IBM SoftwareNetwork 2013

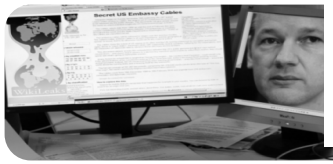
Fare partnership con il Software IBM

Roma, 24 - 25 gennaio 2013

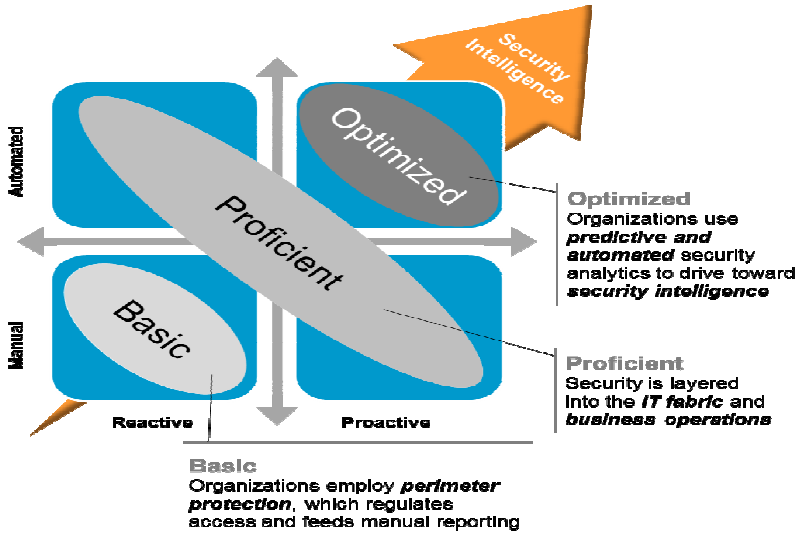
Norberto Gazzoni
IBM Security Systems Channel Manager

IBM Security Systems
L'opportunità per i Business Partner IBM

Il mondo sta diventando più digitalizzato ed interconnesso, aprendo la porta alle minacce emergenti e le perdite di dati…

			IBM Security Solutions Focus
	**DATA EXPLOSION**	Le organizzazioni continuano a muoversi a nuove piattaforme compresi cloud, virtualizzazione, mobile, social business e molto altro ancora	**SECURITY INTELLIGENCE**
	**CONSUMERIZATION OF IT**	Con l'avvento di Enterprise 2.0 e di social business, la linea tra le ore di uso personale e professionale, i dispositivi e dei dati è scomparso	**MOBILE SECURITY**
	**EVERYTHING IS EVERYWHERE**	L'età dei Big Data - l'esplosione di informazioni digitali - è arrivata ed è facilitata dalla pervasività delle applicazioni accessibili da ovunque	**CLOUD SECURITY**
	**ATTACK SOPHISTICATION**	La velocità e la destrezza degli attacchi è aumentata accoppiata con nuove motivazioni della criminalità informatica	**ADVANCED THREAT**

IBM Vi porta nell'Era della **Security Intelligence**



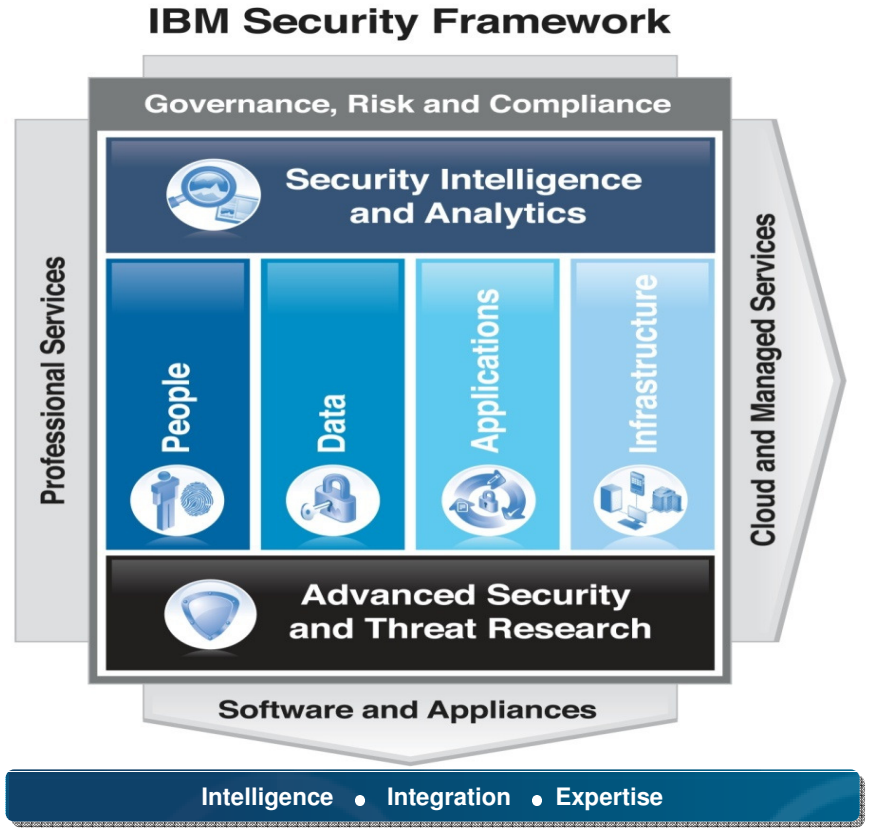
IBM Security Solutions

Le organizzazioni hanno bisogno di un nuovo approccio alla sicurezza che sfrutta l'intelligenza per stare al passo con l'innovazione.
IBM Security Intelligence guida il cambiamento da una strategia "point-product" ad un framework integrato di sicurezza aziendale:
La traduzione dei dati di Security in conoscenze fruibili:

