

InfoPlanet

**La Sicurezza per IBM:
strategia e panoramica**

**Cesare Radaelli, *Security Tiger Team leader,*
*IBM Italia***



Our world is becoming more . . .

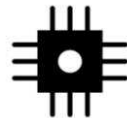


Interconnected



1 trillion

By next year, an estimated 2 billion people will be on the Web... and a trillion connected objects – cars, appliances, cameras, roadways, pipelines – comprising the "Internet of Things."



Instrumented



90%

Nearly 90% of innovation in automobiles is related to software and electronics systems. 30-60% of the value is in the software.



Intelligent



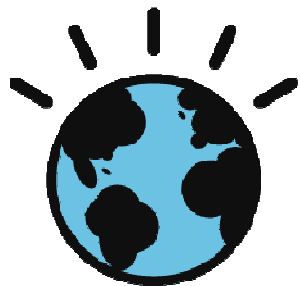
173.8 million

Smart phones sold in 2009. More than the number of laptops sold in the same year, for the 2nd year running (80 million in Q3 2010).

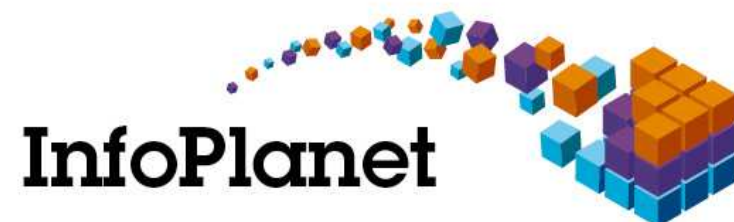
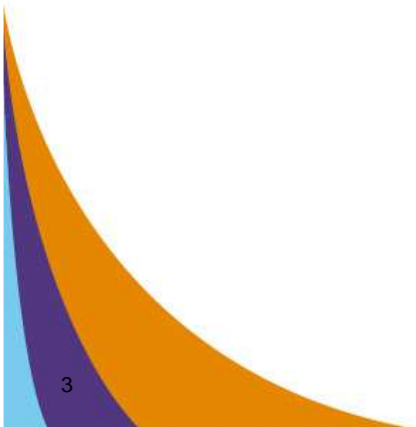
InfoPlanet



A Smart Planet which offers...



New possibilities.
New complexities.
New risks.



Key drivers for security projects

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

Source http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html



ONE voice for security.

IBM SECURITY SOLUTIONS

INNOVATIVE products and services.

IBM SECURITY FRAMEWORK

COMMITTED to the vision of a Secure Smarter Planet.

SECURE BY DESIGN

InfoPlanet




I rischi sono reali!



Attacco Hacker del Gruppo Anonymous al sito di Finmeccanica - AgoraVox Italia - Windows Internet Explorer

http://www.agoravox.it/Attacco-Hacker-del-Gruppo.html

Attacco Hacker del Gruppo Anonymous al sito di Finmeccanica



Il Sito di **Finmeccanica** è stato oggetto intorno alle 21 di ieri di un **attacco** informatico che è stato rivendicato dal gruppo **Anonymous**, la firma collettiva che raggruppa differenti hacker internazionali in una community decentralizzata che ha lo scopo di mettere in atto azioni di protesta. In Italia **Anonymous** ha recentemente attaccato il Sito del Governo e di **Mediaset**. Gli attacchi di **Anonymous** erano stati rivolti in passato anche contro varie società che avevano bloccato i sistemi di transazione online per la raccolta di fondi a favore di **WikiLeaks**, come **Mastercard**, **PayPal**, **Visa** e le **Poste Svizzere**.


L'attacco hacker nei confronti di **Finmeccanica**, come si legge in un comunicato del gruppo, intende essere un'azione "Contro la fornitura di armi alla Libia" e "L'ipocrita condanna di Gheddafi da parte di Berlusconi". **Anonymous** "Giudica inammissibili gli stretti rapporti economici/politici e di 'cooperazione' nel contrasto all'immigrazione clandestina intercorsi fra il governo italiano e quello libico, resosi responsabile, nella figura del Colonnello Muammar Gheddafi e dei suoi collaboratori, di una repressione senza precedenti contro le forze di opposizione e i pacifici manifestanti nel suo Paese".

"Tramite aziende private e a partecipazione pubblica operanti in Italia" scrivono ancora gli hacker, il Governo italiano ha "esportato in Libia ingenti quantità di armamenti leggeri/pesanti e mezzi d'assalto che ora vengono impiegati contro civili inermi e in attività contrarie al rispetto dei diritti umani e della libertà di parola, in palese violazione delle regolamentazioni internazionali sul commercio d'armi".

