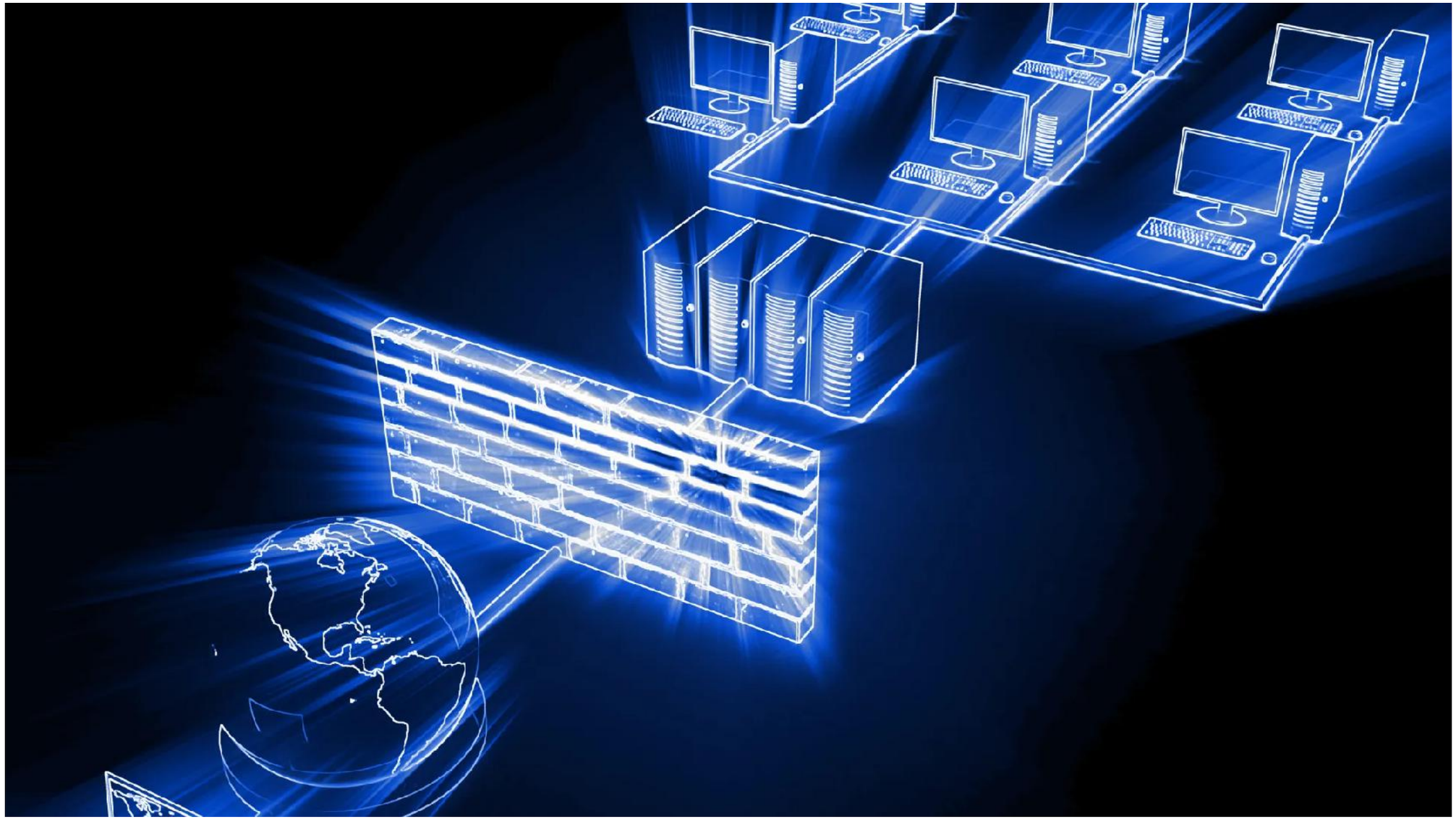


Monitorare per rendere più sicura la superficie di attacco

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(*)