- **Riduce i rischi ed i costi commerciali**
- **Innovazione con agilità e sicurezza**
- **Migliora la continuità operativa**

13 Miliardi di eventi di Security gestiti giornalmente	1,000 Security Patents	9 Security Operations Centers	600 Security Sales Professionals	11 Laboratori di sviluppo per Soluzioni di Security

IBM Security: Fornire l'intelligenza, l'integrazione e le competenze in un Framework completo



Think Integrated.

Incrementa la Accuratezza e la consapevolezza nella Security

- Individuare e prevenire minacce avanzate
- Una maggiore visibilità e consapevolezza della situazione
- Condurre indagini complete sugli incidenti

Semplicità di Gestione

- Semplificare la gestione del rischio e il processo decisionale
- Migliorare le capacità di controllo e di accesso

Riduzione dei costi e complessità

- Fornire una rapida installazione, un minore TCO lavorando con un unico partner strategico, con un ampio portafoglio integrato

Fattori chiave che influenzano il business del sw di sicurezza

Non è più sufficiente proteggere il perimetro - attacchi sofisticati stanno aggirando le difese tradizionali, le risorse IT sono in movimento al di fuori del firewall, e le applicazioni aziendali ed i dati sono sempre più distribuite su diversi dispositivi

1. Advanced Threats

Sofisticati, attacchi mirati, volti a ottenere l'accesso continuo alle informazioni critiche, sono in aumento nella severità e nella ricorrenza.

Advanced Persistent Threats
Stealth Bots Designer Malware
Targeted Attacks Zero-days

2. Cloud Computing

La sicurezza è una delle preoccupazioni principali del cloud, in quanto i clienti drasticamente ripensano il modo in cui sono state progettate, distribuite e consumate le risorse IT.

IBM SmartCloud
vmware
salesforce

BIG DATA

Enterprise Customers

3. Mobile Computing

Come gestire dispositivi di proprietà dei dipendenti e garantire connettività alle applicazioni aziendali sono esigenze da indirizzare per i CIO ampliando il supporto per dispositivi mobili.

Windows Phone

4. Regulations and Compliance

Le pressioni normative e le conformità continuano ad aumentare insieme alla necessità di memorizzare i dati sensibili e le aziende diventano suscettibili ai fallimenti di audit.

PCI Security Standards Council
HIPAA
Sarbanes-Oxley
Financial and Accounting Disclosure Information

Mobile Security

- Know who is connecting from mobile devices
- Maintain better control over new devices

"We manage 20,000 endpoints across 49 countries and six continents, supporting PCs, Macs, servers, and just about every flavor of mobile device. With our old solution, we had two engineers managing 2,500 endpoints. Now we need only one engineer managing 20,000 endpoints and we have 98 percent compliance against our policy baselines." — Shahin Pirooz, Executive Vice President, CTO CenterBeam

People

- ***IBM Security Access Manager for Cloud and Mobile*** provides risk-based access control for mobile users. Built in risk scoring support improves assurance of mobile and on-premise user access. Strong mobile authentication is enhanced with One-Time Password (OTP) capability
- ***IBM Endpoint Manager for Mobile Devices*** provides customizable enrollment questions that can be used for reporting, policy targeting, and requiring employees to accept the organization's mobile policy prior to authorization

Data

- ***IBM Security Access Manager for Cloud and Mobile*** provides access to a select subset of corporate data, based on the risk profile of the interaction
- ***IBM Endpoint Manager for Mobile Devices*** provides advanced data separation and device enrollment for a more secure BYOD program

