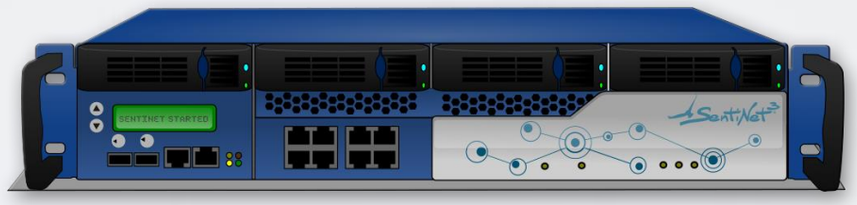
SentiNet³®

Unified Proactive Monitoring

Monitorare la superficie di attacco



Dott. Antonio Capobianco
(Founder and CEO Fata Informatica)

Fata Informatica®

Vulnerabilità

- Difetto o debolezza che può essere sfruttata per violare la politica di sicurezza di un sistema(*)

- Riduzione della vulnerabilità
  Pratica ciclica di identificazione, classificazione e risanamento delle vulnerabilità(*)

(*)Definizioni tratte da Wikipedia

Fata Informatica®

Come ridurre le Vulnerabilità

Web filtering

Threat prevention platform

Anti malware

Security Information Event Management

Intrusion detection systems

Anti spam

Ips

Security policy

Anti virus

Intrusion prevention systems

Unified Threat management

Firewall

Content filtering

CyberDefence

Network security platform

SentiNet3®
Unified Proactive Monitoring

www.SentiNet3.com

Come ridurre le Vulnerabilità

Hardening

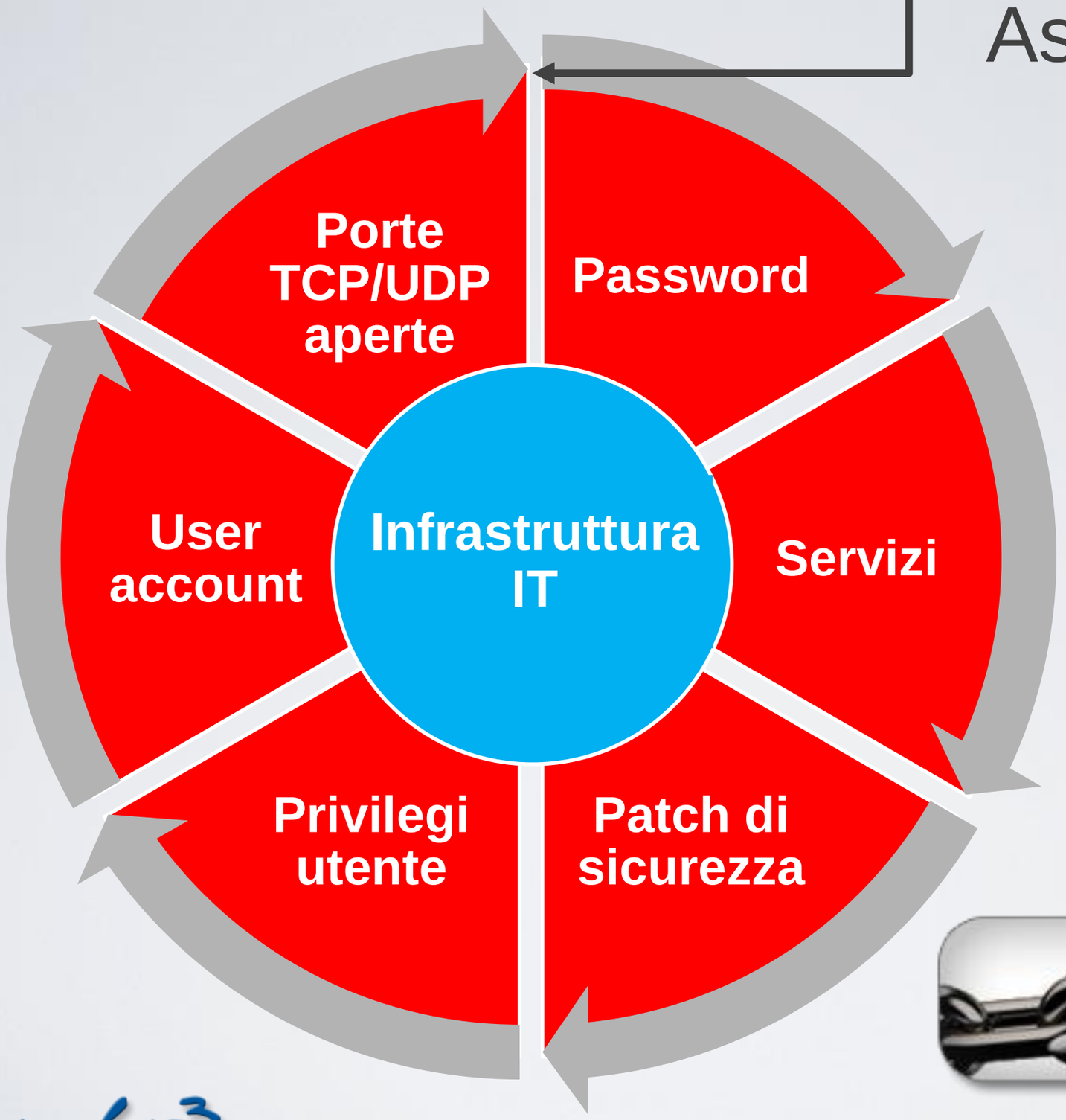
- Riduzione **superficie di attacco**
  - Rimozione software non necessario
  - Disabilitazione di servizi, moduli kernel, protocolli non necessari

- Riconfigurazione servizi esistenti per aumentarne la **robustezza**
  - Policy per complessità password
  - Abilitazione log di sicurezza
  - Installazione patch di sicurezza
  - Rimozione utenti non necessari

