

Security Intelligence.
Think Integrated.



BANCA POPOLARE
DI MILANO

IBM Security Intelligence: “Sicurezza in Continua Evoluzione”



Angelo Rolfi

Sicurezza e Continuità Operativa
B.ca Popolare di Milano

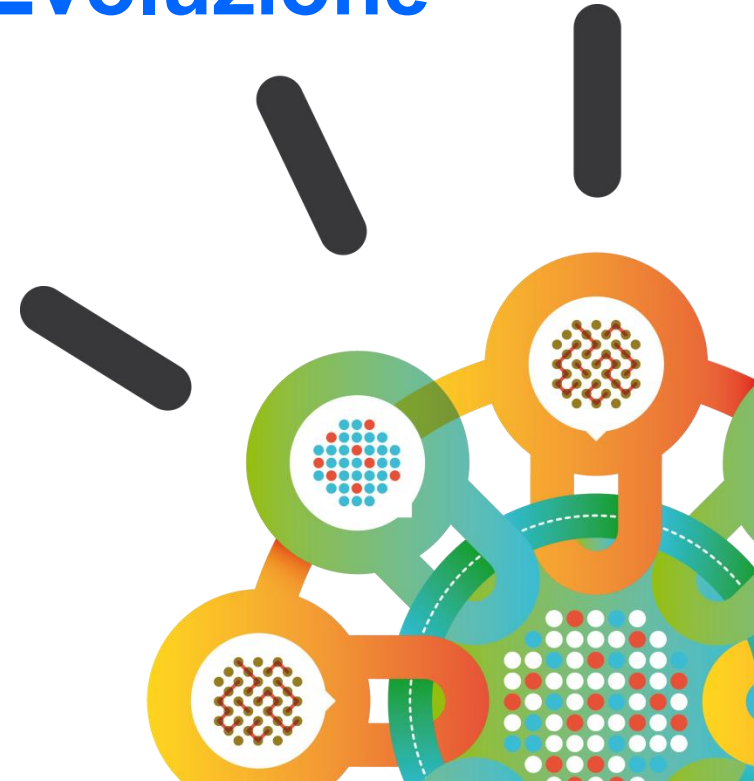
angelo.rolfi@bpm.it



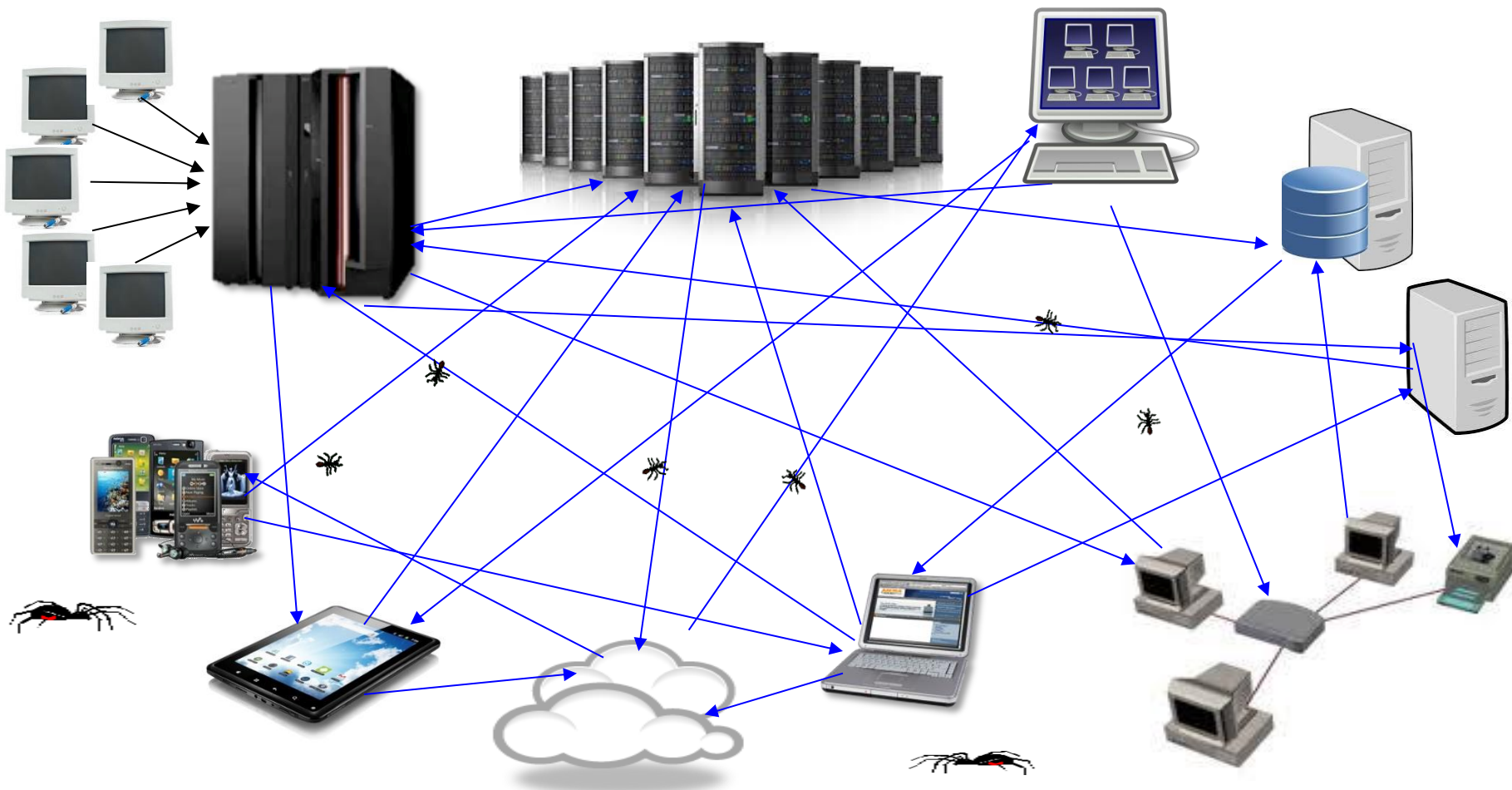
Luigi Perrone

Technical Pre-Sales System Engineer
IBM Security Systems

luigi_perrone@it.ibm.com



L'evoluzione dei sistemi ICT



**Eterogeneità, Interconnessione, Complessità
...e la Sicurezza ???**



Benvenuti nel CyberWorld, ...un mondo non così tanto cordiale !



[SICUREZZA]

Cybercrime Le aziende sotto attacco