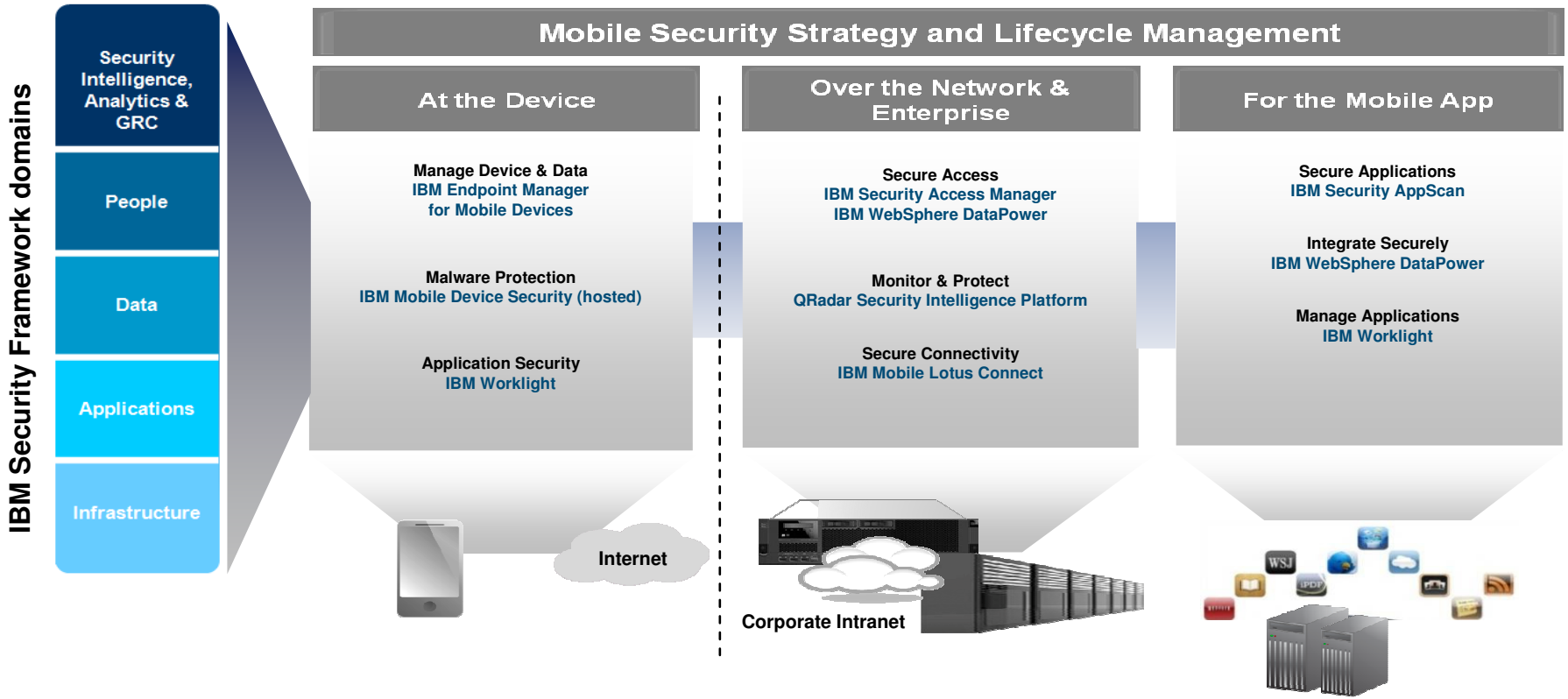
Applications

- ***IBM Security Access Manager for Cloud and Mobile*** provides integration of access management into mobile application development with IBM Worklight

Infrastructure

- ***IBM Endpoint Manager for Mobile Devices*** provides enhanced mobile device control with device configuration baselines to help address internal and regulatory policy and compliance requirements

Securing the Mobile Enterprise



Cloud Security

- Reduce security exposures in Cloud environments
- Integrate event data

"Besides the cost reduction, one major advantage is that we will be able to offer cloud-based services for our customers with confidence."-Mr. Masaru Ito, Sales and Business Planning Leader, Cloud Services Division EXA Corporation

People

- ***IBM Security Access Manager for Cloud and Mobile*** provides identity mediation across cloud service providers, and enables federated SSO
- ***IBM Security Privileged Identity Manager*** controls and tracks shared access to sensitive user IDs and demonstrates compliance
- ***IBM Security Identity Manager*** provides rapid integration with cloud, SaaS and on-premise services across heterogeneous environments

Data

- ***IBM Security Privileged Identity Manager*** helps prevent misuse of privileged identities to servers, applications and databases

Applications

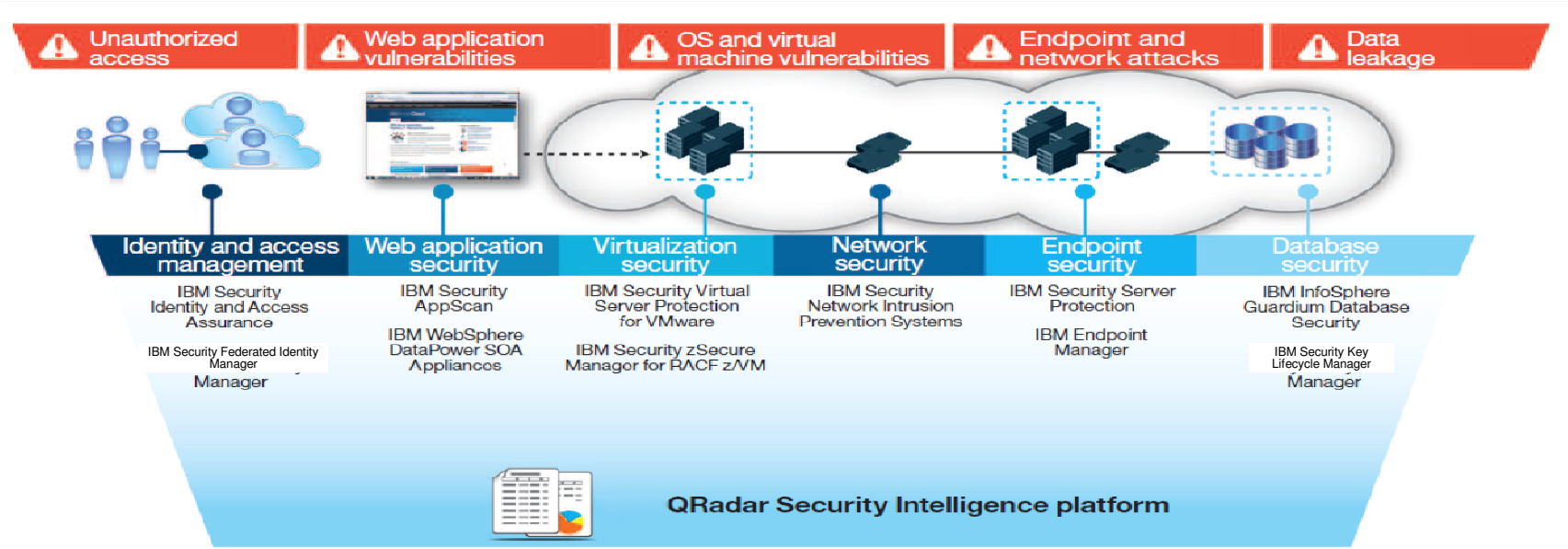
- ***QRadar Security Intelligence Platform*** utilizes cloud infrastructures to monitor activity across geographically distributed locations, such as bank branches and retail stores, for greater threat detection