UPDATE: attacchi sono stati diretti anche verso i siti di **ENI** e **Unicredit**.

Profilo personale, articoli e statistiche

Pubblicità



Imposta Google come pagina iniziale

Ultimi articoli dell'autore

- Articolo 104 per Bradley Manning: l'Esercito USA getta via le Chiavi della sua Cella
- Attacco Hacker del Gruppo Anonymous al sito di Finmeccanica
- Apple presenta iPad 2 e iOS 4.3
- News Corp presenta The Daily, il Primo Quotidiano per Tablet che nasce Digitale

Tutti gli articoli dell'autore

Articoli correlati

Tecnologia

Mi piace Connect Facebook Twitter YouTube Videos Aiuta AgoraVox

Cerca... Traduci Articoli recenti

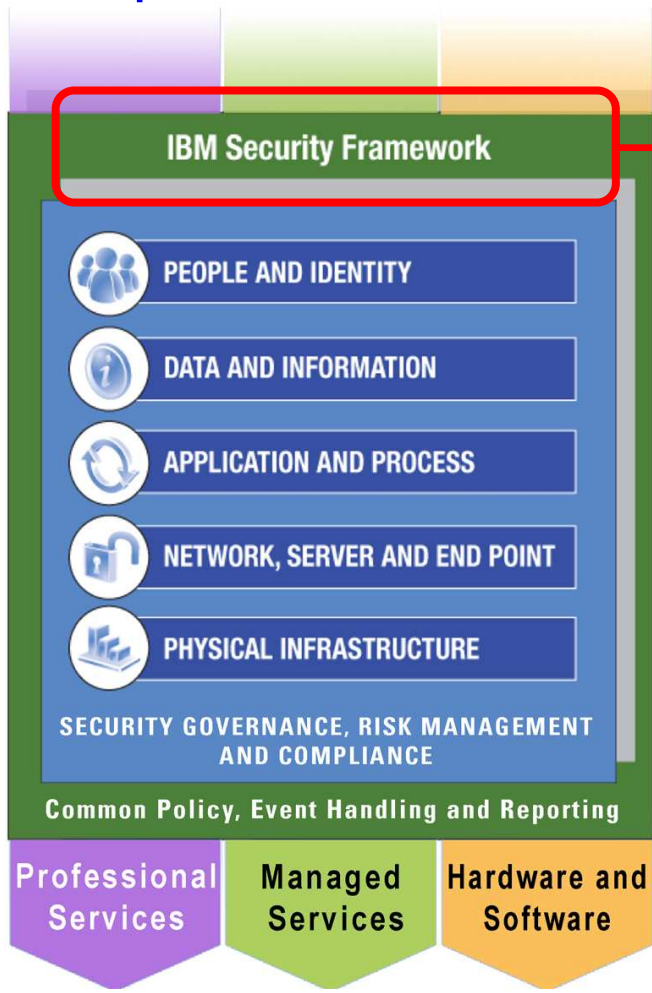
start

InfoPrint M... Mail - Inbo... CGI SW Un... AT&T Net... Attacco Ha... 87% 10.19

InfoPlanet



The IBM Security Framework foundation addresses your challenges of cost, complexity and compliance