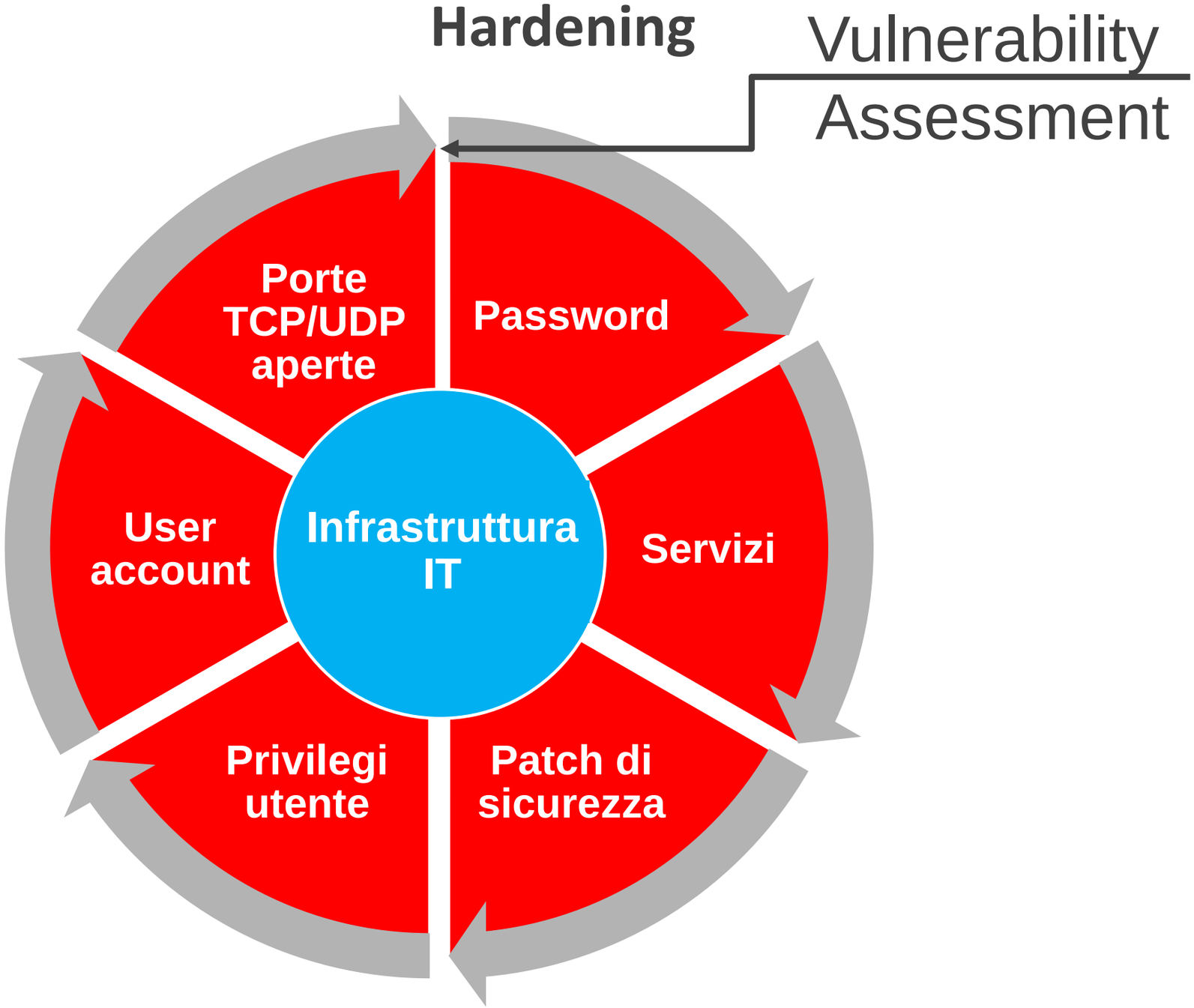
(*)Definizioni tratte da Wikipedia

Come ridurre le Vulnerabilità

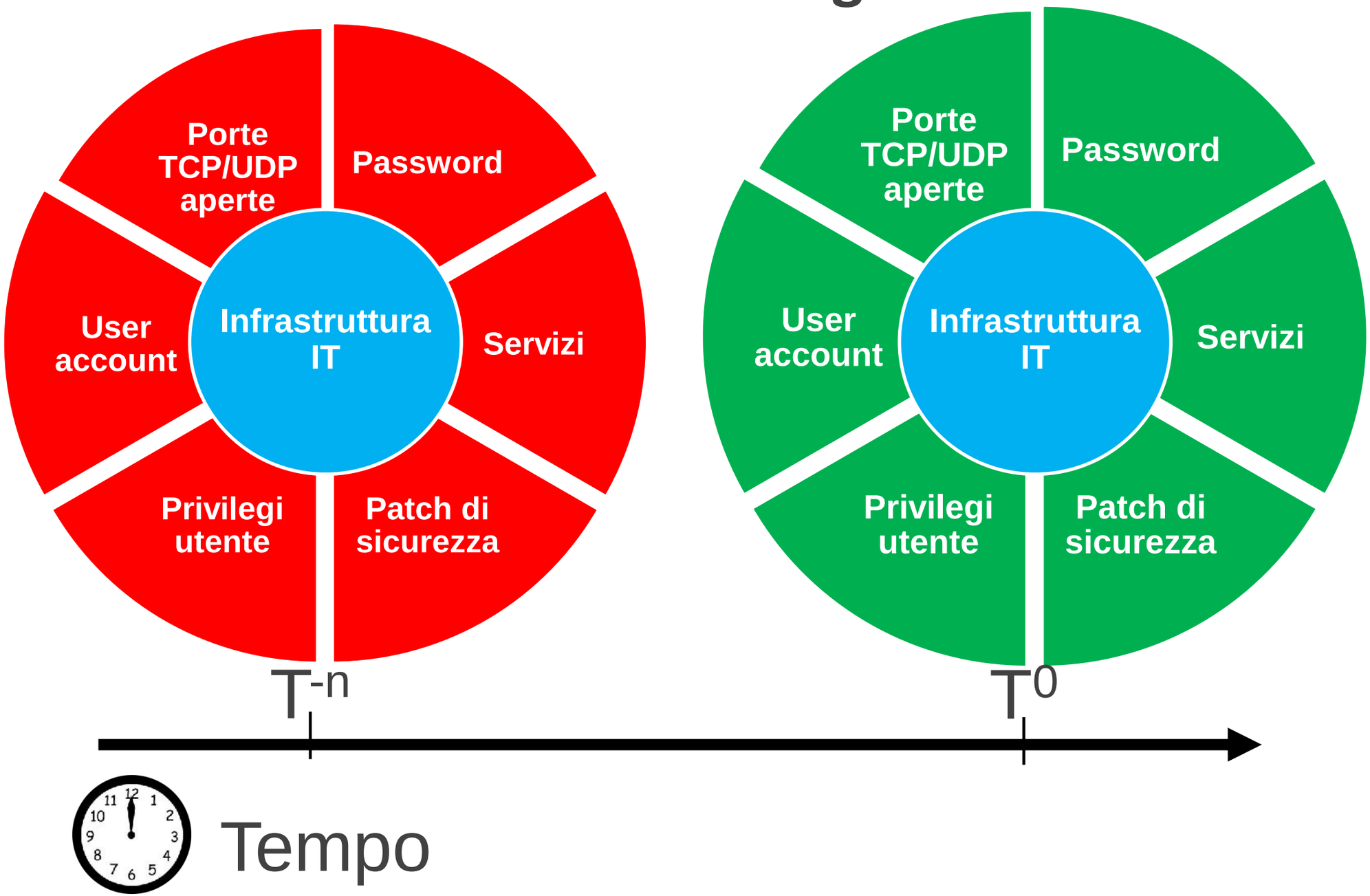
Come ridurre le Vulnerabilità

Hardening

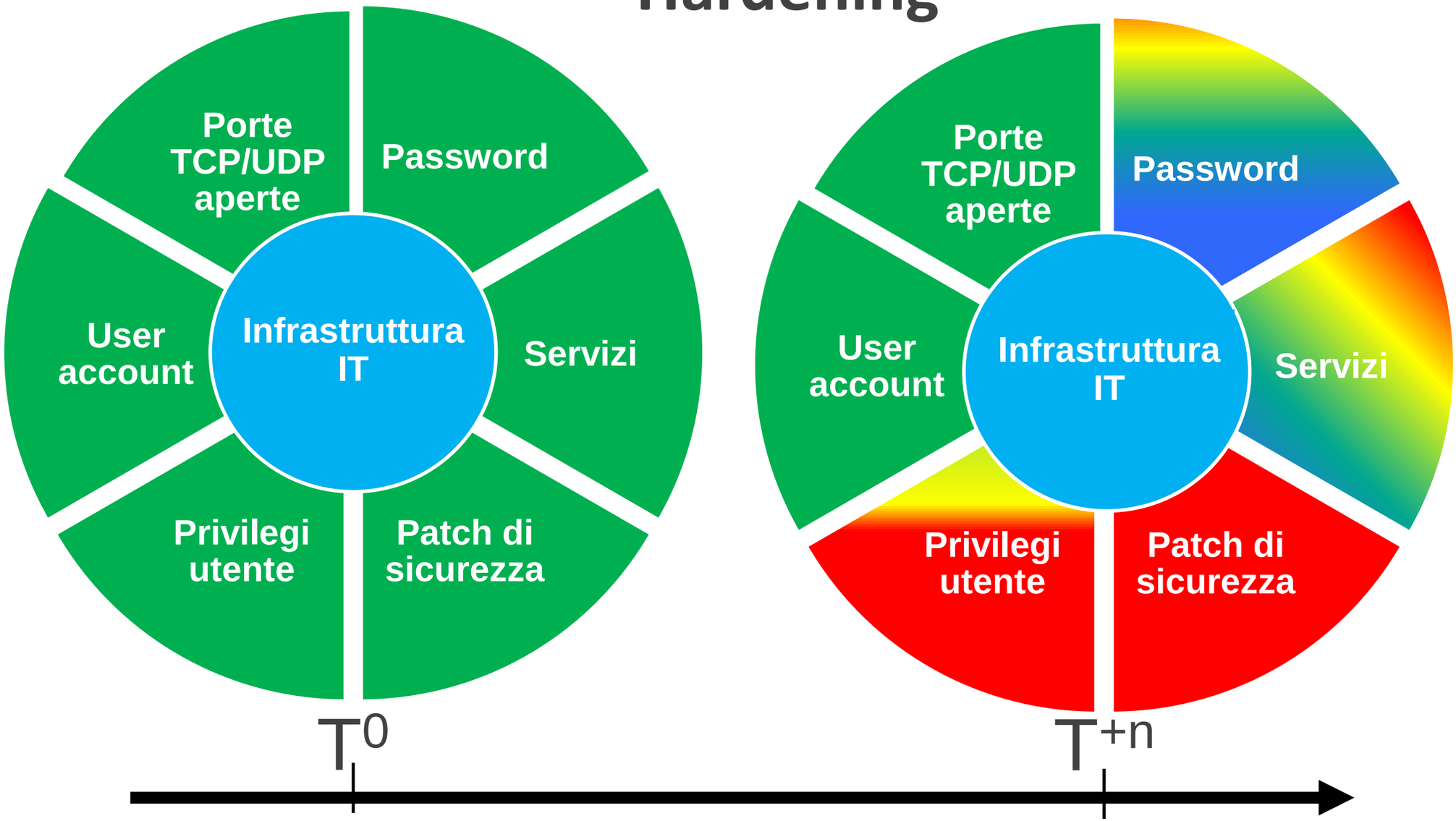
- Riduzione **superficie di attacco**
  - Rimozione software non necessario
  - Disabilitazione di servizi, moduli kernel, protocolli non necessari
- Riconfigurazione servizi esistenti per aumentarne la **robustezza**
  - Policy per complessità password
  - Abilitazione log di sicurezza
  - Installazione patch di sicurezza
  - Rimozione utenti non necessari