Infrastructure

- ***IBM Security zSecure*** integrates mainframe event data into QRadar for enhanced monitoring
- ***IBM SmartCloud for Patch Management*** helps reduce threat of attack and compliance risk by slashing remediation cycles from weeks to hours. It helps

IBM Delivers Security Solutions Across all Cloud Security Domains

IBM protects against common cloud risks with a broad portfolio of flexible, layered security solutions



Protect against threats, regain visibility and demonstrate compliance with activity monitoring, anomaly detection and security intelligence

Data Security

- Real-time analytics of sensitive data access
- Automate compliance and data security management

Data Security

"We are thoroughly impressed with IBM InfoSphere Guardium Data Redaction, its capabilities and accuracy rates. This technology is helping us comply with PCI-DSS requirements for historical content management of documents and forms."

— Leslie Ross, Head of BCIT, Aviva UK Health

People

- ***IBM InfoSphere Optim Data Masking*** enforces data privacy policies and safeguards data by masking data using out of the box services or through customized masking routines. Sensitive data can be de-identified on demand
- ***IBM InfoSphere Guardium*** logs user activity for compliance reporting, and prevents access, if appropriate

Data

- ***IBM InfoSphere Guardium*** enhances security intelligence with database security insights and protection. It monitors and audits Hadoop activity in real-time to support compliance requirements and protect data. And IBM InfoSphere Guardium automates compliance controls across all data environments

Applications

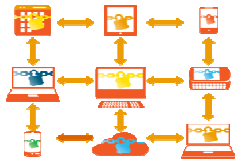
- ***IBM InfoSphere Guardium*** optimizes data security for DB2 on System i and DB2, IMS and VSAM on System z

Infrastructure

- ***IBM InfoSphere Guardium*** provides expanded integration and automation to further reduce TCO in large enterprise-wide deployments
- ***IBM Security Key Lifecycle Manager*** supports updated key management interoperability standards for non-IBM storage devices in multi-vendor organizations

IBM's Data Security Strategy

Data Security



- Protect data in any form, anywhere, from internal or external threats
- Streamline regulation compliance process
- Reduce operational costs around data protection

Security Solutions

integrate

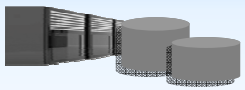
Governance, Security Intelligence, Analytics