Fata Informatica®

Hardening

Vulnerability Assessment

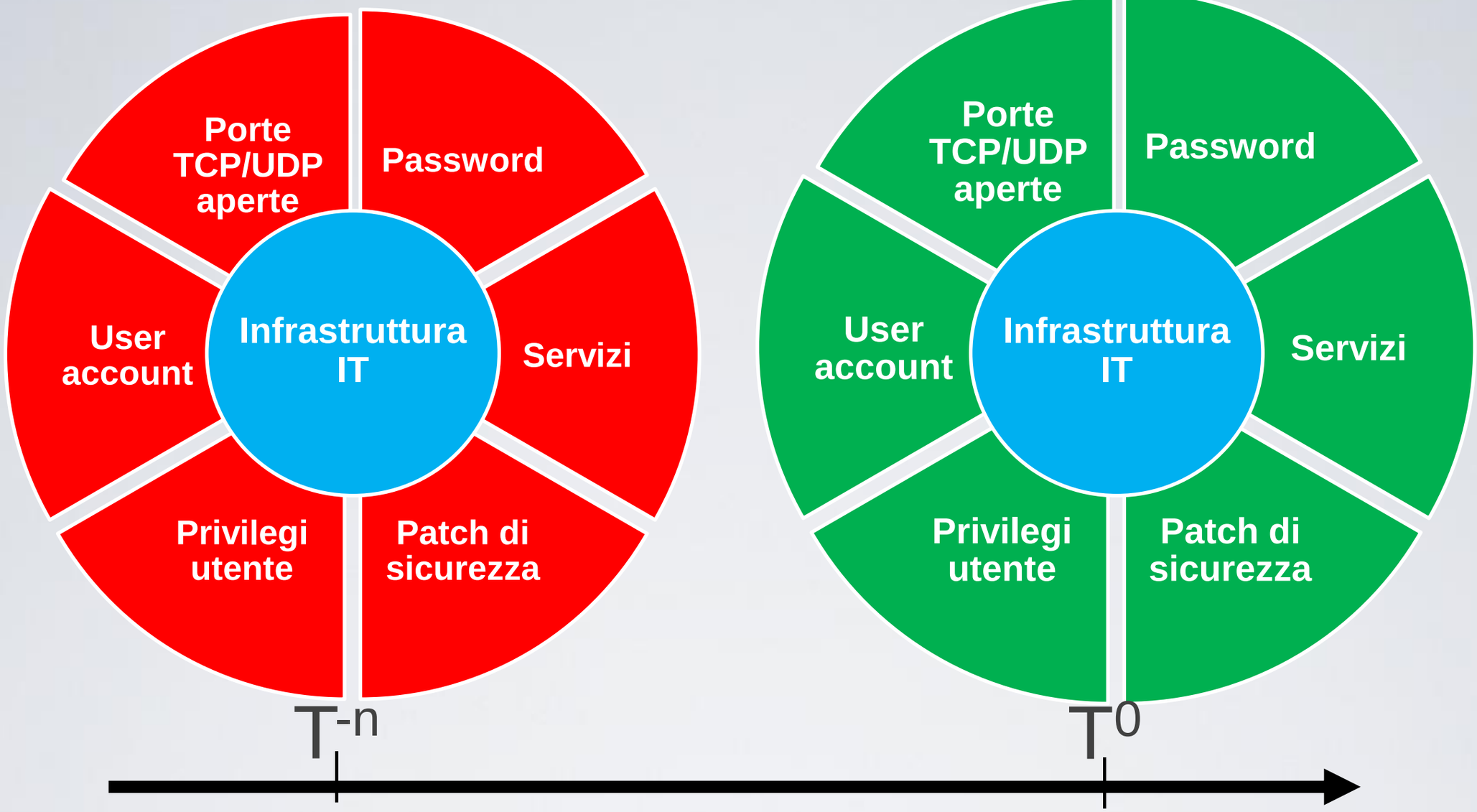


SentiNet3®
Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Hardening

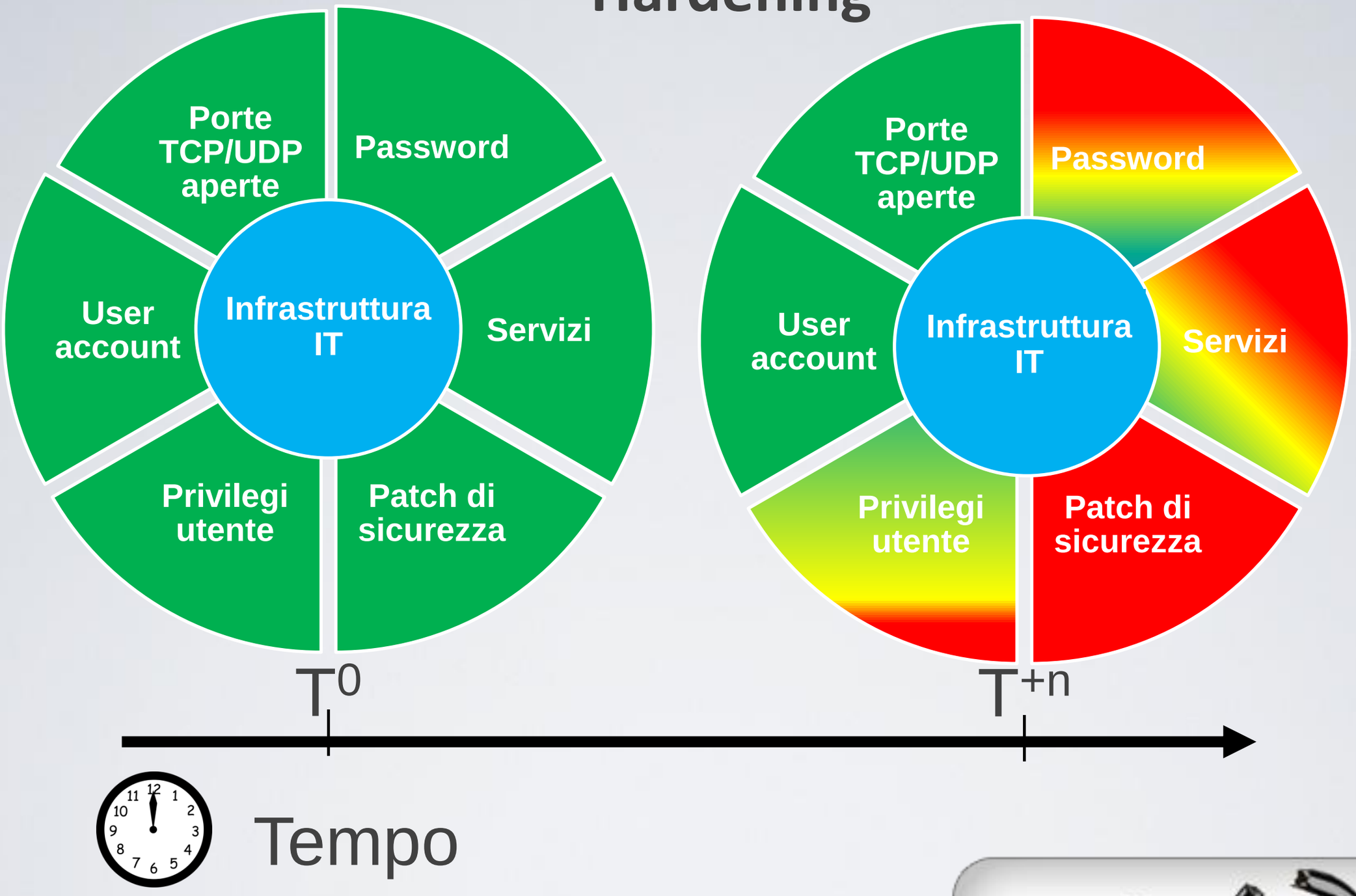


SentiNet3® Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Hardening

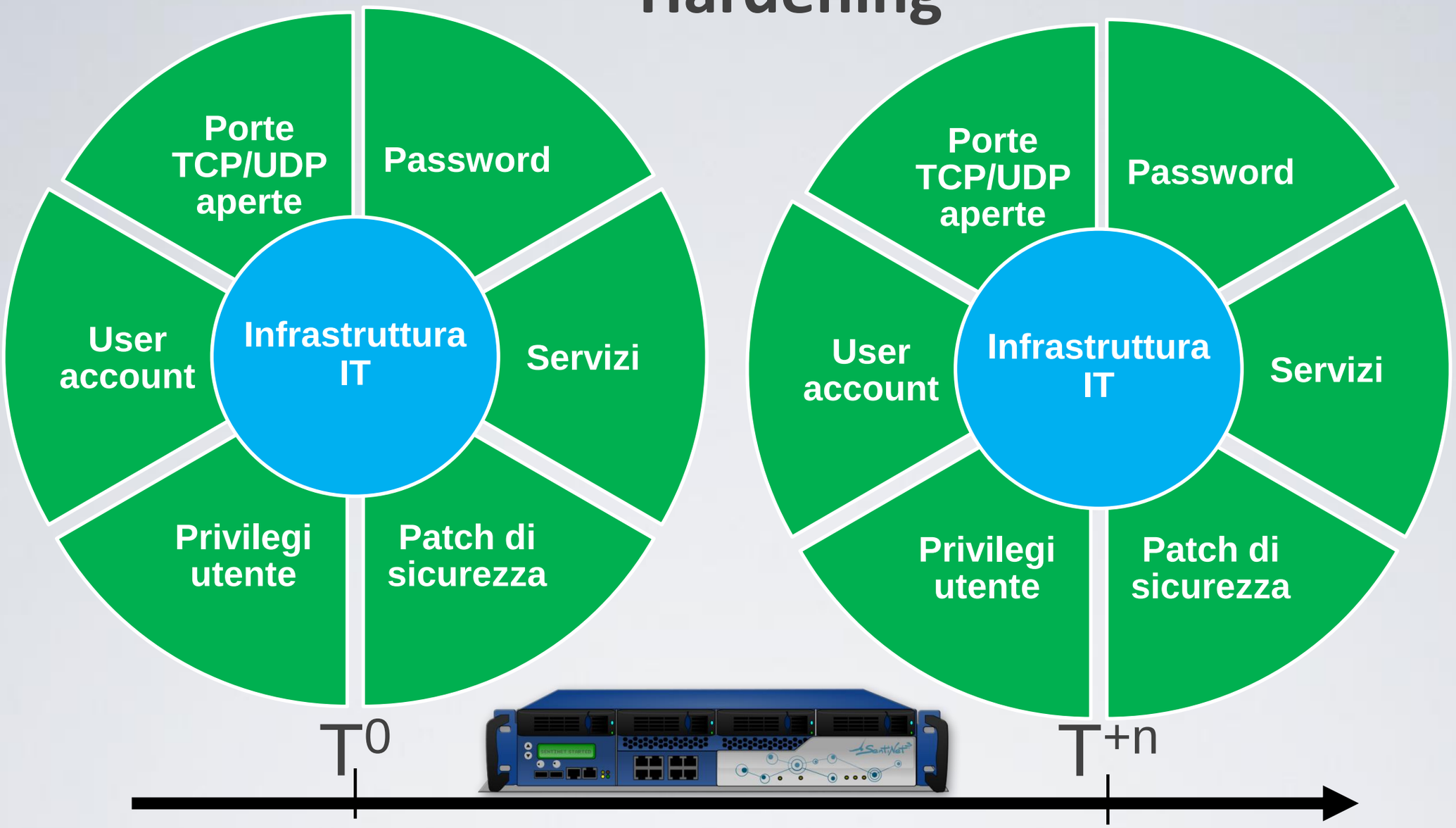


SentiNet3® Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Hardening



SentiNet3® Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Cosa è Sentinet3

- Sistema di Monitoraggio infrastruttura IT
- Sistema di Monitoraggio della sicurezza degli host (HIDS)
- Sistema di Monitoraggio della sicurezza della Rete (NIDS)
  - basato su regole
  - basato su comportamenti
- Sistema di alerting (via sms ed email)
- Sistema proattivo di reazione agli eventi

SentiNet3® Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Sentinet³® per limitare la superficie d'attacco

- Controllo su nuovi software installati
- Controllo sui servizi attivi
- Controllo sulle porte tcp e udp aperte
- Controllo sui nuovi dispositivi inseriti in rete

SentiNet³®
Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Sentinet³® per aumentare la robustezza

IT Security Patch monitoring

- Windows Security Updates
- Critical Debian and Ubuntu Updates
- Critical Updates Red Hat
- Critical Updates Aix, Solaris
- Critical Updates Router e Switch Cisco
- Aggiornamento Anti-Virus
- …

SentiNet³® Unified Proactive Monitoring

www.SentiNet3.com

Sentinet³® per aumentare la robustezza

Controllo Utente

- Abilitazione policy di sicurezza sulle password
- Controllo sulla forza delle password
- Controllo sui nuovi utenti
- Controllo su utenti non autorizzati
- Controllo su permessi specifici utente
- …

www.SentiNet3.com

Fata Informatica®

Sentinet^{3}® per aumentare la robustezza

Host Based Intrusion Detection Systems

- Antivirus check
- File integrity checking
- Log monitoring
- Rootkit detection
- Active response

SentiNet^{3}®
Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Si conosce veramente la propria infrastruttura informatica?

Le informazioni che si hanno sono corrette e allineate alla sua evoluzione.