Build a strong foundation for IT security

Create and sustain security governance

Manage risk

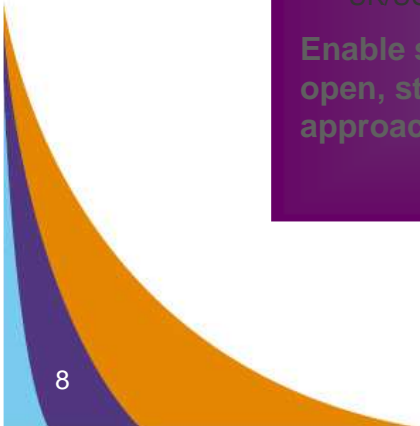
Ensure compliance



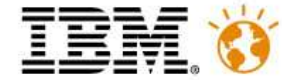
IBM's Approach to Secure by Design



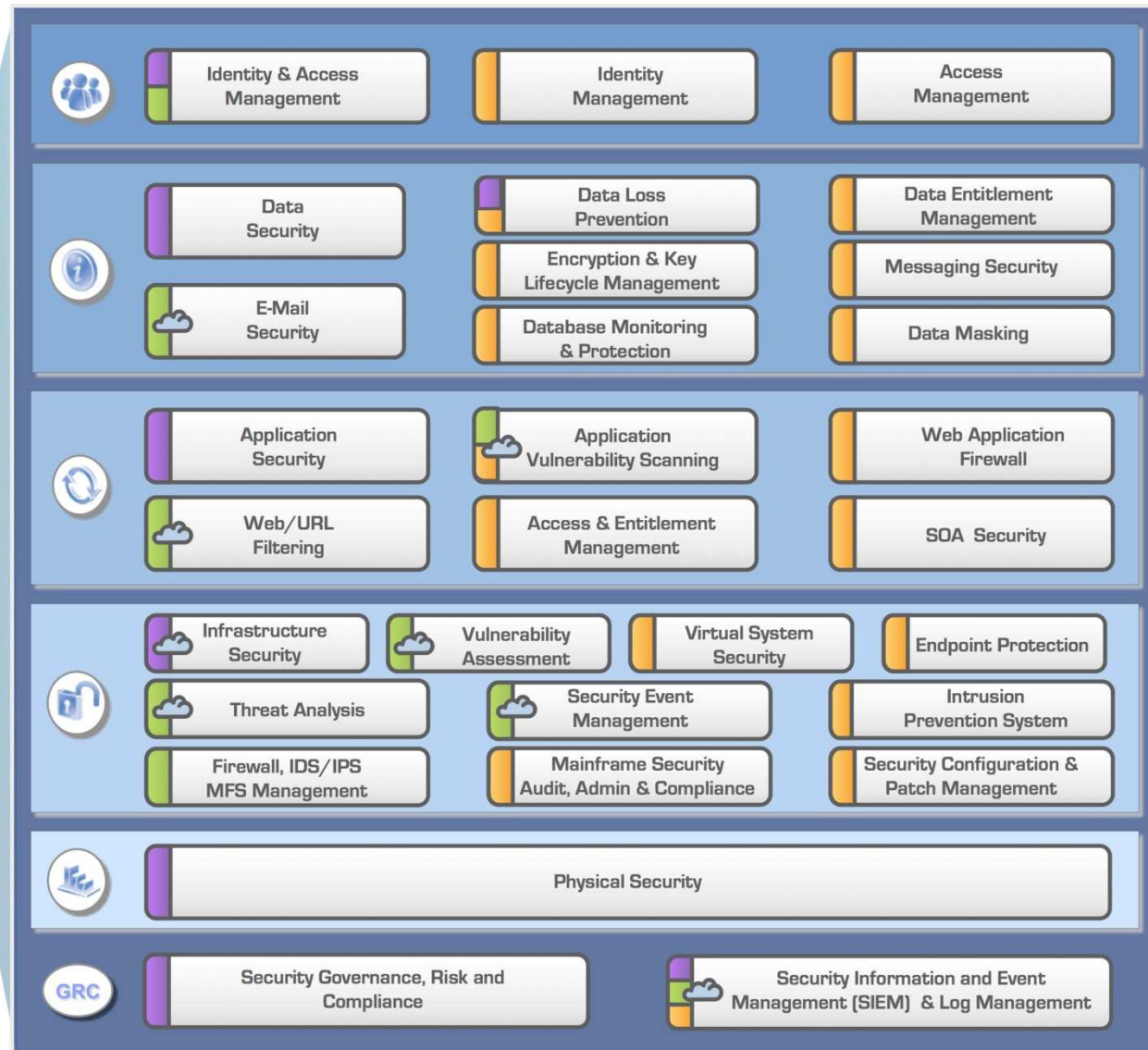
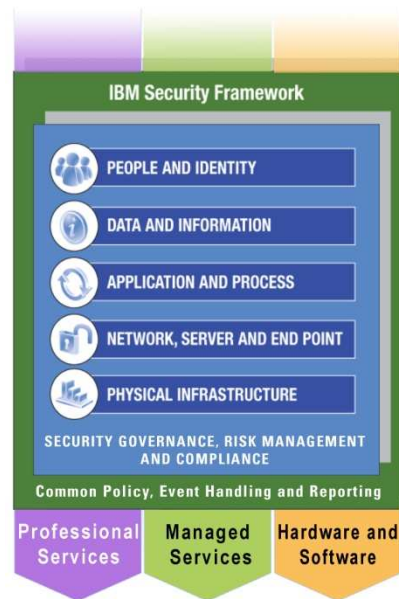
Powered by IBM Research



IBM Security Framework



- Professional Services
- Managed Services
- Products
- Cloud Delivered



InfoPlanet



IBM acquisitions included in the Security Portfolio



- **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.
- ...



