecting Networks	Protecting Mainframes
Business Challenge	Mitigate threats against servers; prevent data loss	Mitigate threats against networks; prevent data loss	Mitigate threats against mainframes; protect against vulnerabilities from configuration; contain the privileged users
Software	Server Protection Server Protection VMWare	Intrusion Detection System	Tivoli® zSecure suite
Professional Services	Server security services	Network security services	
Managed Services	Managed IDS, Privileged User Mgmt	Managed Network Security Platform	

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

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

Gruppo Intergea



Ecco come una concessionaria auto guida un business sicuro.

Il mondo in cui lavoriamo diventa sempre più interconnesso. Ma mentre continuano a crescere le connessioni in rete tra le aziende, crescono anche le minacce e i rischi. Malware come spam, virus e worm, responsabili di intrusioni, furti di dati e di identità, sono solo alcuni tra i tanti pericoli. Per fortuna, su un pianeta più intelligente, abbiamo gli strumenti per proteggere dati vitali e aiutare ad assicurare la continuità del business.

Gruppo Intergea, azienda di medie dimensioni che vende auto e servizi nel Nord Italia, ha sentito l'esigenza di potenziare la sicurezza della sua infrastruttura IT. Un compito non semplice, con 27 sedi operative sul territorio. Con l'aiuto di IBM e dei suoi Business Partner, Intergea ha attivato una soluzione di Internet Security Systems intelligente che non solo è in grado di prevenire, riconoscere e rispondere attivamente alle possibili intrusioni, ma è anche in grado di identificare, e bloccare automaticamente, i tentativi di sfruttare le vulnerabilità della rete, causa potenziale di rallentamenti, interruzioni o perdite di dati. Così il business di Intergea viaggia sempre veloce e sicuro. Le medie imprese sono il motore di un pianeta più intelligente. Costruiamolo insieme. Scopri di più: ibm.com/auto/it

“Thanks to the proactive nature of our new IBM security system, we’re protected from not only known security threats, but also from vulnerabilities that we don’t even know about.”

*— Luca Pisanu, IT Manager
Gruppo Intergea*

Componenti della Soluzione:

- IBM Internet Security Systems
- IBM Proventia® Desktop Endpoint Security
- IBM Internet Scanner®
- IBM Proventia Intrusion Prevention System GX3002

INTERGEA
GRUPPO

IBM Security Solutions, one coordinated voice for security.

IBM has established a more efficient and dynamic, cross-company approach for its IT security portfolio in which research, design, development, marketing, services and support for IT security solutions for IBM clients worldwide are consolidated and linked together.



- ✓ *IBM is the Trusted Partner delivering products and services recognized for leadership in IT security*
- ✓ *IBM's philosophy of Secure By Design; Factor Security and Privacy into the initial design, not bolted on after the fact*
- ✓ *IBM security solutions allow customers to address the 3 Cs; Complexity, Compliance and Cost*

one coordinated voice for security.

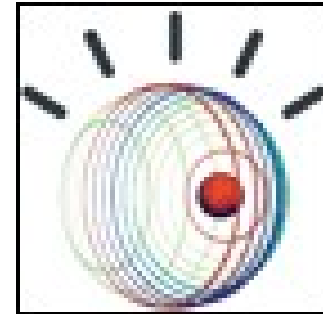
IBM Security Solutions. Secure by Design.
a trusted partner
a coordinated voice
a comprehensive approach

Hardware Software Services

Nuova pubblicazione IBM sulla Sicurezza

- 1 Un approccio di business alla sicurezza
- 2 La mitigazione delle minacce all'infrastruttura IT
- 3 Identity and access management
- 4 La sicurezza delle applicazioni
- 5 La sicurezza fisica
- 6 I Managed Security Services
- 7 La sicurezza IBM per il Cloud Computing

**Un pianeta più intelligente
è anche più sicuro.**





Grazie
per l'attenzione!

IBM Software

PCTY2010 
Pulse Comes to You

Cesare Radaelli
IBM Security Solutions
Security TT Leader Italy

cesare.radaelli@jit.ibm.com