Hardening
Vulnerability Assessment
Porte TCP/UDP aperte
Password
Servizi
Patch di sicurezza
Privilegi utente
User account
Infrastruttura IT

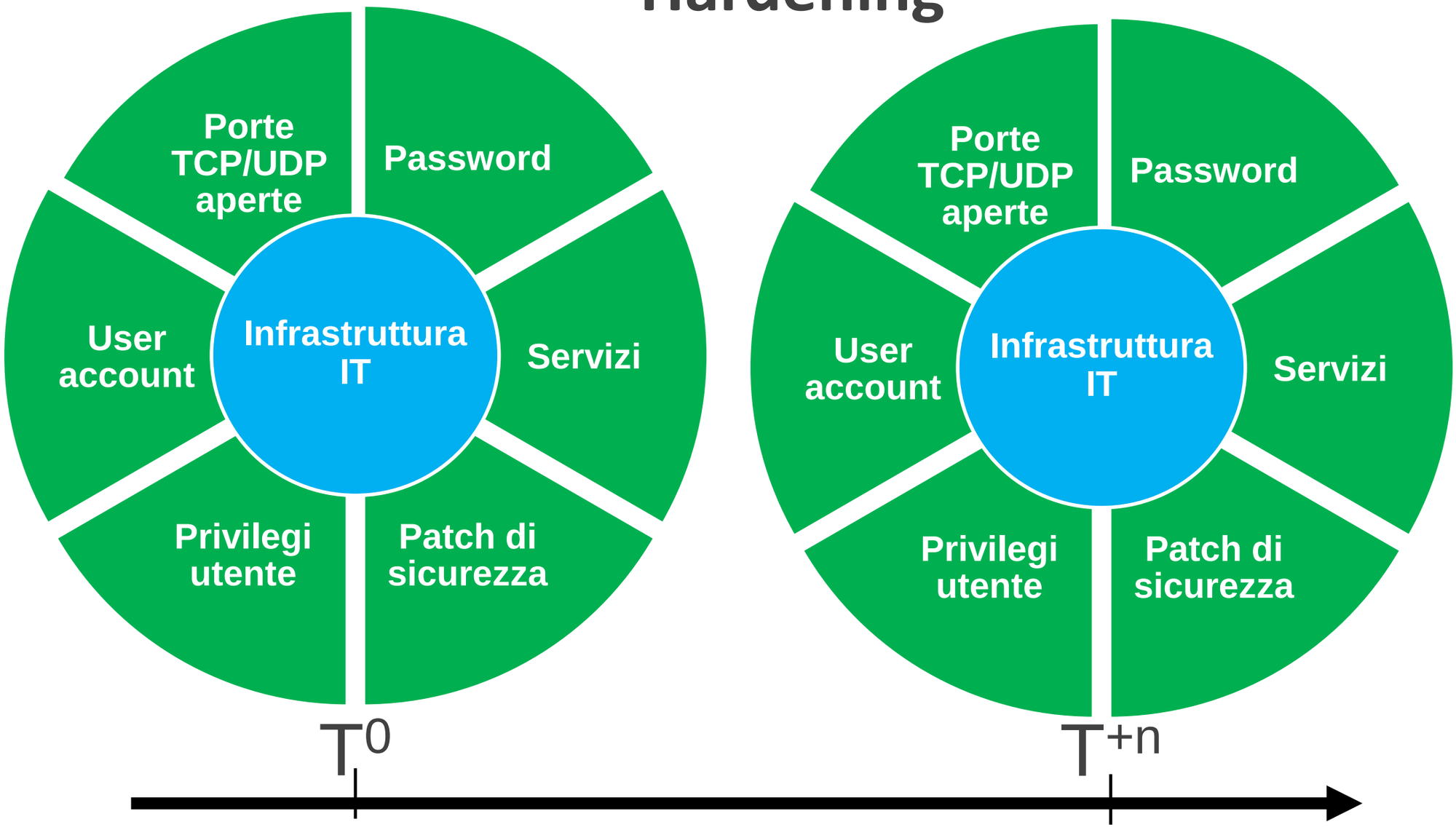
Hardening


Porte TCP/UDP aperte
Password
User account
Infrastruttura IT
Servizi
Privilegi utente
Patch di sicurezza
Porte TCP/UDP aperte
Password
User account
Infrastruttura IT
Servizi
Privilegi utente
Patch di sicurezza
T-n
T0
Tempo

Hardening


Porte TCP/UDP aperte
Password
User account
Infrastruttura IT
Servizi
Privilegi utente
Patch di sicurezza
Porte TCP/UDP aperte
Password
User account
Infrastruttura IT
Servizi
Privilegi utente
Patch di sicurezza
T0
T+n
Tempo

Hardening


Porte TCP/UDP aperte
Password
User account
Infrastruttura IT
Servizi
Privilegi utente
Patch di sicurezza
Porte TCP/UDP aperte
Password
User account
Infrastruttura IT
Servizi
Privilegi utente
Patch di sicurezza
T0
T+n
Tempo