InfoPlanet



Security governance, risk management and compliance

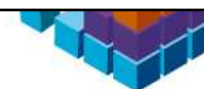


BUSINESS VALUE

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

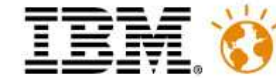


	Security Strategy Design	Pen Testing & Vuln. Assessment	Sec. Compliance Assessment	Incident Response
Business Challenge	Design and implement secure deployment strategies for advanced technologies such as Cloud, virtualization, etc.	Identify and eliminate security threats that enable attacks against systems, applications and devices	Perform security compliance assessments against PCI, ISO 27001 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	PCI Assessors ISO e Law Compliance assessment	Policy definition services; CERT team
Managed Services		App Vulnerability and Source Code Scanning OnDemand		Managed Protection Services



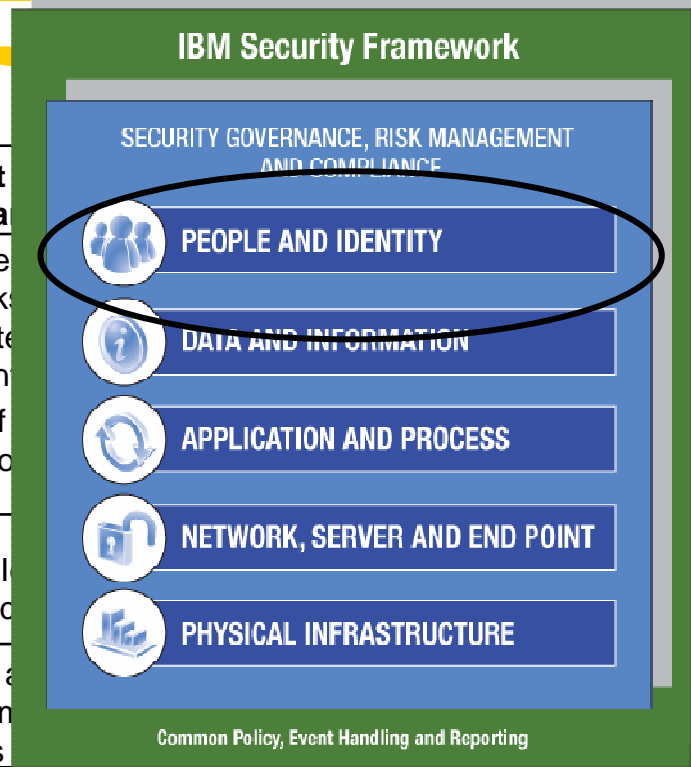


People and identity



BUSINESS VALUE

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



	Cost Management		to	Auditing, reporting and managing access to resources
Business Challenge	<ul style="list-style-type: none"> On average, it takes 2 weeks to get all system accounts secured 30% of password resets require a call 		end 0 ent es	<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	<ul style="list-style-type: none"> Tivoli® Identity Assurance 		y	<ul style="list-style-type: none"> Tivoli Identity and Access Assurance, Tivoli Security Information and Event Manager
Professional Services	<ul style="list-style-type: none"> Identity and Access Management Services 		nal	<ul style="list-style-type: none"> Compliance Assessment Services, Privileged Identity Management
Managed Services	<ul style="list-style-type: none"> Managed Identity Management 	Professional services Managed services Hardware and software	ent	<ul style="list-style-type: none"> Managed User Monitoring and Log Management



InfoPlanet



Data and information



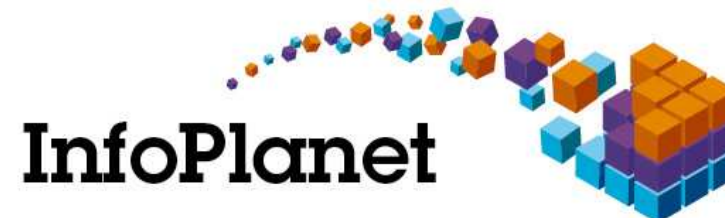
BUSINESS VALUE

Understand, deploy and properly manage sensitive business data

	Protecting Critical Databases		Business and Monitoring Data Access and Preventing Data Loss
Business Challenge	<ul style="list-style-type: none"> Mitigate threats against databases from external attacks and internal privileged users 		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Guardium Database Monitoring & Protection 		<ul style="list-style-type: none"> Data Loss Prevention; Tivoli Security Information and Event Manager
Professional Services	<ul style="list-style-type: none"> Data Security Assessment Services 	<ul style="list-style-type: none"> Professional services Managed services Hardware and software 	<ul style="list-style-type: none"> Data Security, Compliance Assessment Services

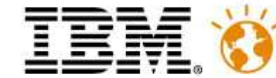
This is not intended to be a comprehensive list of all IBM products and services