Aziende e cyber sicurezza, decisamente un rapporto difficile. Oltre un terzo di quelle mondiali a tutt'oggi non ha ancora approntato un piano di emergenza da seguire per tirarsi fuori dai guai in caso di incidente informatico e solo una piccola percentuale è adeguatamente preparata per

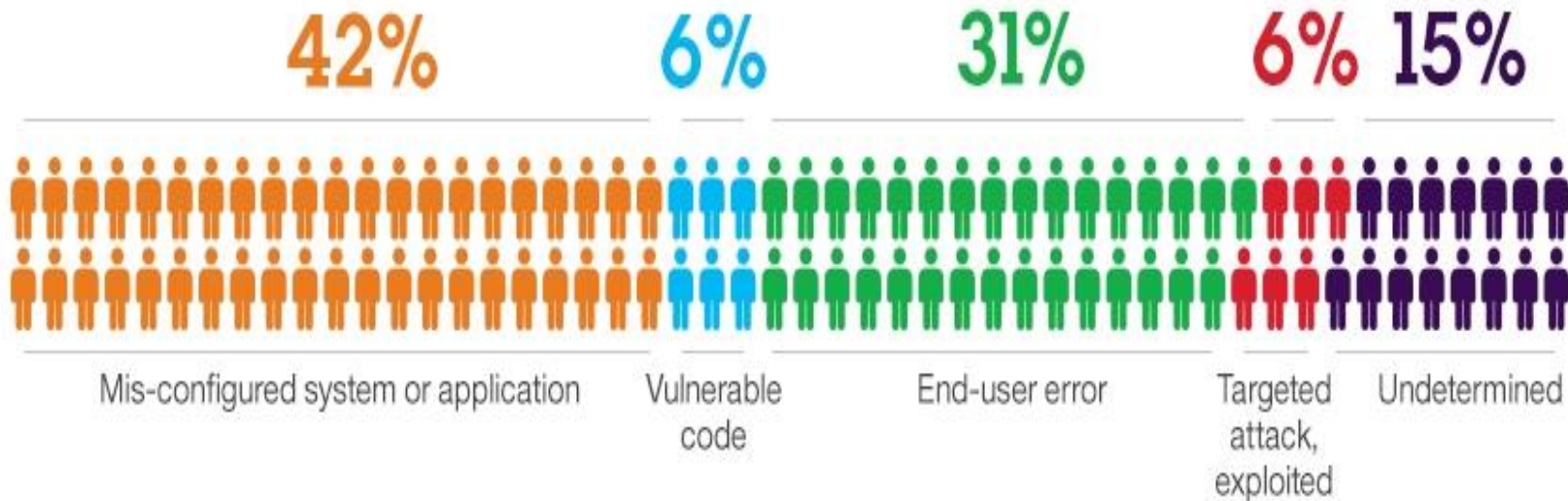
“E’ chiaro che la sicurezza va affidata a personale altamente specializzato e andrebbe considerata come una componente “core” del business aziendale e, dunque, governata all’interno dell’azienda stessa. Ma a volte non è possibile formare un team interno e quindi è meglio affidarsi a partner fidati con cui lavorare a stretto contatto”.