La sua rappresentazione grafica è

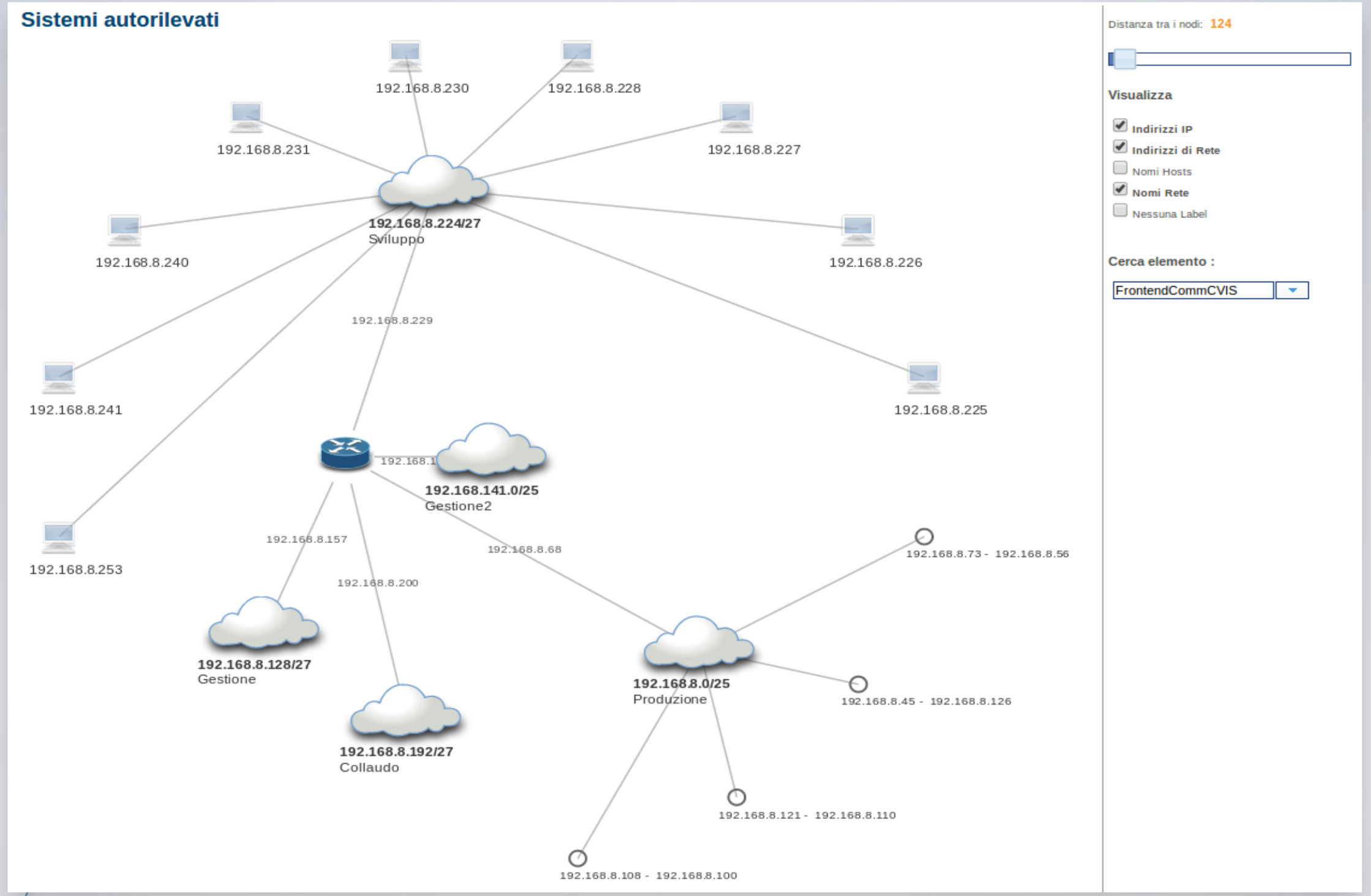
- realmente completa e aggiornata
- adeguata a rappresentare i livelli fisici e logici di tutto sistema.

SentiNet3® Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Rilevamento automatico e disegno della Rete