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





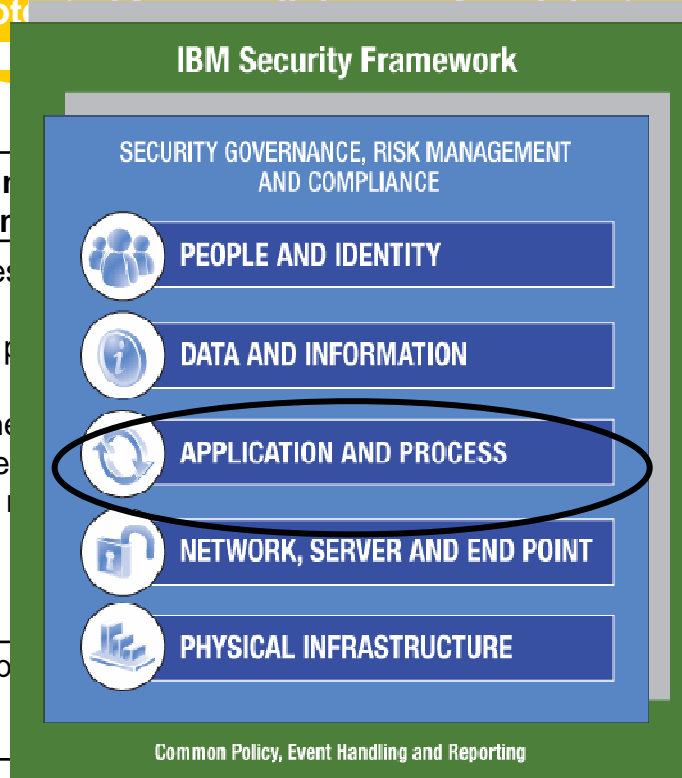
Application and process



BUSINESS VALUE

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

Keep applications secure, protected, and hardened against failure



	Security in Development	Adding App Controls	Providing SOA Security
Business Challenge	<ul style="list-style-type: none"> Vulnerabilities early in the development process are orders of magnitude cheaper to fix versus after application is deployed 	<ul style="list-style-type: none"> Reducing time to market, up to their application development costs or coding access and their underlying infrastructure 	<ul style="list-style-type: none"> Establishing trust and high performance for services that span corporate boundaries is a top priority for SOA-based deployments
Software	<ul style="list-style-type: none"> Rational® AppScan 	<ul style="list-style-type: none"> Identity and Assurance 	<ul style="list-style-type: none"> WebSphere® DataPower®; Tivoli Security Policy
Professional Services	<ul style="list-style-type: none"> Secure App Development Process Enablement App Vulnerability and Source Code Scanning 	<ul style="list-style-type: none"> Managed Vulnerability Scanning 	<ul style="list-style-type: none"> Managed Access Control





Network, server and end point



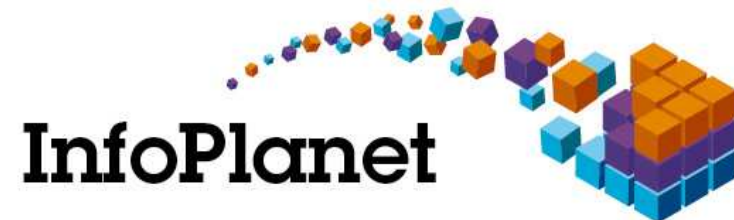
BUSINESS VALUE

Optimize service availability by... Optimize, technology and process

	Protecting...	IBM Security Framework	Protecting works	Protecting Mainframes
Business Challenge	•Mitigate the... prevent data	<p>SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE</p> <p>PEOPLE AND IDENTITY</p> <p>DATA AND INFORMATION</p> <p>APPLICATION AND PROCESS</p> <p>NETWORK, SERVER AND END POINT</p> <p>PHYSICAL INFRASTRUCTURE</p> <p>Common Policy, Event Handling and Reporting</p>	... network threats and data loss	•Mitigate threats against mainframes; protect against vulnerabilities from configuration; contain the privileged users
Software	•Server Protection Server Protection VMWare		... Network Intrusion Detection System	•Tivoli® zSecure suite
Professional Services	•Server security security as services		... Network security management	
Managed Services	•Managed IBM Privileged User	<p>Professional services</p> <p>Managed services</p> <p>Hardware and software</p>	... Managed Network	

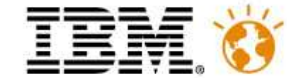
This is not intended to be a comprehensive list of all IBM products and services