Monitoring & Allerting

- 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

Come 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

Come 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

Controlli 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
- …

Sistemi per aumentare la robustezza

Host Based Intrusion Detection Systems

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

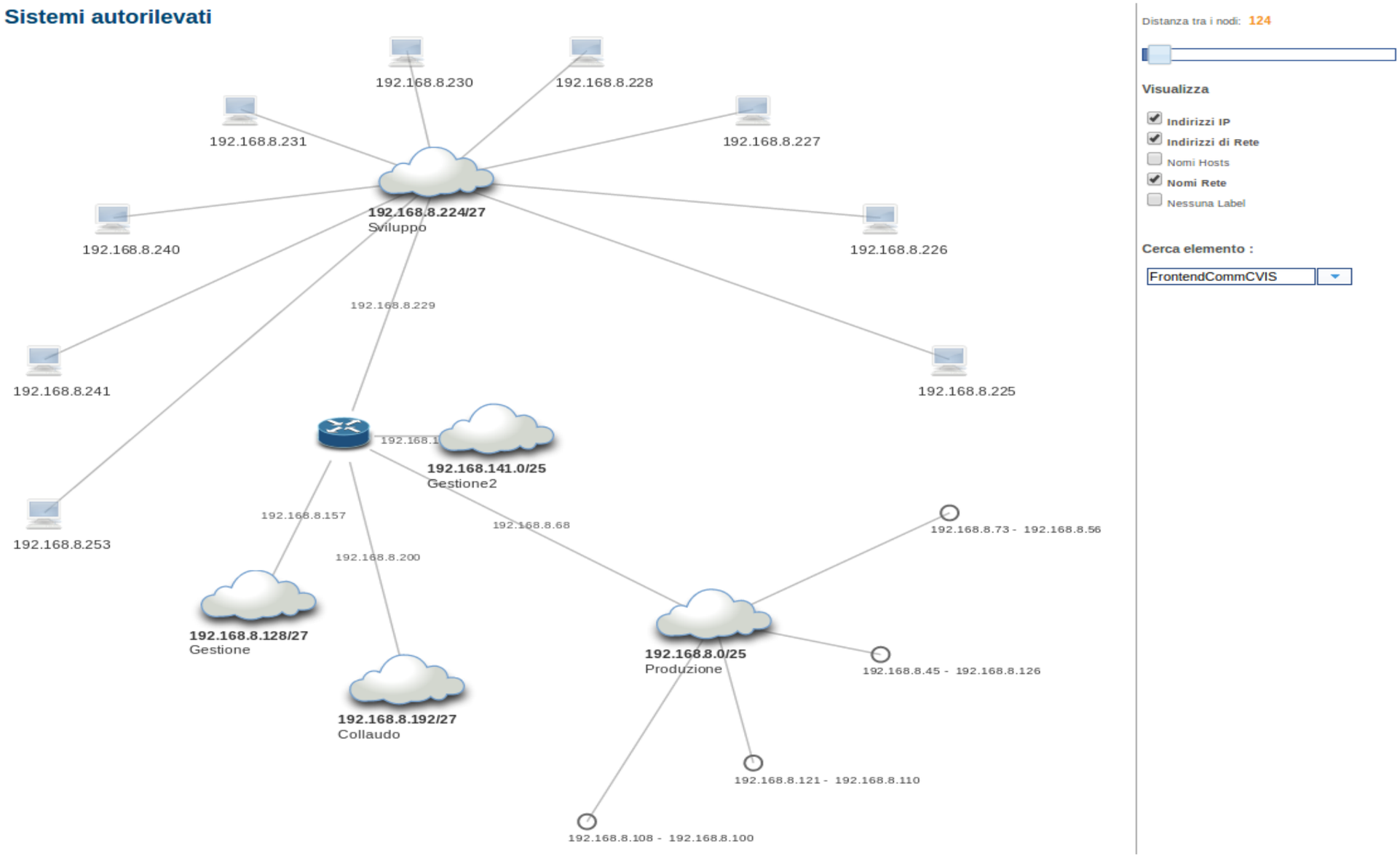
Si conosce veramente la propria infrastruttura informatica?