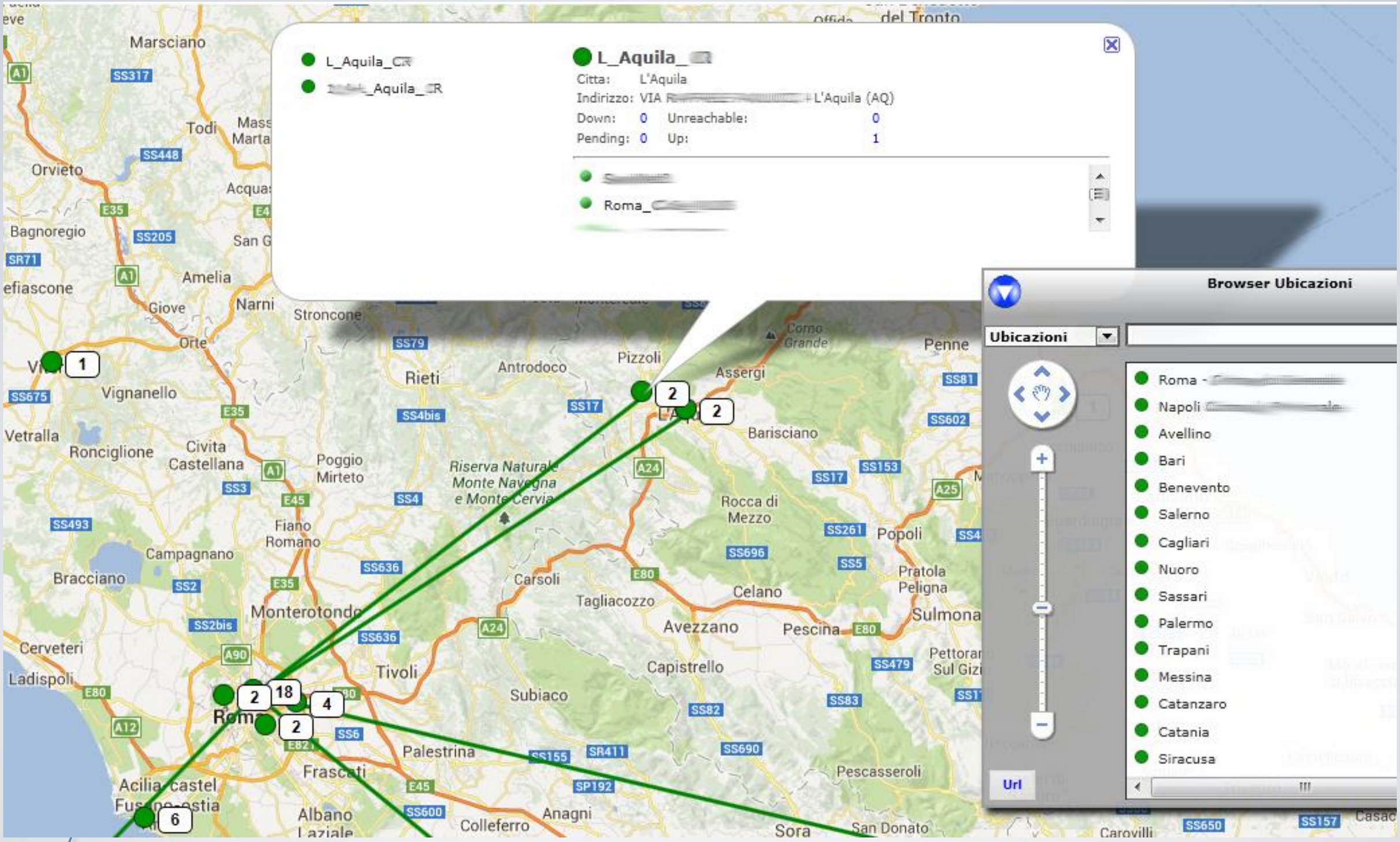


SentiNet3® Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Google Map

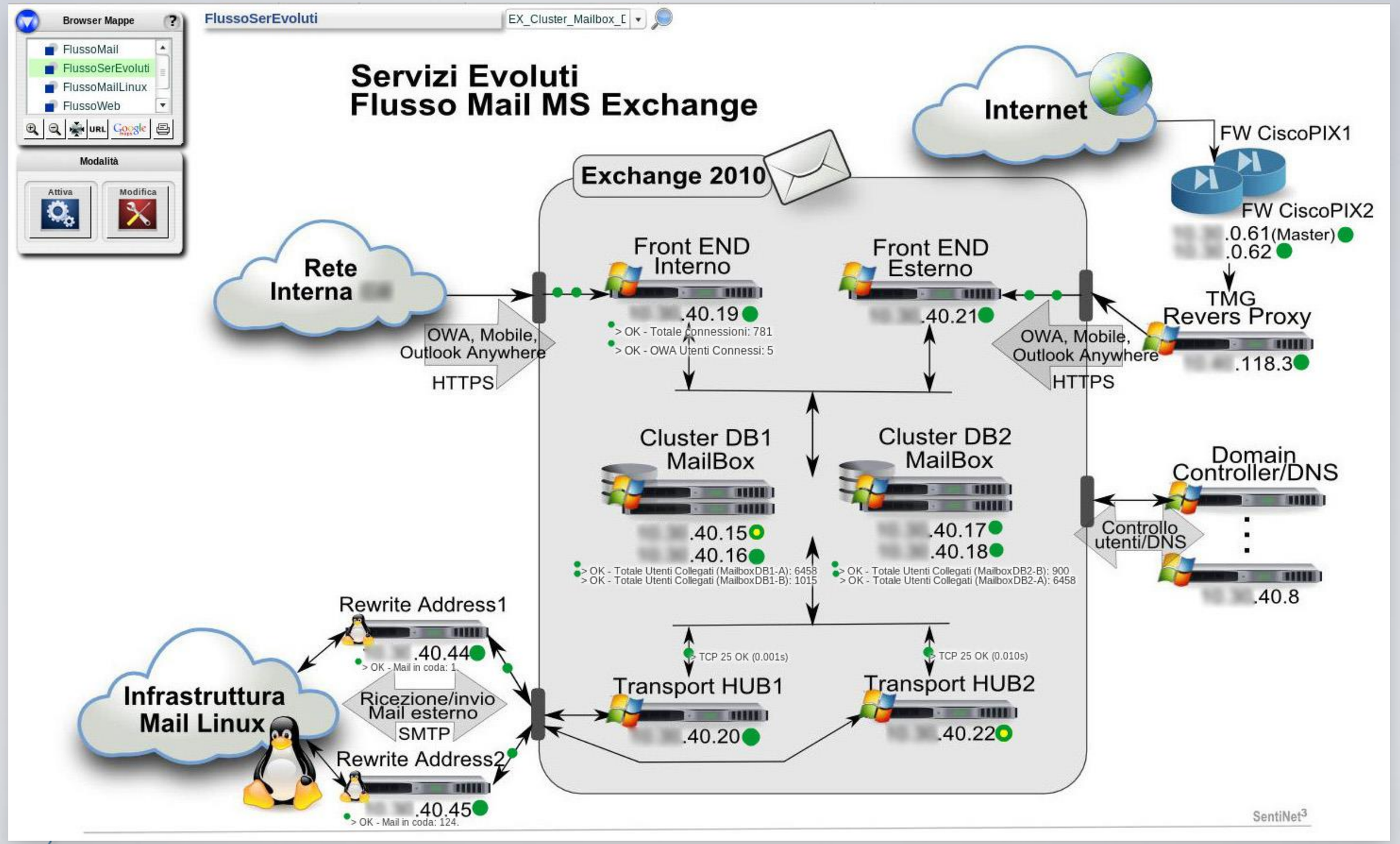


SentiNet3®
Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Mappa Funzionale/Applicativa



SentiNet® Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Controllo Intrusioni fisiche in LAN

SentiNet3®
Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Sentinet³® come NSM

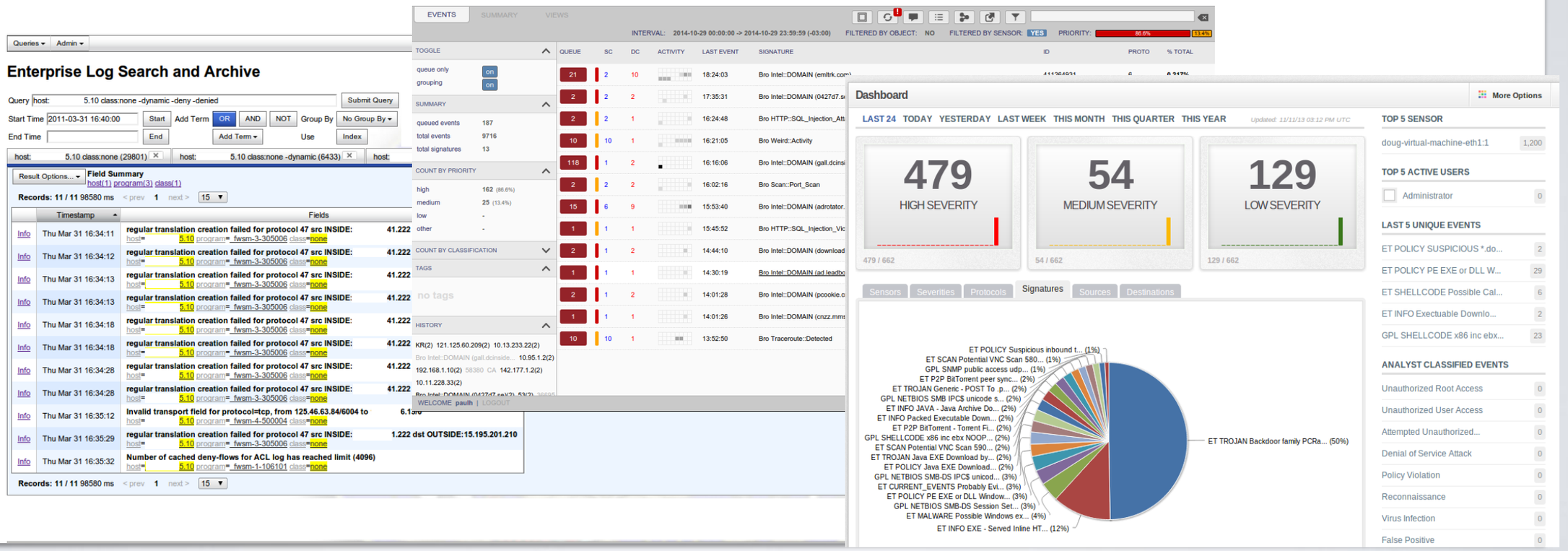
- Oltre il semplice IDS: **Network Security Monitoring**
  - Molteplicità dei dati:
    - Alert data (NIDS e HIDS)
    - Asset data e servizi (ip, mac, dns, hostname, ecc)
    - Session data (profilazione delle connesioni)
    - Transaction data (http,ftp,dns,ssl, ecc)
    - Full content packet data

SentiNet³® Unified Proactive Monitoring

www.SentiNet3.com

Sentinet³® come NSM

- **NSM** - Governare la complessità dei dati
  - Ricerche diverse, strumenti diversi

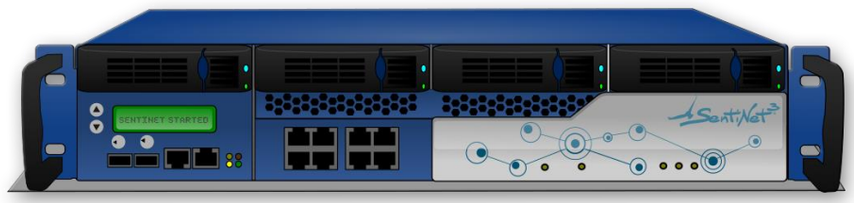


SentiNet³® Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Perché Sentinet³® come Network Security System?