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





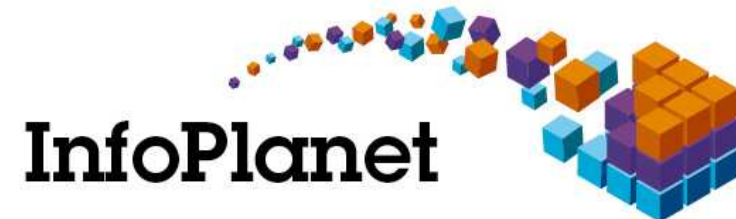
Physical infrastructure



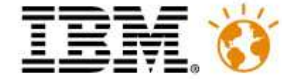
BUSINESS VALUE

Provide actionable intelligence for physical infrastructure security

Business challenge	<ul style="list-style-type: none"> • Legacy systems, interconnected infrastructure 		<p>Professional services</p> <p>Managed services</p> <p>Hardware and software</p>	Command and Control	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • IT Security partnerships 			<ul style="list-style-type: none"> • Command Control Center Solution 	
Professional Services	<ul style="list-style-type: none"> • Base Surveillance services 			<ul style="list-style-type: none"> • Command Control Center Solution Services 	



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

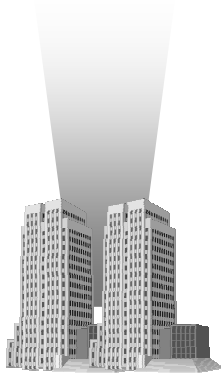


X-Force Threat Analysis Service

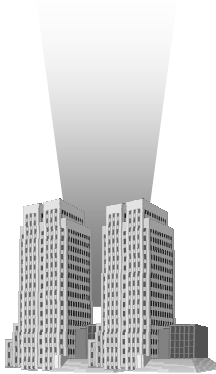
Subscription service

Cloud based

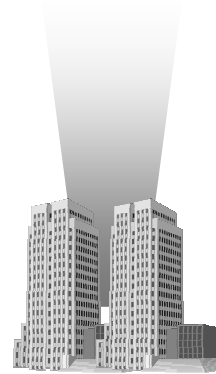
Monitoring and management



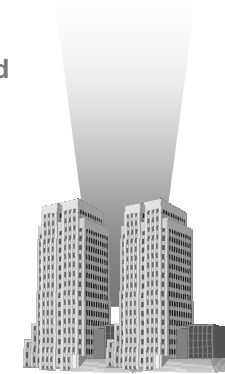
Offsite management of logs and events from IPS's, Firewalls and OSs



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



InfoPlanet

IBM has unmatched global and local expertise in security



3,000+ security and risk management patents

InfoPlanet



IBM X-Force Research and Development

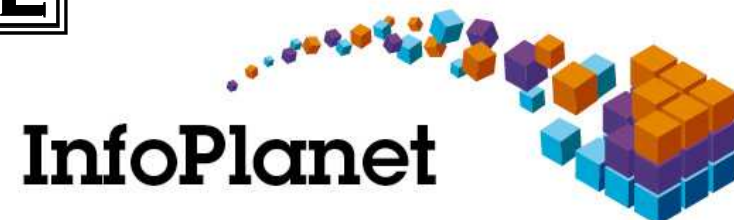


- **What does it do?**

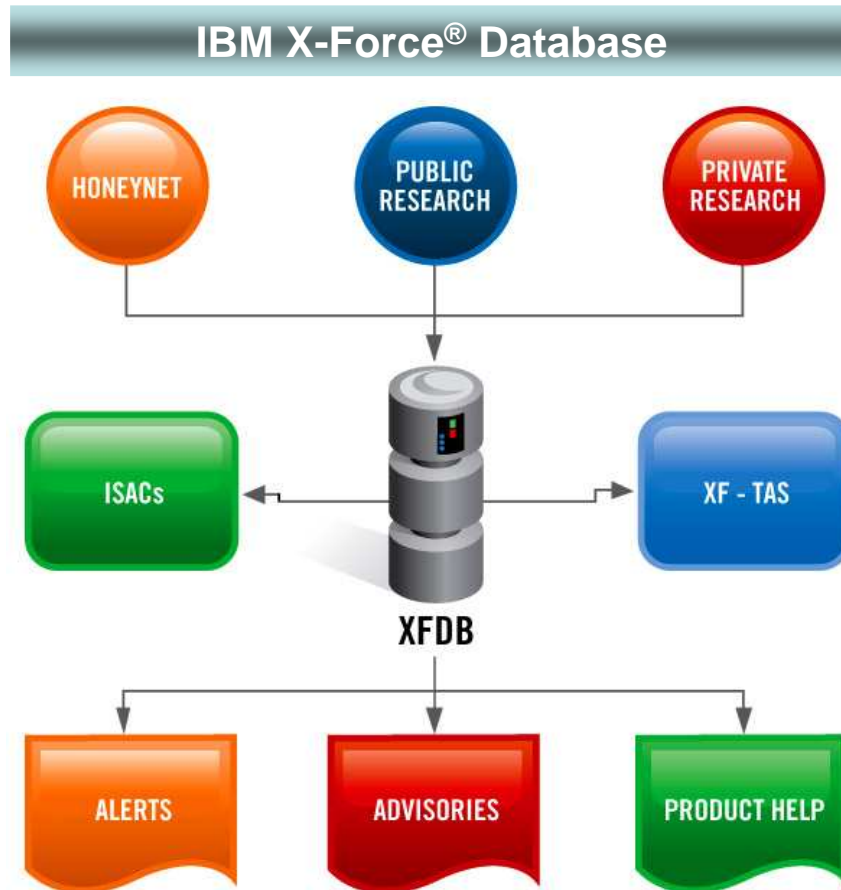
- Researches and evaluates vulnerabilities and security issues
- Develops assessment and countermeasure technology for IBM security offerings
- Educates the public about emerging Internet threats