Audit, Reporting, and Monitoring

Policy-based Access and Entitlements

Data Discovery and Classification

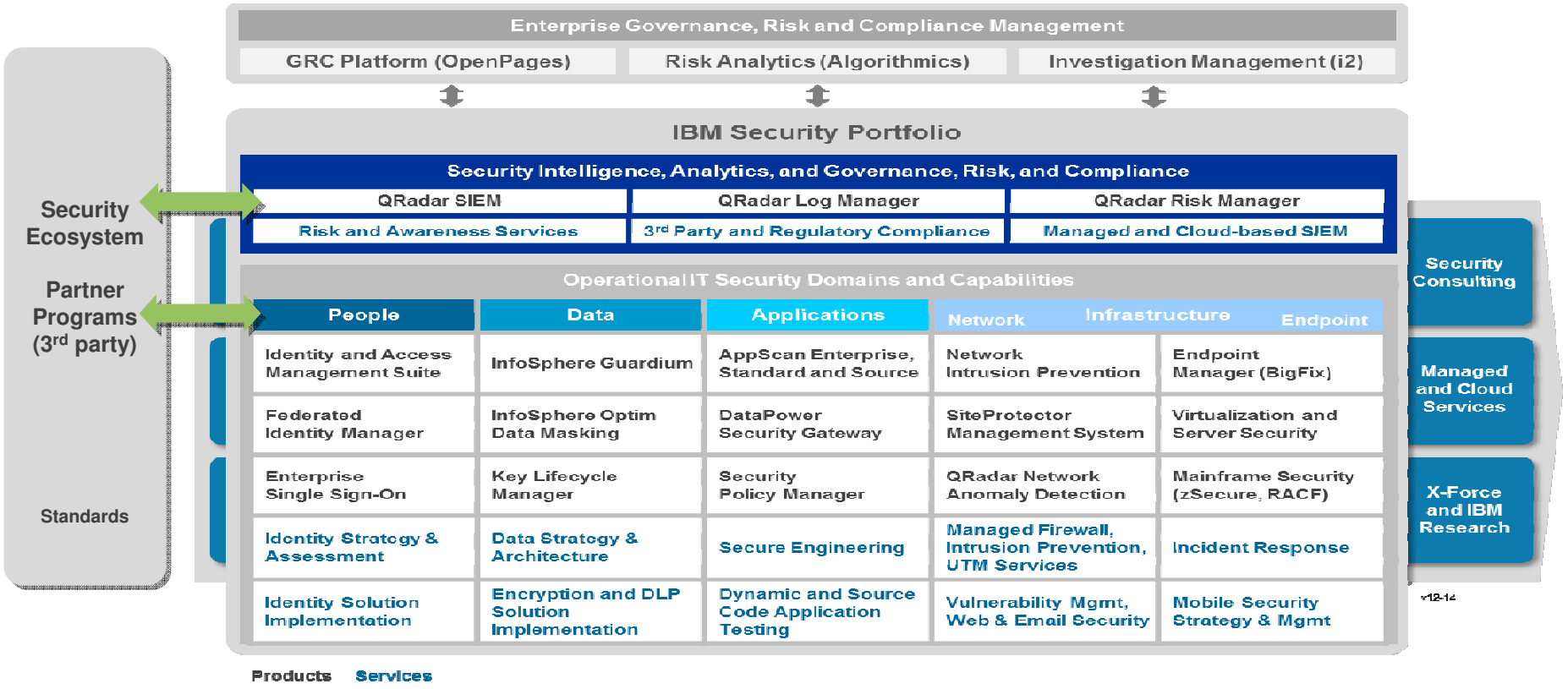
Enforcement

Data at Rest	Data in Motion	Data in Use
Protection & Encryption	Network Loss Prevention	Endpoint Loss Prevention
		
Stored (Databases, File Servers, Big Data, Data Warehouses, Application Servers, Cloud/Virtual ..)	**over Network** (SQL, HTTP, SSH, FTP, email,. ...)	**at Endpoint** (workstations, laptops, mobile,...)