Uno sguardo a numeri e statistiche



The Human Factor: *How Breaches Occur*

Many elements can contribute to the vulnerability of your organization, however none is more prevalent than the human factor, **which accounts for approximately 80%.**



Difese tradizionali si...ma non bastano

Malware



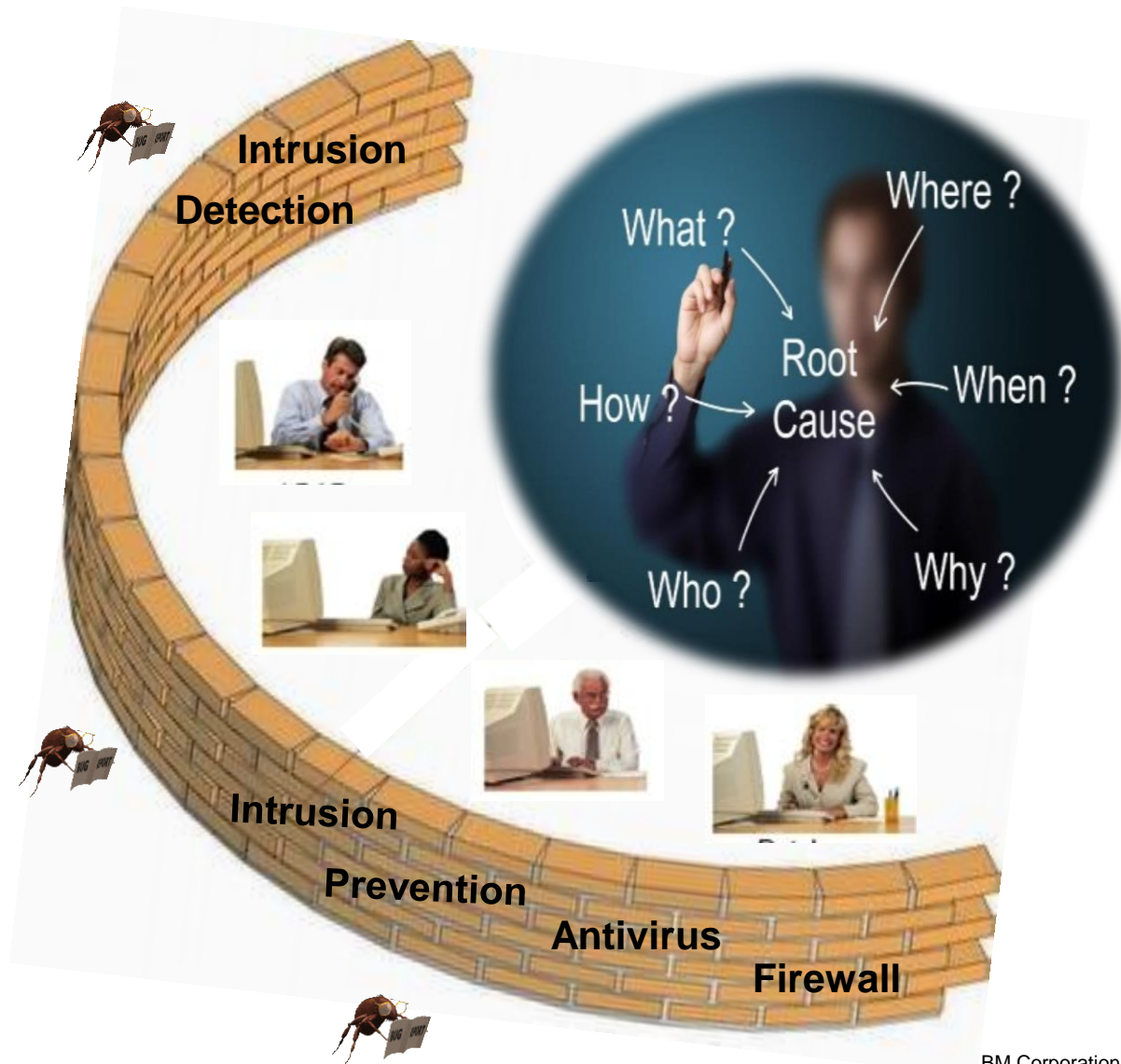
Backdoors



Phishing



Persistence



Un'infrastruttura di controllo solida e reattiva

- Radar**[®]
Log Manager
- Radar**[®]
Network Anomaly
Detection
- Radar**[®]
SIEM
- Radar**[®]
Risk Manager
- Radar**[®]
Vulnerability
Manager



SECURITY INTELLIGENCE



Security Intelligence...integrata !