- **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

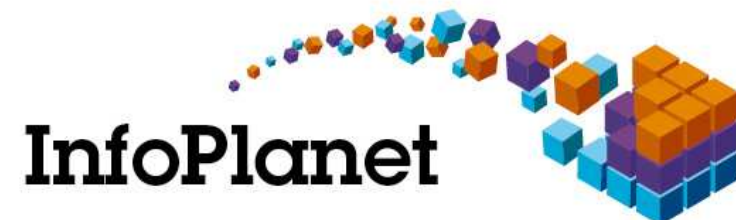


Most comprehensive vulnerability database in the world

- 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

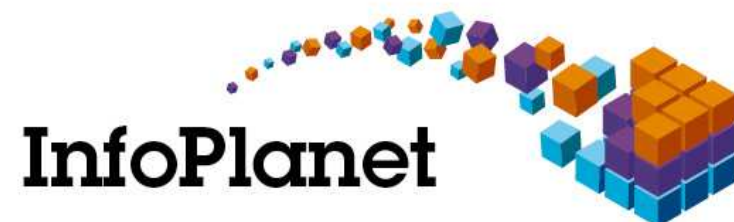


IBM continues to research and test new, more robust and more focused approaches to enterprise security



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



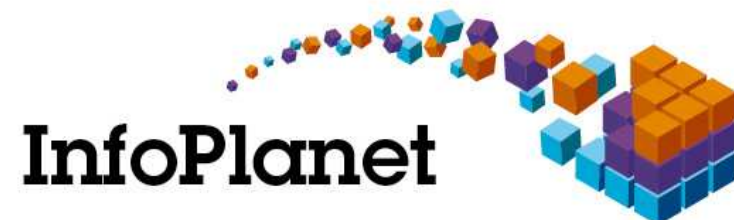
- Mine intelligence from logs and audit records from multitude of event sources
- Consolidate and correlate events and data at line speeds and present them to the analyst in a meaningful manner
- Put control back into the hands of decision makers, such as security analysts, by taking over repetitive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



Resources



<http://www-03.ibm.com/security/started.html>

The screenshot shows the IBM website's security section. At the top, there's a navigation bar with 'Home', 'Solutions', 'Services', 'Products', 'Support & downloads', and 'My IBM'. A search bar is also present. The main heading reads 'Built in. Not bolted on. Smarter security solutions from IBM' with an illustration of a head containing gears. Below this is a navigation menu with 'Overview', 'Getting Started', 'Threat Landscape', 'Security Compliance', and 'Resources'. The 'Secure by Design.' section includes a paragraph explaining the concept, a list of four elements supporting secure design, and a video player titled 'IBM Emphasizes the Importance of Secur...' by IBM Security Solutions. To the right, there's a 'News and Announcements' sidebar with several news items.

Built in. Not bolted on.
Smarter security solutions from IBM

Secure by Design.

We believe that security is intrinsic to your business processes, development and daily operations. It should be factored into the initial design of any IT or critical infrastructure solution, not bolted on after the fact. This concept we call "Secure by Design" means that cost-effective security begins with the creation of secure systems from the start. When you build security into the overall design of a system whether it be an employee onboarding process or a cloud delivery model – it allows you to create an agile environment that will embrace changes within the security landscape.

There are four elements which support a secure design:

- Understanding of the design point for security
- Knowledge of the threats in the solution's operating environment
- Utilization of enabling technologies that provide or enforce secure behaviors
- Ongoing validation of the secure design

This preemptive approach of IBM Security Solutions can allow you to securely, safely, and confidently adopt new forms of technology. Cloud computing, virtualization, smart grids, business models like tele-working and outsourcing, can be more safely leveraged for cost benefit, innovation and shorter time to market.