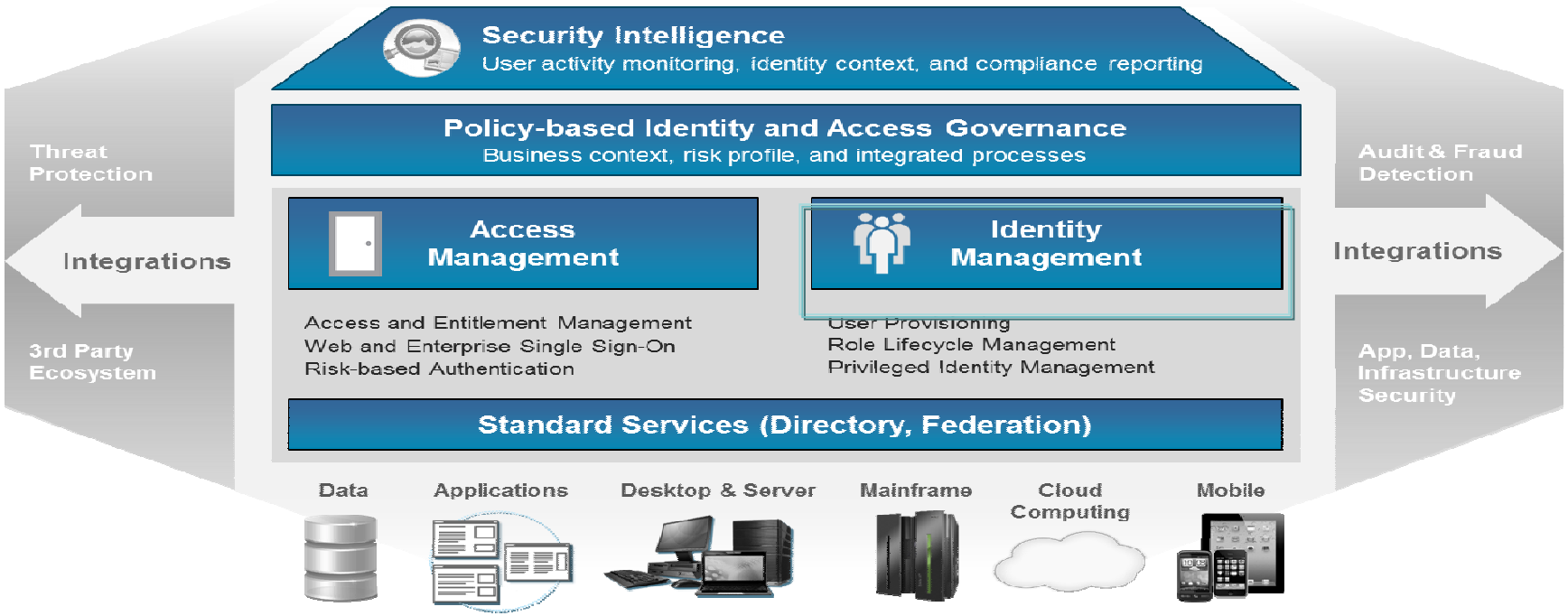
integrate

IT & Business Process

Un Portfolio completo in tutti i domini di sicurezza



IBM Identity and Access Management - Visione e Strategia



Gestire e ampliare l'identità aziendale in tutti i domini di sicurezza

Introduciamo l'IBM Security Privileged Identity Manager

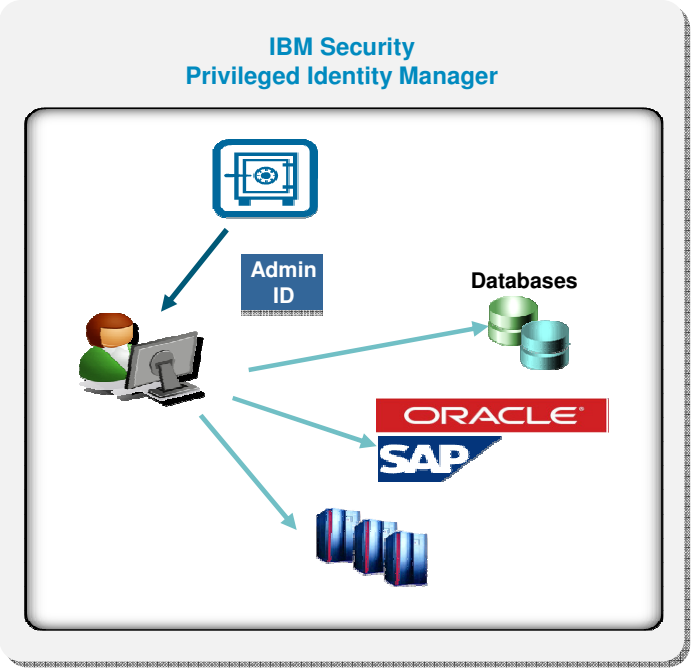
Gestione centralizzata, verifica e controllo delle identità condivise in tutta l'azienda

Vantaggi principali della release

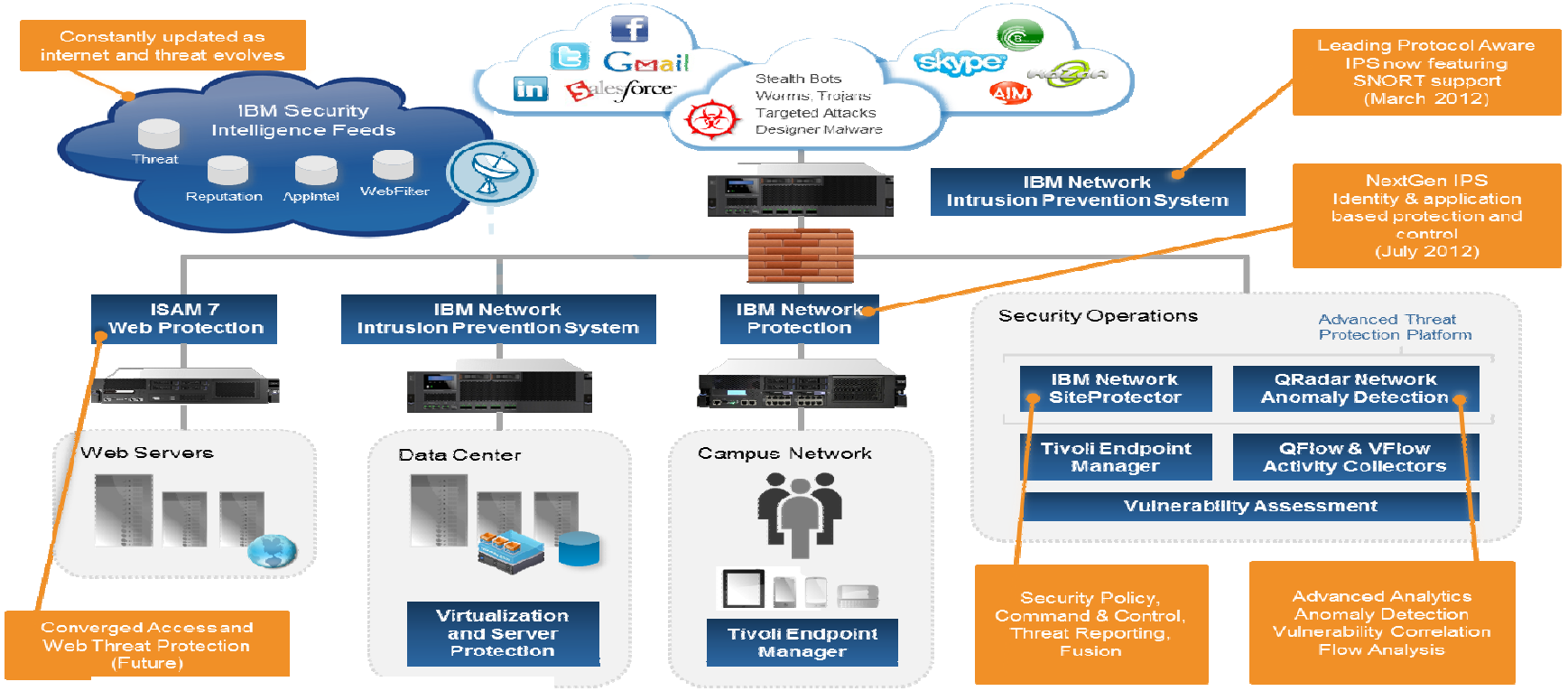
- ***Controllo accesso condiviso per ID utente sensibili***
  - *Check-in / check-out usando secure credential vault*
- ***Richiesta, approvazione e ri-validazione degli accessi privilegiati***
  - *Riduzione dei rischi, migliorare la conformità*
- ***Monitorare l'utilizzo delle identità condivise***
  - *Provide accountability*
- ***Gestione automatizzata delle password***
  - *Automatizzare il checkout degli ID, automatizzare la reimpostazione della password per eliminare il furto di password*