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

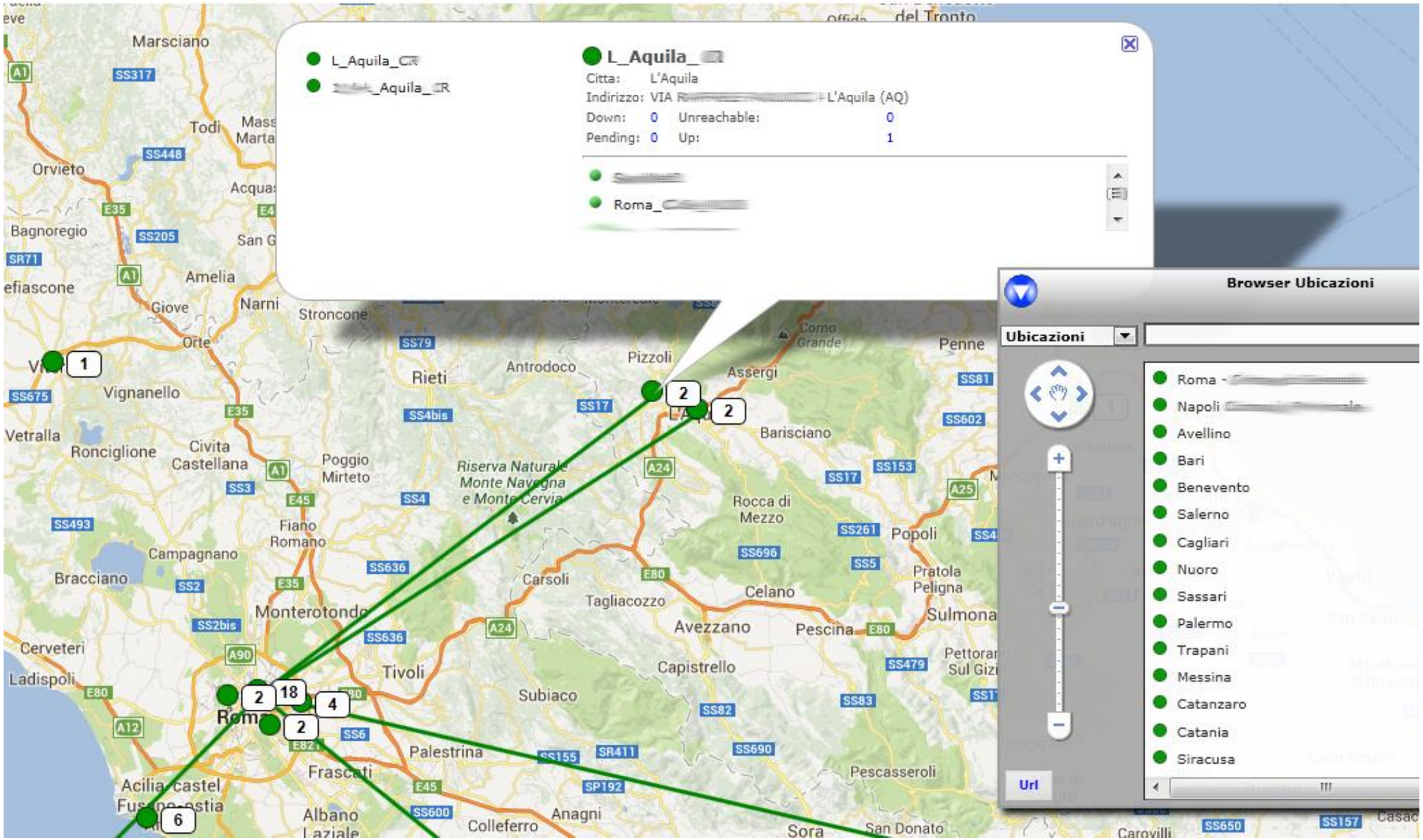
La sua rappresentazione grafica è

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

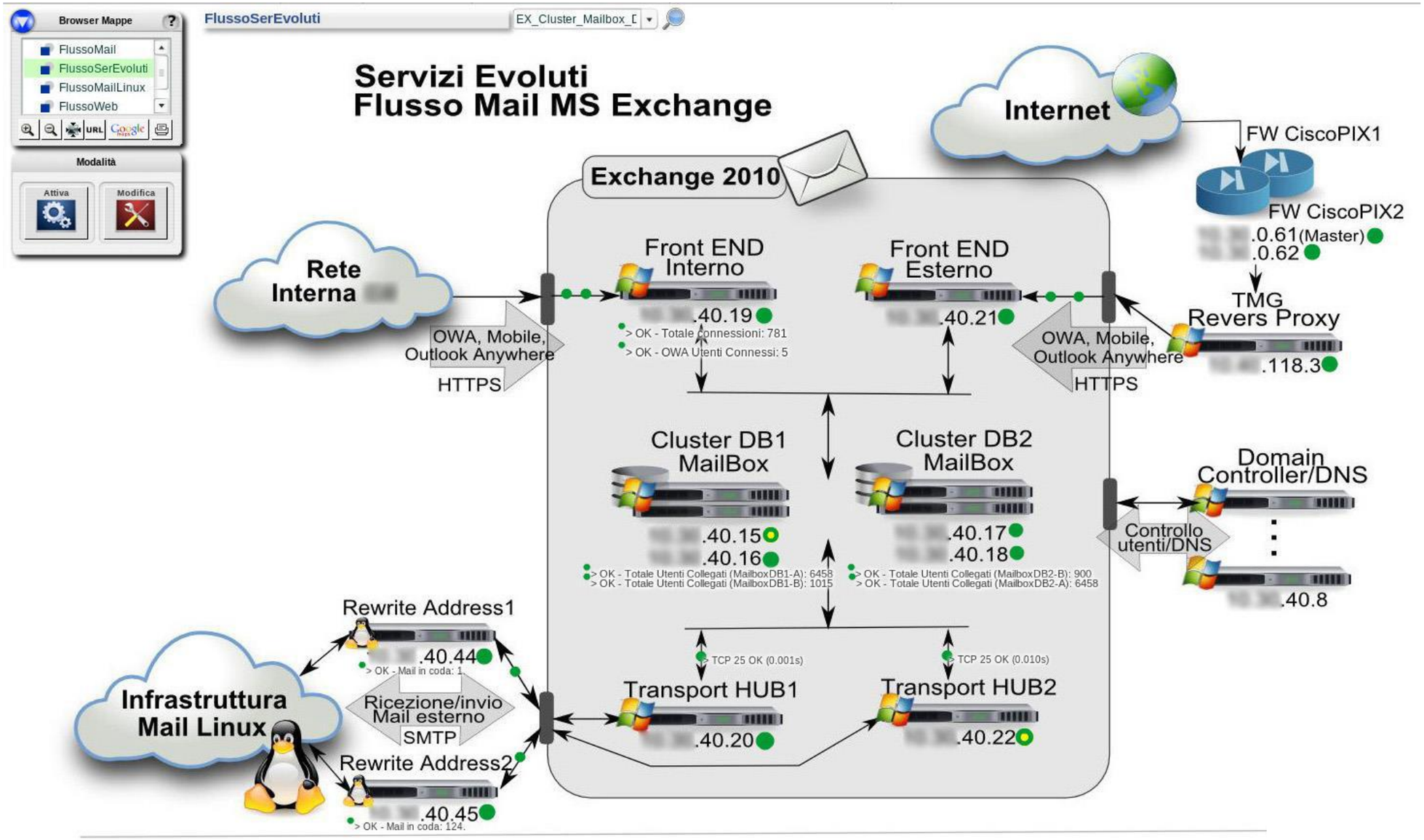
Rilevamento automatico e disegno della Rete