IBM Emphasizes the Importance of Secur...
by IBM Security Solutions

News and Announcements

- ESG Report - Databases at Risk
- IBM Takes Action to Improve Cloud Security
- Independent Research Firm Names IBM a Leader in Managed Security Services
- IBM's New Cloud Offering Helps Companies Improve IT Service Desk Operations

The Redbooks cover features the IBM logo at the top right. The title 'IBM Security Solutions Architecture for Network, Server and Endpoint' is prominently displayed. Below the title, three bullet points highlight the content: 'Comprehensive discussion of the IBM Security Framework and IBM Security Blueprint', 'Detailed insight into the threat and vulnerability landscape', and 'Extensive solution architecture and component introduction'. A large graphic of a red globe with a black swoosh is on the right. The authors' names are listed: Axel Buecker, Kent Browne, Louis Foss, Jaco Jacobs, Vladimir Jeremic, Carsten Lorenz, Craig Stabler, and Joris Van Herzele. The Redbooks logo is at the bottom right, and the URL 'ibm.com/redbooks' is at the bottom left.

IBM

IBM Security Solutions Architecture for Network, Server and Endpoint

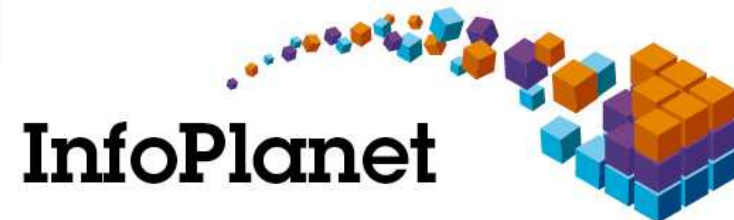
- Comprehensive discussion of the IBM Security Framework and IBM Security Blueprint
- Detailed insight into the threat and vulnerability landscape
- Extensive solution architecture and component introduction

Axel Buecker
Kent Browne
Louis Foss
Jaco Jacobs
Vladimir Jeremic
Carsten Lorenz
Craig Stabler
Joris Van Herzele

Redbooks

ibm.com/redbooks

<http://www.redbooks.ibm.com/astracts/sg247581.html>



Resources



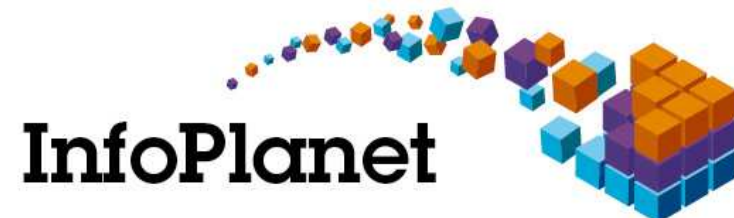
The screenshot shows the homepage of the IBM Institute for Advanced Security. At the top, there is a navigation bar with links for Home, New to The Institute, Security Topics, Community, Events, Resources, Security Tweets, and Login. The main banner features the headline "The new hackers" with a sub-headline "They're organized. Well-funded. And they're gunning for your network." and a "Learn more" link. Below the banner, there are several sections: "Community Login" with an email and password field, "Upcoming Events" listing conferences in Las Vegas, Orlando, and New York, "Meet our Experts" featuring Harriet Pearson and Jack Danahy, and three columns for "Learn", "Connect", and "Engage". A central blue banner reads "Security In A Smarter Planet: Critical Infrastructure, Stuxnet And Advanced Threats".

- 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

The graphic features a stylized globe composed of concentric, multi-colored lines (red, green, blue, yellow) with a red core, set against a white background with a black border.

<http://www.instituteforadvancedsecurity.com/>



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.

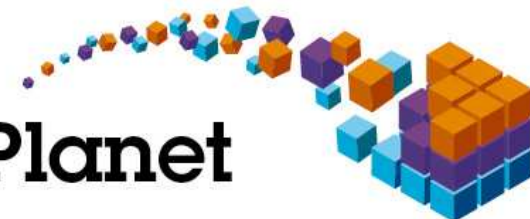
- ✓ *IBM is the Trusted Partner delivering products and services recognized for leadership in IT security*
- ✓ *IBM's philosophy of Secure By Design; Factor **Security** and **Privacy** into the initial design, not bolted on after the fact*
- ✓ *IBM security solutions allow customers to address the 3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



one coordinated voice for security.



InfoPlanet





Grazie @...Voi !



Cesare Radaelli

IBM Security Solutions

Security TT Leader
Italy

Circonvallazione Idroscalo
20090 Segrate, Italy

Tel +39 348 5219272

cesare.radaelli@it.ibm.com