IBM security solution

- ***Privileged Identity Management (PIM), la nuova soluzione che fornisce una gestione completa delle identità e la funzionalità di Enterprise Single Sign-On per utenti privilegiati***

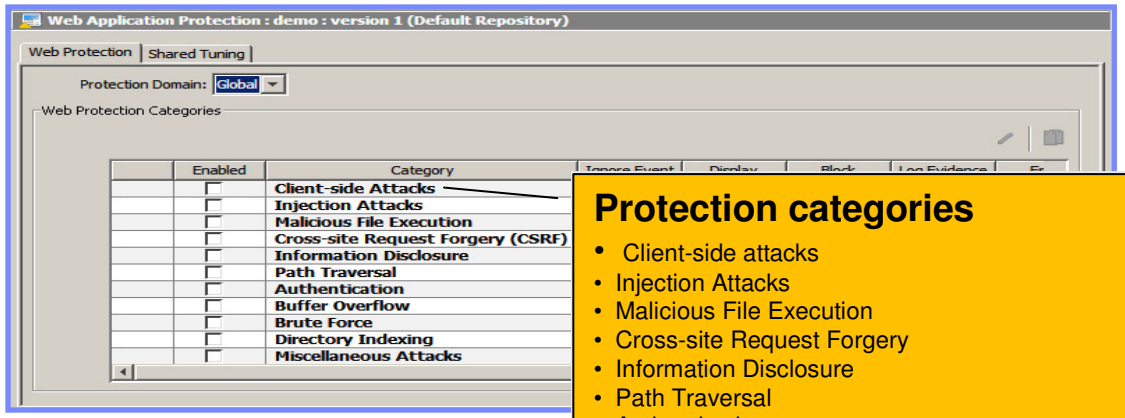


Advanced Threat Protection Platform



La protezione delle Applicazioni Web ed Appscan

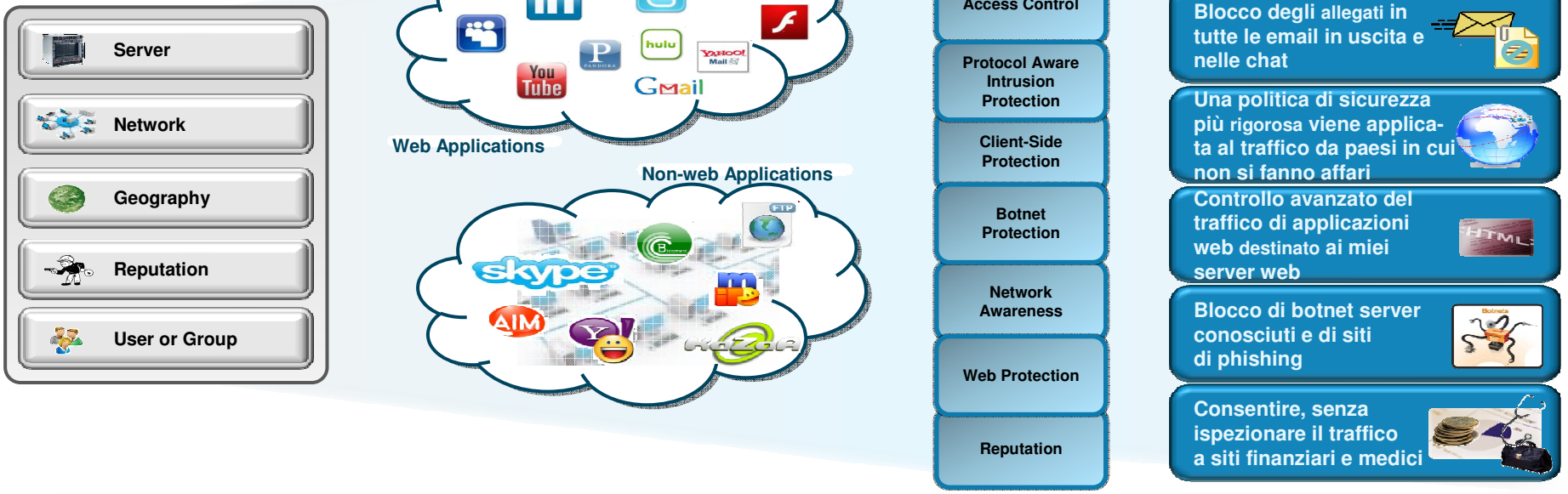
- ✓ **L'analista di rete crea una virtual patch attivando una policy IPS per la protezione delle applicazioni Web**
- ✓ **L'analista di rete abilita categorie di protezione policy based in base ai tipi di vulnerabilità scoperte con AppScan**



Protection categories

- Client-side attacks
- Injection Attacks
- Malicious File Execution
- Cross-site Request Forgery
- Information Disclosure
- Path Traversal
- Authentication
- Buffer Overflow
- Brute Force
- Directory Indexing
- Miscellaneous Attacks