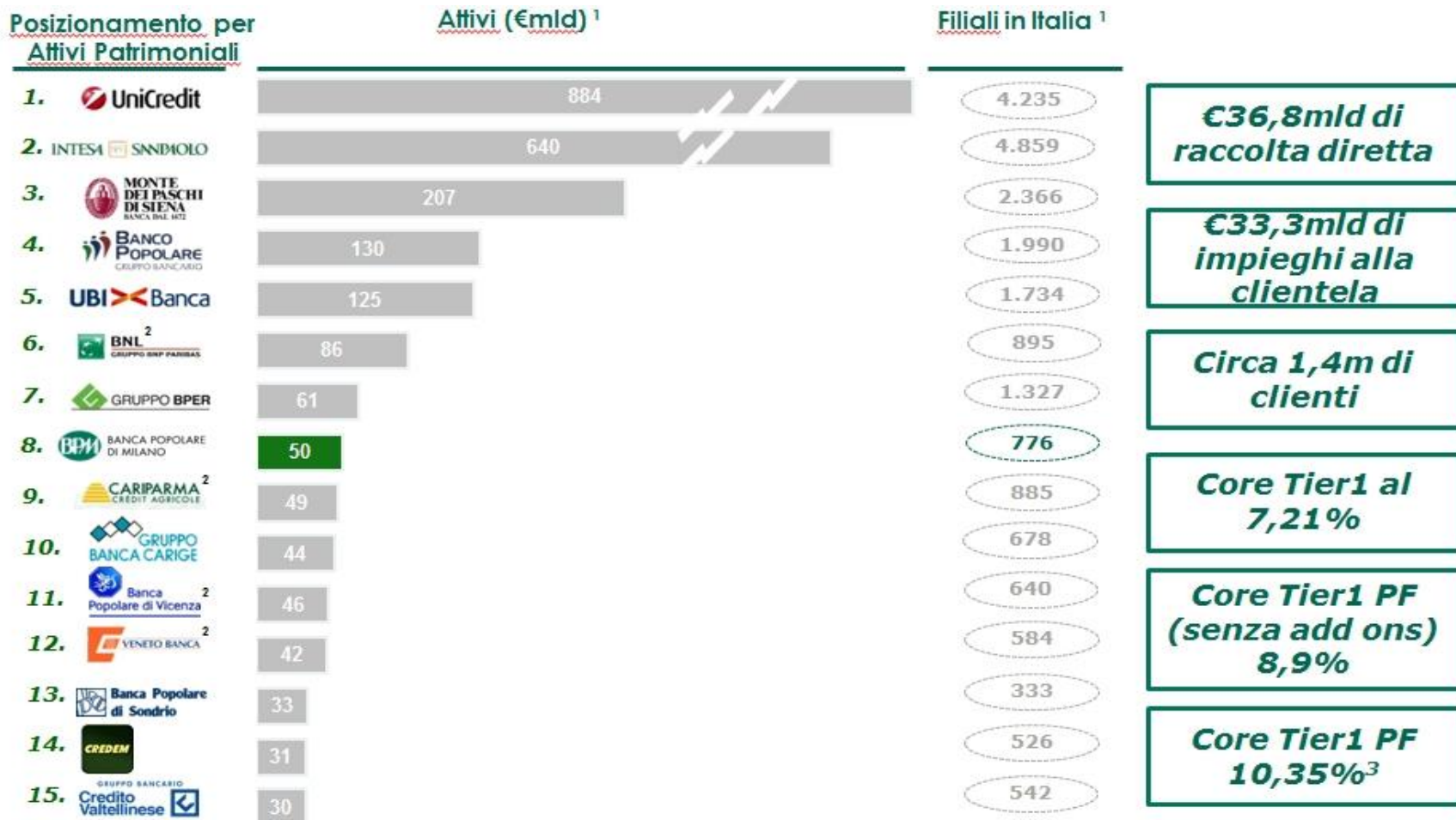


Think Integrated.