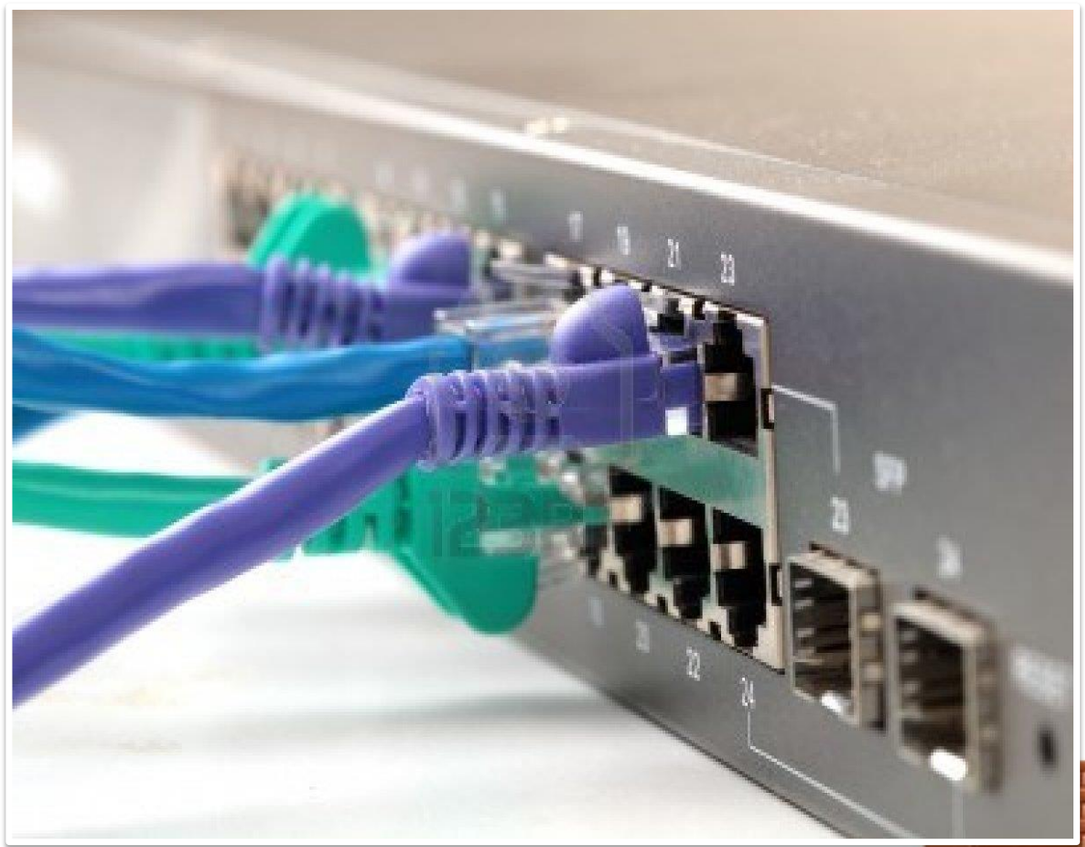
Google Map

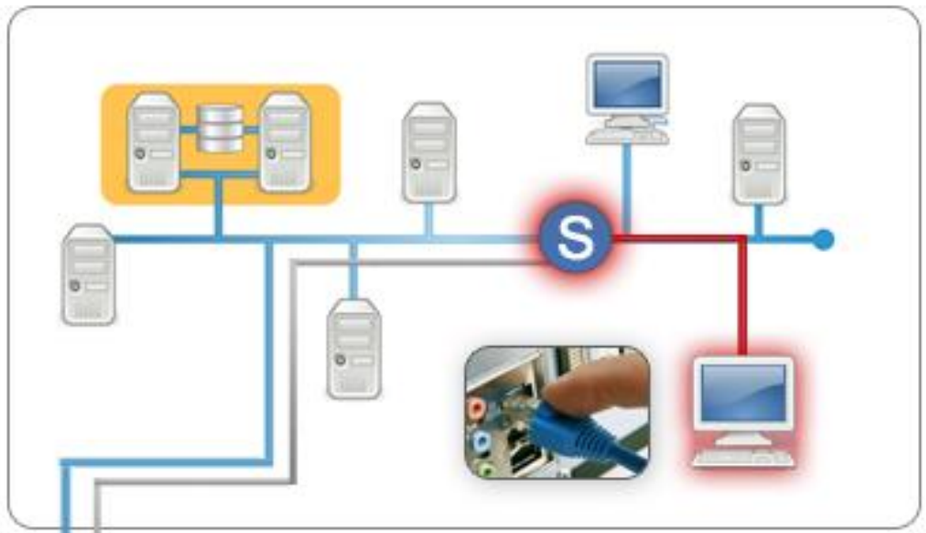

L_Aquila_CR
L_Aquila_CR
L_Aquila_
Citta: L'Aquila
Indirizzo: VIA L'Aquila (AQ)
Down: 0 Unreachable: 0
Pending: 0 Up: 1
Roma_
Browser Ubicazioni
Ubicazioni
Roma -
Napoli
Avellino
Bari
Benevento
Salerno
Cagliari
Nuoro
Sassari
Palermo
Trapani
Messina
Catanzaro
Catania
Siracusa
Url
Marsciano
Orvieto
Todi
Bagnoregio
Amelia
Narni
Stroncone
Rieti
Antrodoco
Pizzoli
Assergi
Penne
Barisciano
Vignanello
Ronciglione
Civita Castellana
Vetralla
Poggio Mirteto
Riserva Naturale Monte Navegna e Monte Cervia
Fiano Romano
Campagnano
Bracciano
Monterotondo
Rocca di Mezzo
Popoli
Pratola Peligna