L'introduzione di Controlli avanzati



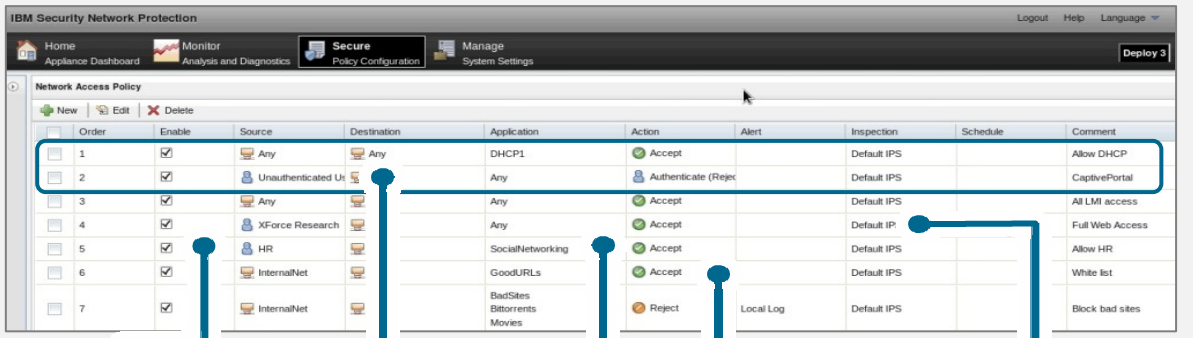
Who	What	Controls	Security
172.29.230.15, 192.168.0.0 /16	80, 443,25, 21, 2048-65535	?	

Completo controllo: Superare l'approccio del semplice Blocco

- **Network Control** per utenti, gruppi, sistemi, protocolli, applicazioni ed azioni delle applicazioni
- **Blocco in evoluzione, siti ad alto rischio**, come phishing e malware con le categorie costantemente aggiornate
- **Comprehensive up-to-date web site coverage** with industry-leading 15 Billion+ URLs *(50-100x the coverage comparatively)*
- **Ricco Supporto per le applicazioni** con più di 1000 applicazioni + e con azioni singole

"We had a case in Europe where workers went on strike for 3 days after Facebook was completely blocked…so granularity is key."

– SecureDevice



Limit the use of social networking, file sharing, and web mail for common users

Allow full access to social networking sites for marketing and HR teams`

Tailored Security Policies for individual uses, groups or networks

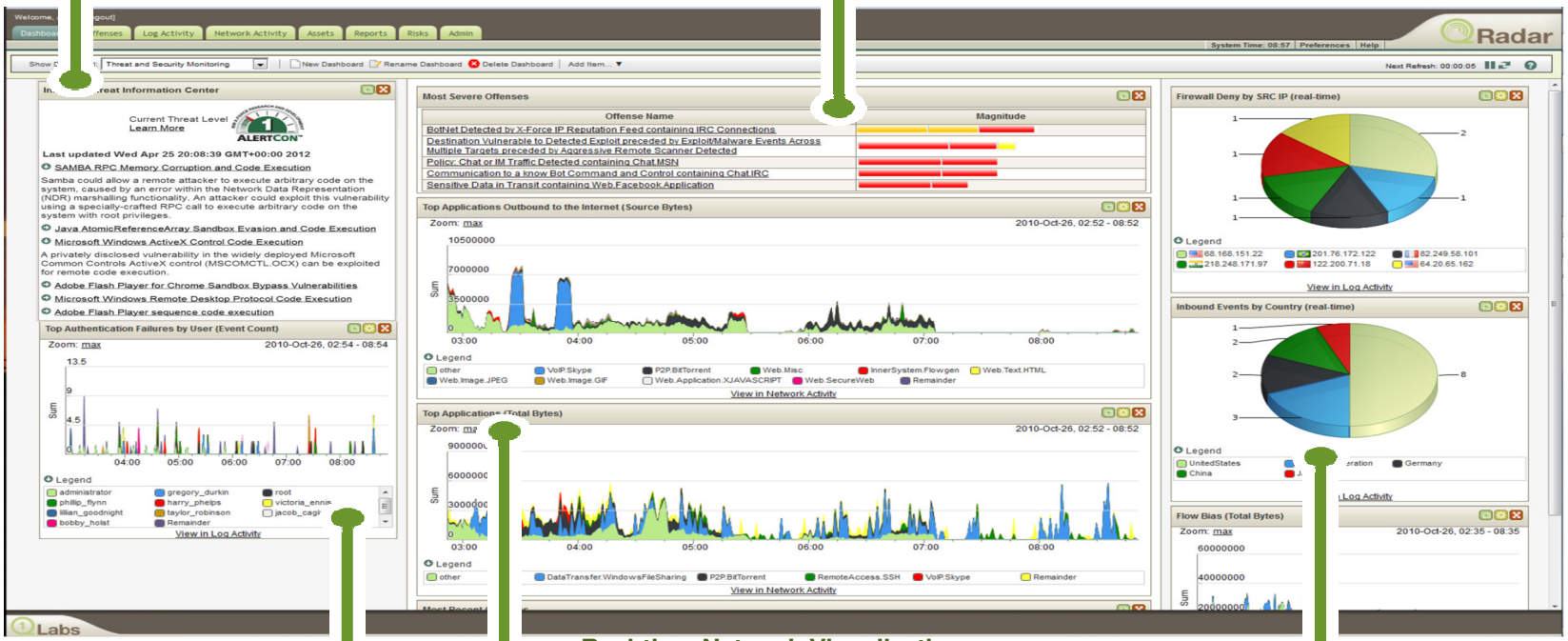
Flexible network access policies controls access to systems and applicable security policy by IP, Port, Protocol and vlan.

Stop broad misuse of the corporate network by blocking sites that introduce undue risk and cost

Q1Labs Q-Radar: Che succede sulla mia rete?

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation



Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events