Una scelta strategica per la sicurezza



BPM: uno dei più grandi gruppi bancari italiani



Fonte: Bilanci Societari al 31 dicembre 13

1. Dati a Settembre '13

2. Dati a Giugno '13

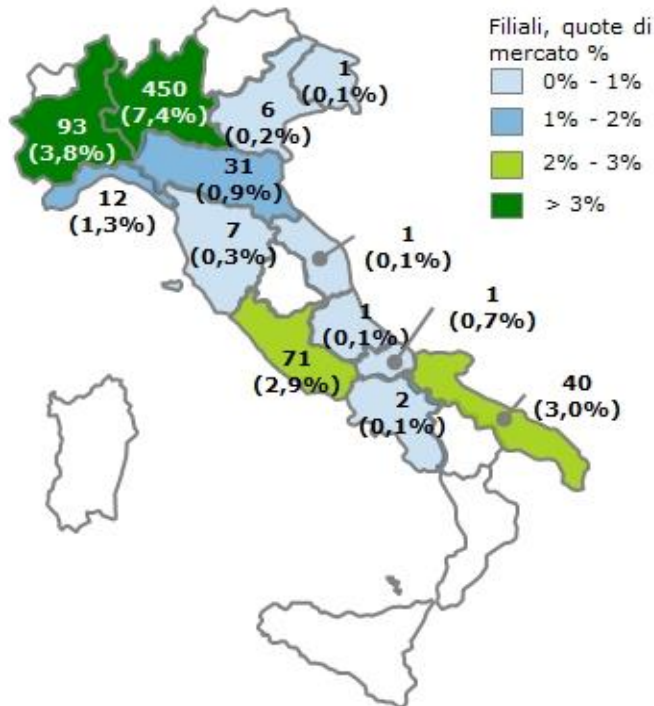
3. Escluso add-ons imposti da Banca d' Italia in Giugno 2011 e includendo l'aumento di capitale per €500m



BANCA POPOLARE DI MILANO

Solida e radicata presenza nell'Italia del Nord

Distribuzione e quote di mercato delle 716 filiali BPM per regione



Filiali e quote di mercato per aree geografiche più rilevanti



Quote di mercato superiori al 10% in 6 province: Alessandria (20,7%), Lecco (13,0%), Foggia (12,6%), Varese (12,8%), Milano (12,7%), Monza-Brianza (11,9%)

Fonte: Bilancio societario BPM al 31 dicembre 2013, Banca d'Italia, Istat e Unioncamere

¹ Include Piemonte, Lombardia, Liguria

² Dati 2011



Il perchè della Security Intelligence di BPM

OBIETTIVI

- Gestione avanzata degli eventi di sicurezza con analisi e allarmi in tempo reale
- Una piattaforma di sicurezza efficiente e di facile gestione
- Normative & Compliance

EVOLUZIONI

- Analisi sistemica dei rischi e delle vulnerabilità
- Piattaforma di sicurezza aperta a future esigenze ed integrazioni.

STATO INIZIALE

- Gestione dei Log segmentata verticalmente (FW, Teradata, Server vari, ecc.)
- Diverse soluzioni custom per la raccolta eventi e monitoraggio
- Processi custom batch per logging eventi mainframe
- Nessuna possibilità di correlazione tra eventi di diversa natura ed investigazione in tempi ridotti