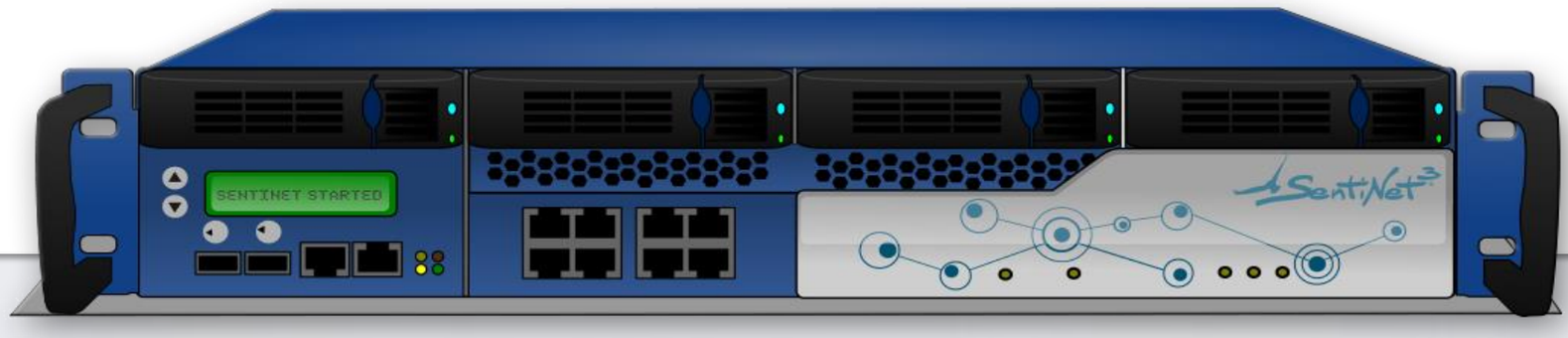


SentiNet³®
Unified Proactive Monitoring

www.SentiNet3.com

Sentinet3® per il Security Monitoring 1/2

- Facilità di utilizzo
- Controllo continuo post hardening
  - Limitare la superficie di attacco
  - Aumentare la robustezza dell'infrastruttura IT
- Sistema di protezione integrato
  - NIDS, HIDS, NSM
- Controllo attacchi in corso



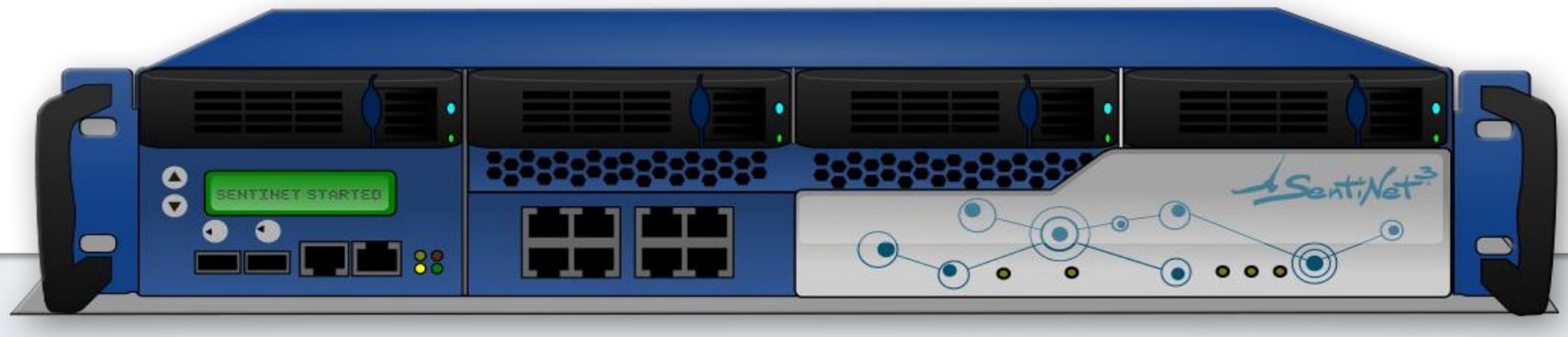
Unified Proactive Monitoring

www.SentiNet3.com

Sentinet3® per il Security Monitoring 2/2

Visione a più livelli sempre aggiornata e intuitiva dell'intera infrastruttura informatica

- Autorilevamento e disegno infrastruttura di rete
- Google Map
- Mappe Funzionali e Applicative
- Banda Utilizzata
- Controllo intrusione fisica in LAN
- SLA - Service Level Agreement
- …



Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Ministero degli Affari Esteri

Success Story

Monitoraggio della Rete Mondiale Visti

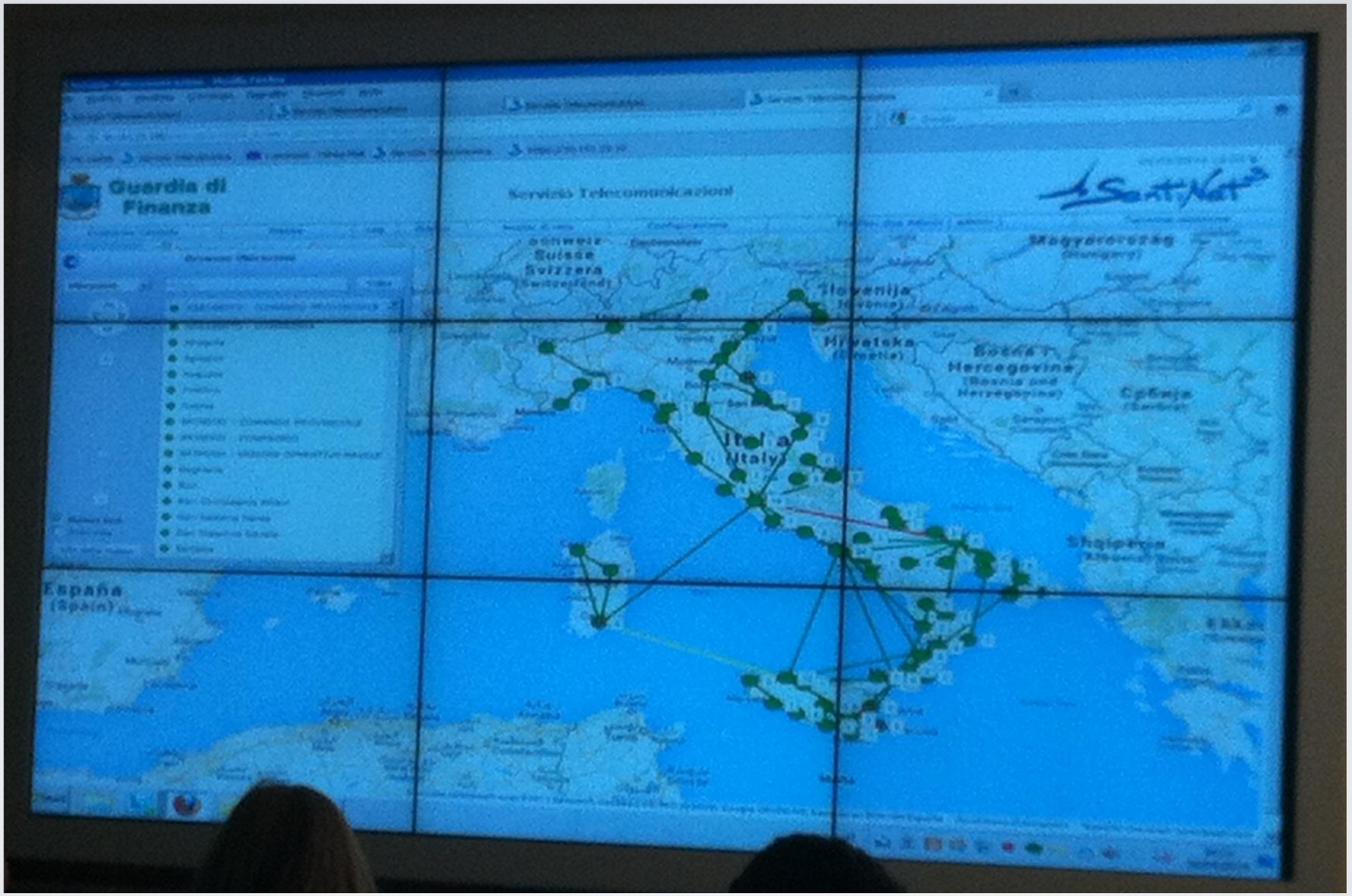
SentiNet3®
Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