Sulmona
Carsoli
Tagliacozzo
Celano
Avezzano
Pescina
Cerveteri
Ladispoli
Tivoli
Capistrello
Subiaco
Palestrina
Frascati
Pescasseroli
Albano Laziale
Colleferro
Anagni
Sora
San Donato
1
2
2
2
18
4
2
6

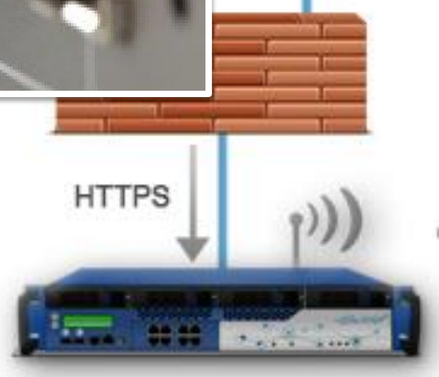
Mappa Funzionale/Applicativa



Controllo Intrusioni fisiche in LAN







HTTPS

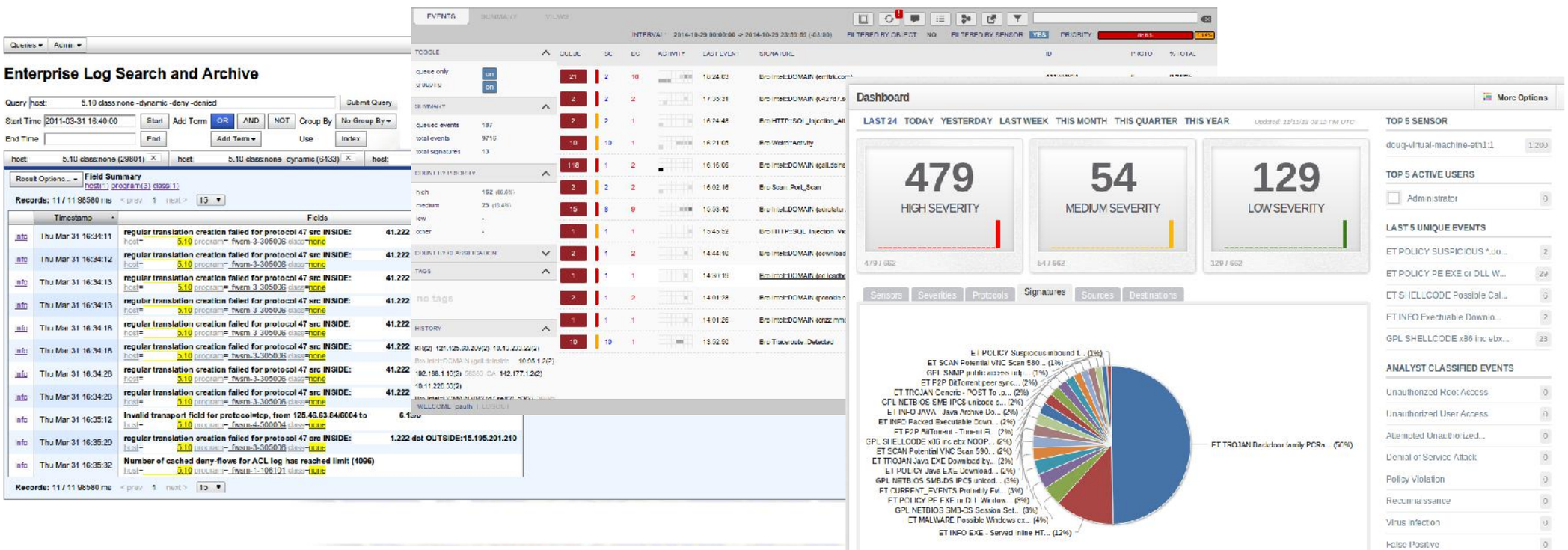
HTTPS

Network Security Monitoring

- 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

Network Security Monitoring

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



Cos'è 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

Cos'è 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
- …