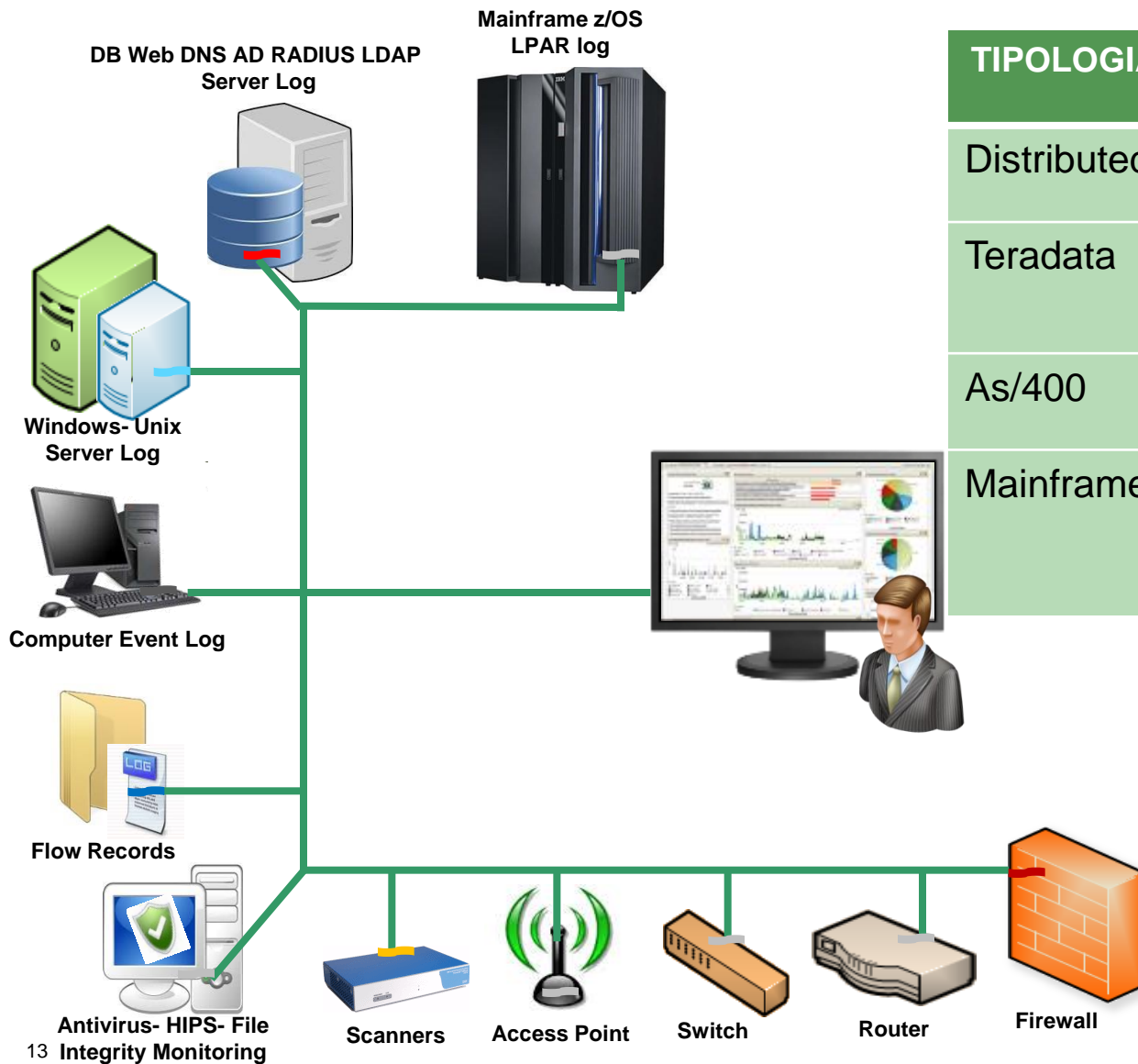


Qradar: una scelta tecnologica

- Sostituzione soluzioni custom per la raccolta eventi e per il monitoraggio con strumenti e dashboard avanzati in grado di fornire una maggiore efficienza e reattività, oltre alla riduzione del carico gestionale e di mantenimento del software
- Salvataggio degli eventi di sicurezza (sia in formato strutturato che nativo) in un unico repository capace di fornire integrità e protezione dei log raccolti
- Gestione automatica del fail-over (H.A.)
- Ricerche correlate su più fonti per singolo evento con evidenza di situazioni anomale
- Automazione dei processi di analisi e correlazione degli eventi con capacità di segnalazioni proattiva delle criticità
- Interfacce dedicate con viste personalizzate per differenti ruoli amministrativi
- Dashboard e report diversificati per tipologia utente