Guardia di Finanza

Success Story



SentiNet3®
Unified Proactive Monitoring

info@sentinet3.com

www.SentiNet3.com

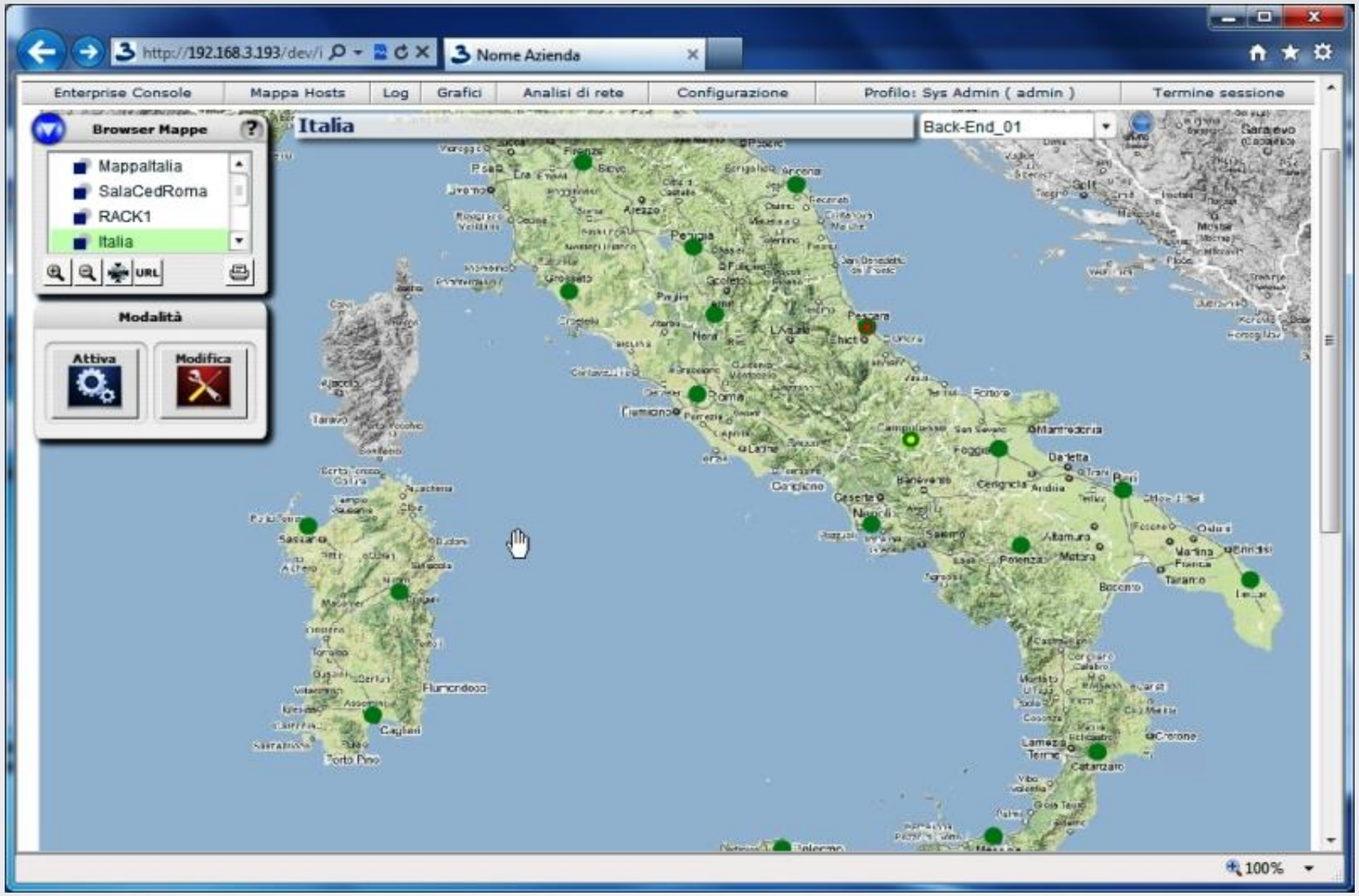
Fata Informatica®

ESERCITO

Success Story

Monitoraggio del

SIGE Sistema Informativo Gestionale dell'Esercito Italiano



SentiNet3®
Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

NATO
Locked Shield 2014

Success Story

Console di Controllo Applicativo

Rete_Mondiale_Visti Trattato Schengen			
[redacted]/ **Connessione**	At: 2013-01-30 13:06:53	GPING OK - 64 bytes from [redacted]	p_req=1 ttl=255 time=0.493 ms
[redacted]/ **Connessione**	At: 2013-01-30 13:06:14	GPING OK - 64 bytes from [redacted]	p_req=1 ttl=255 time=0.593 ms
ApplicationServer			
DataBase Centrale			
Black_Box			
Linuxfront Comunicazione con Sede Mosca RMV			
[redacted]/ **Connessione**	At: 2013-01-30 13:07:00	GPING OK - 64 bytes [redacted]	icmp_req=1 ttl=64 time=0.653 ms
[redacted]/ **ComunicazioneProcPraticheVisto**	At: 2013-01-30 13:04:43	Servizio MAELINK **ON**	
[redacted]/ **ComunicazioniRMV**	At: 2013-01-30 13:03:57	Servizio [redacted] **ON**	
[redacted]/ **Disk_root**	At: 2013-01-30 12:46:44	Filesystem / used: **(76%)**	
[redacted]/ **TelegrammiUscita**	At: 2013-01-30 13:06:51	Pratiche rmv in uscita: **(0)**	
[redacted]/ **TelegrammiCentrale**	At: 2013-01-30 13:04:26	Pratiche rmv preparate: **(0)**	
[redacted]/ **TelegrammiIngresso**	At: 2013-01-30 13:05:32	Pratiche rmv in ingresso: **(12)**	
DataBase Multipolo			
FeVIS (S.P.o.C.)			
Server_Posta SMTP			
Flusso_Pratiche_VIS Analisi flusso pratiche visto nel circuito [redacted]			
[redacted]/ **ErroriCVIS**	At: 2013-01-30 13:07:31	Messaggi in errore: **(26)**	