Sorgenti: acquisizione e controllo

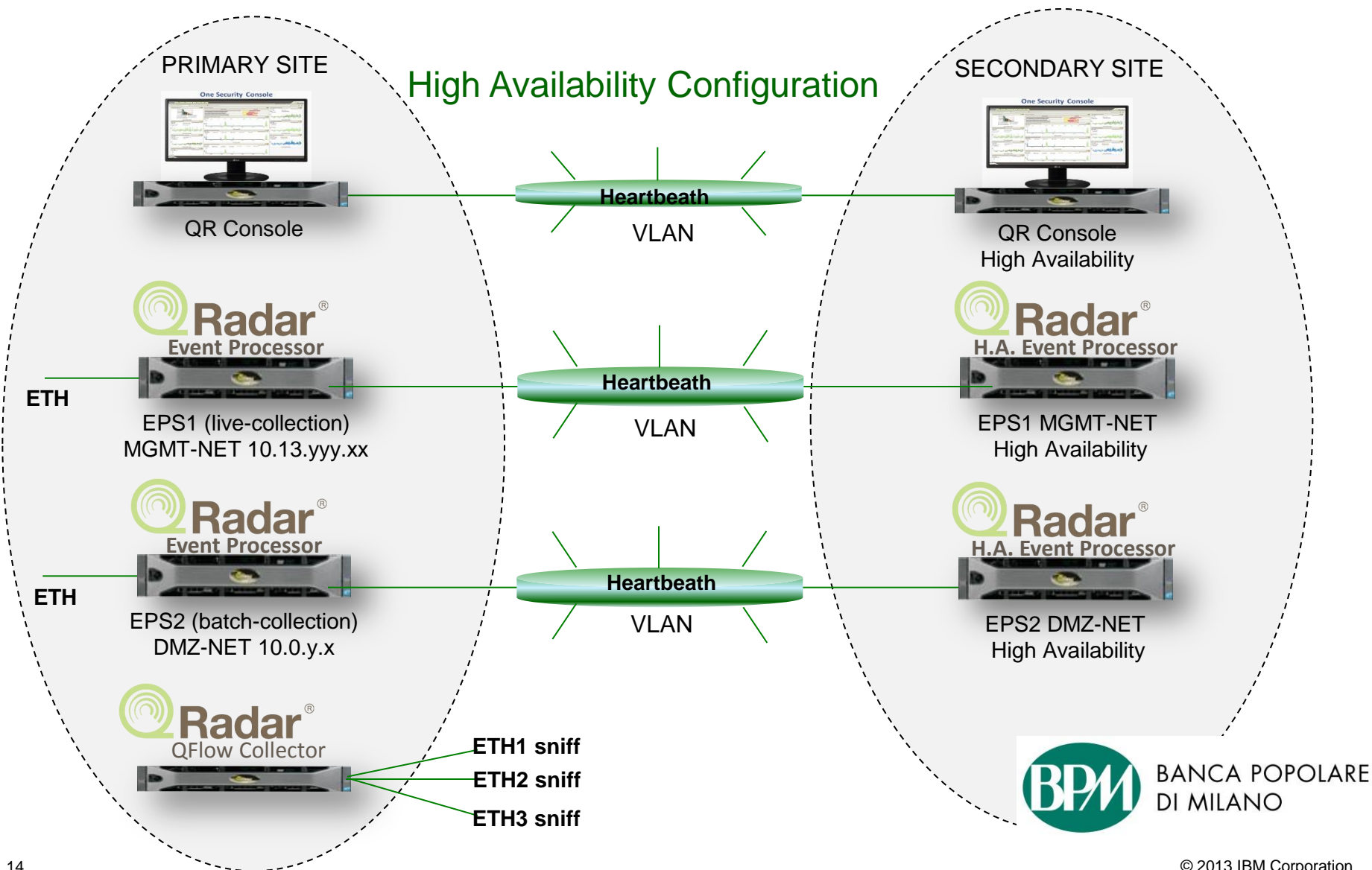


| TIPOLOGIA | SORGENTI | EPS |
|-------------|----------|-------------|
| Distributed | 230 | 111.835.516 |
| Teradata | 1 | 1.517.541 |
| As/400 | 1 | 1.487.918 |
| Mainframe | 18 | 106.253.377 |



BANCA POPOLARE DI MILANO

Schema architetturale





Qradar... per soddisfare la Compliance

Compliance Garante 1

i log degli Amministratori di Sistema collezionati centralmente nel sistema Qradar, consentono di effettuare con efficacia i controlli di conformità previsti dal provvedimento, demandando ai responsabili quelli di 1 livello

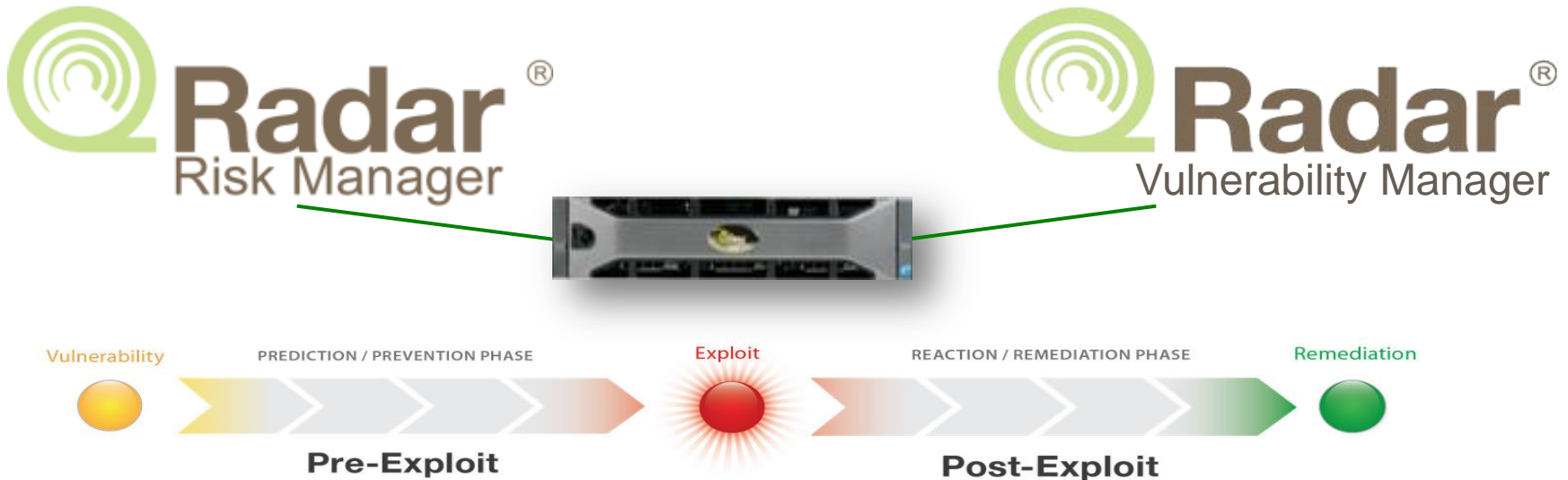
Compliance Garante 2

i log di tracciatura dell'accesso dei dipendenti in consultazione ai dati della clientela collezionati centralmente nel sistema Qradar consentono di generare gli alert previsti dal Provvedimento, utili per le attività di verifica (exploit & post-exploit)



Qradar ...come evoluzione della sicurezza

- Pianificazione gestione nuove Log-Source
- Definizione profilatura ruoli/utenti del Qradar con individuazione funzioni dell'IT e di governance (report/dashboard riepilogativi)
- Implementazione Risk Manager per la valutazione e simulazione dei rischi
- Attivazione del Vulnerability Manager per la verifica e la gestione delle vulnerabilità



Una Security Intelligence.... Innovativa !

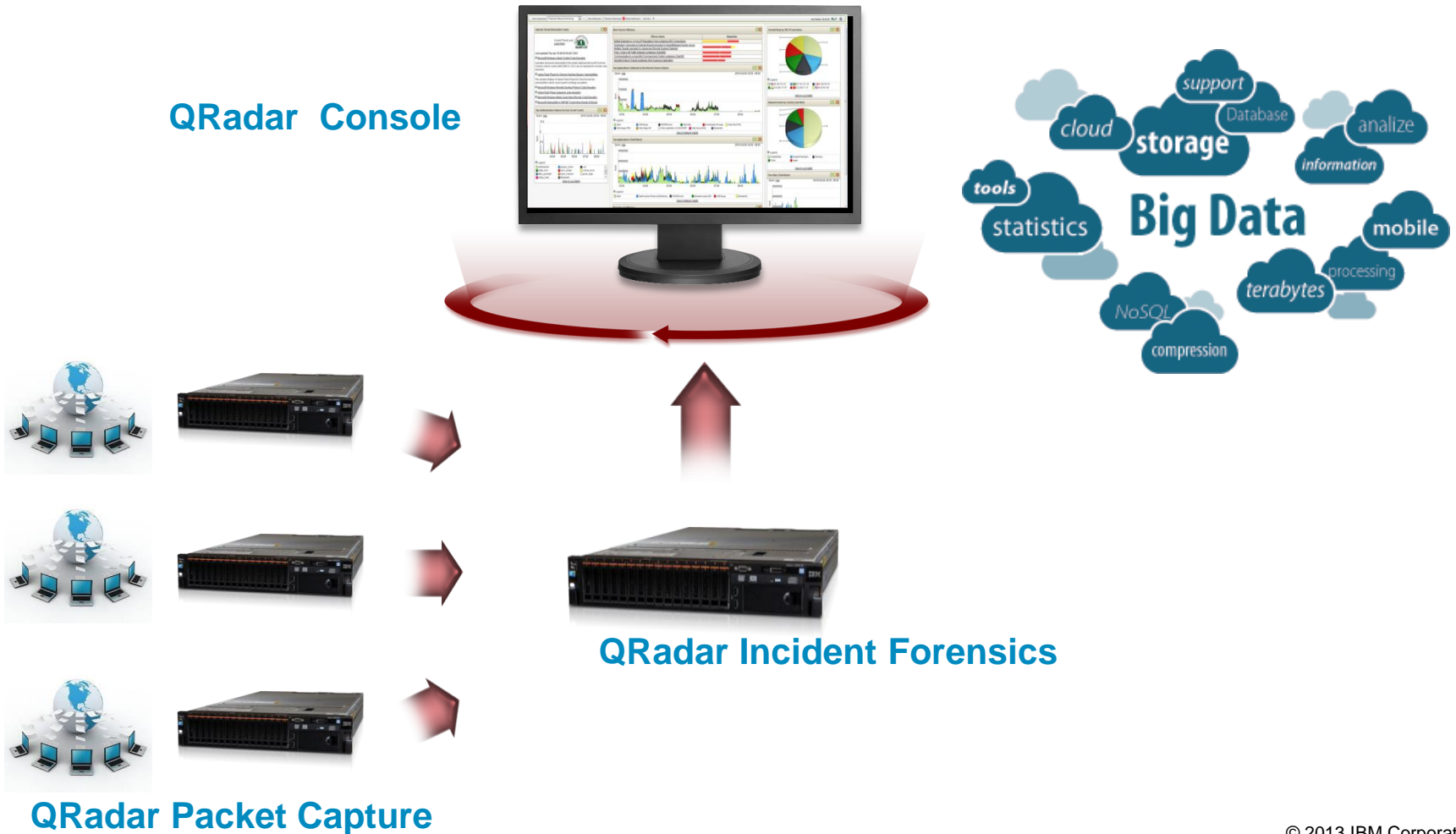
Le organizzazioni hanno bisogno di un nuovo approccio alla sicurezza che sfrutta l'intelligenza per stare al passo con l'innovazione



Se l'impensabile dovesse accadere è fondamentale trovare rapidamente come si è verificato l'evento, minimizzare il suo impatto , e fare tutto il possibile per evitarne un altro !

Qradar Incident Forensics

Ripercorrere le occorrenze «step-by-step» relative ad un incidente di sicurezza



Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security



© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.