[redacted]/ **MessaggiUscita**	At: 2013-01-30 13:05:41	Coda Messaggi verso LVIS: **(96)**	

SentiNet3®
Unified Proactive Monitoring

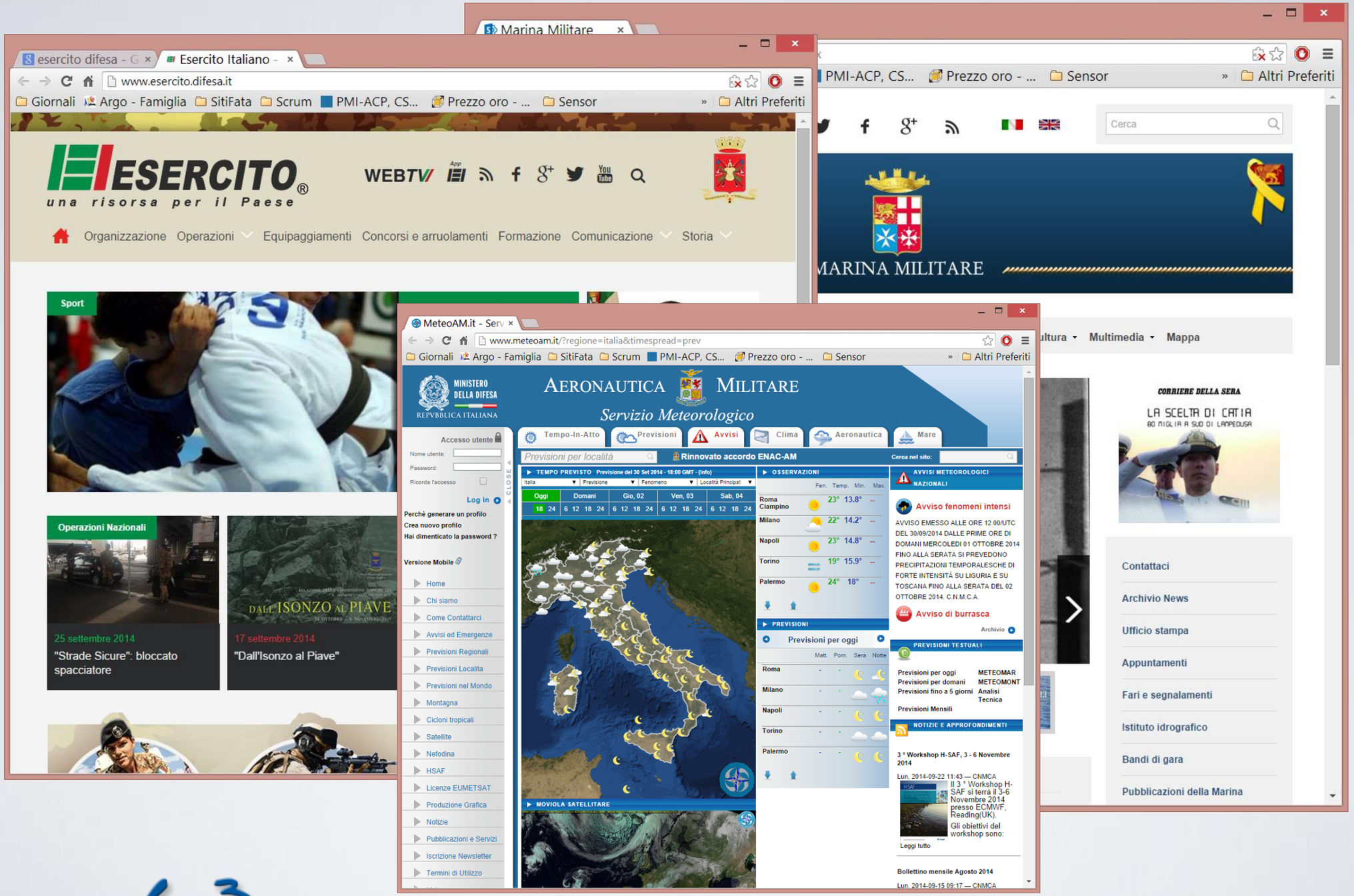
info@sentinet3.com

www.SentiNet3.com

Fata Informatica®

MINISTERO DELLA DIFESA

Success Story



SentiNet3®
Unified Proactive Monitoring

info@sentinet3.com

www.SentiNet3.com

Fata Informatica®

I 8 punti che rendono Sentinet3® un prodotto Enterprise unico!

1. Veloce messa in esercizio
   … parliamo di giorni, non mesi o anni!
2. Facilità di utilizzo
   Per il manager e per i tecnici
3. Facilità di personalizzazione
   Contatto diretto con la casa madre!
4. Flessibilità
   … un prodotto di Unified Monitoring!
5. Supporto senza … scuse!
   Noi non apriamo ticket!
6. Aperto al mondo open source
   Prodotto Open integrabile con plug in Nagios
7. Licenze perpetue ed illimitate
   Costi certi e contenuti. 10 volte meno dei concorrenti.
8. Made in Italy
   Prodotto da Fata Informatica dal 2004

SentiNet3® Unified Proactive Monitoring

www.SentiNet3.com

Fata Informatica®

I nostri clienti

CARABINIERI

ESERCITO

COMANDO C4 DIFESA

Ministero dello Sviluppo Economico

Ministero degli Affari Esteri

Rai Way

Istituto Nazionale di Geofisica e Vulcanologia

ITALFERR
GRUPPO FERROVIE DELLO STATO ITALIANE

NUCLECO
società per l'ecoingegneria nucleare

CNA

Guardia di Finanza

Polizia di Stato

iPZS ISTITUTO POLIGRAFICO E ZECCA DELLO STATO

AlmavivA
The Italian Innovation Company

FASTWEB

acea

WIND

SELEX
Sistemi Integrati
Una Società Finmeccanica

GRUPPO VITROCISET

SentiNet3®
Unified Proactive Monitoring

www.SentiNet3.com