Evoluzione della sicurezza IT

1988

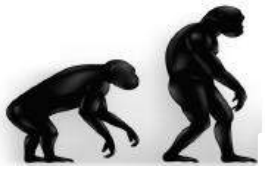
Physical Security…

Prevent the bad guys to enter the computers room

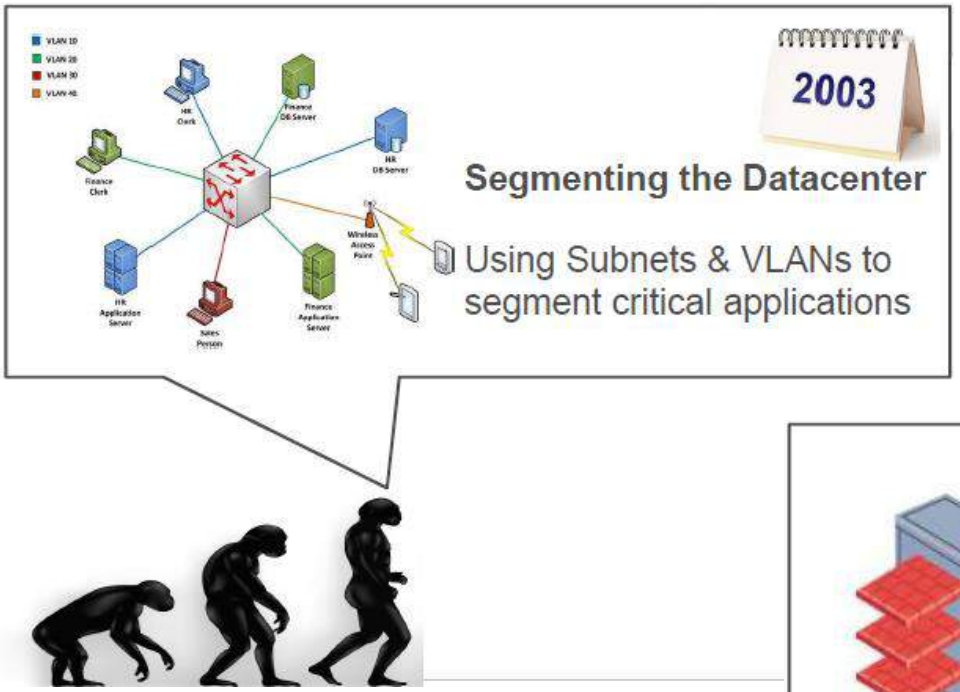
1998

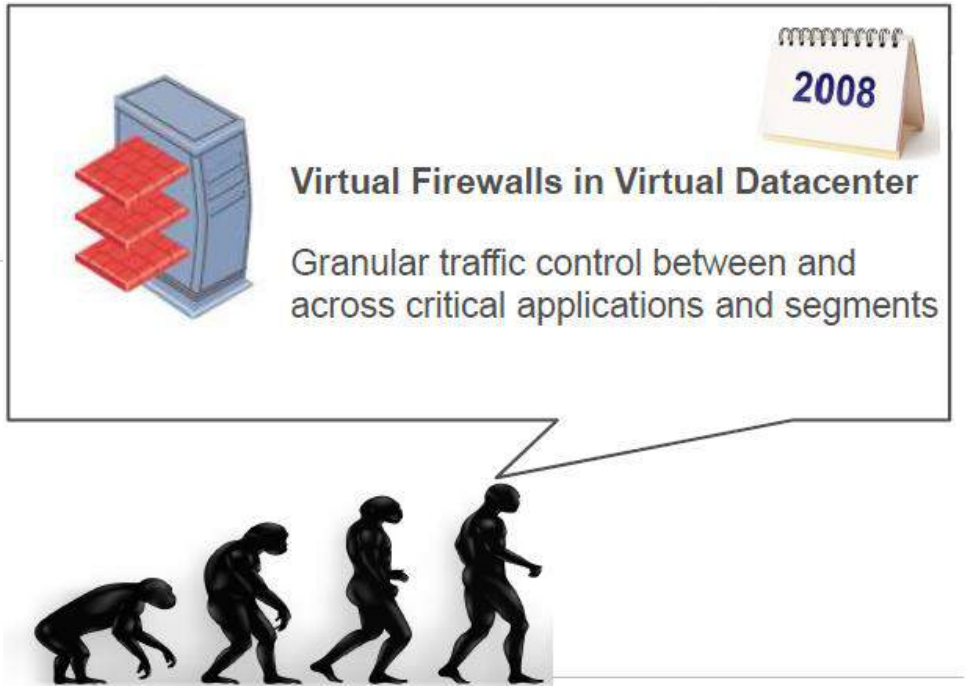
Internet & DMZ Firewalls…

Traffic Control to the Datacenter

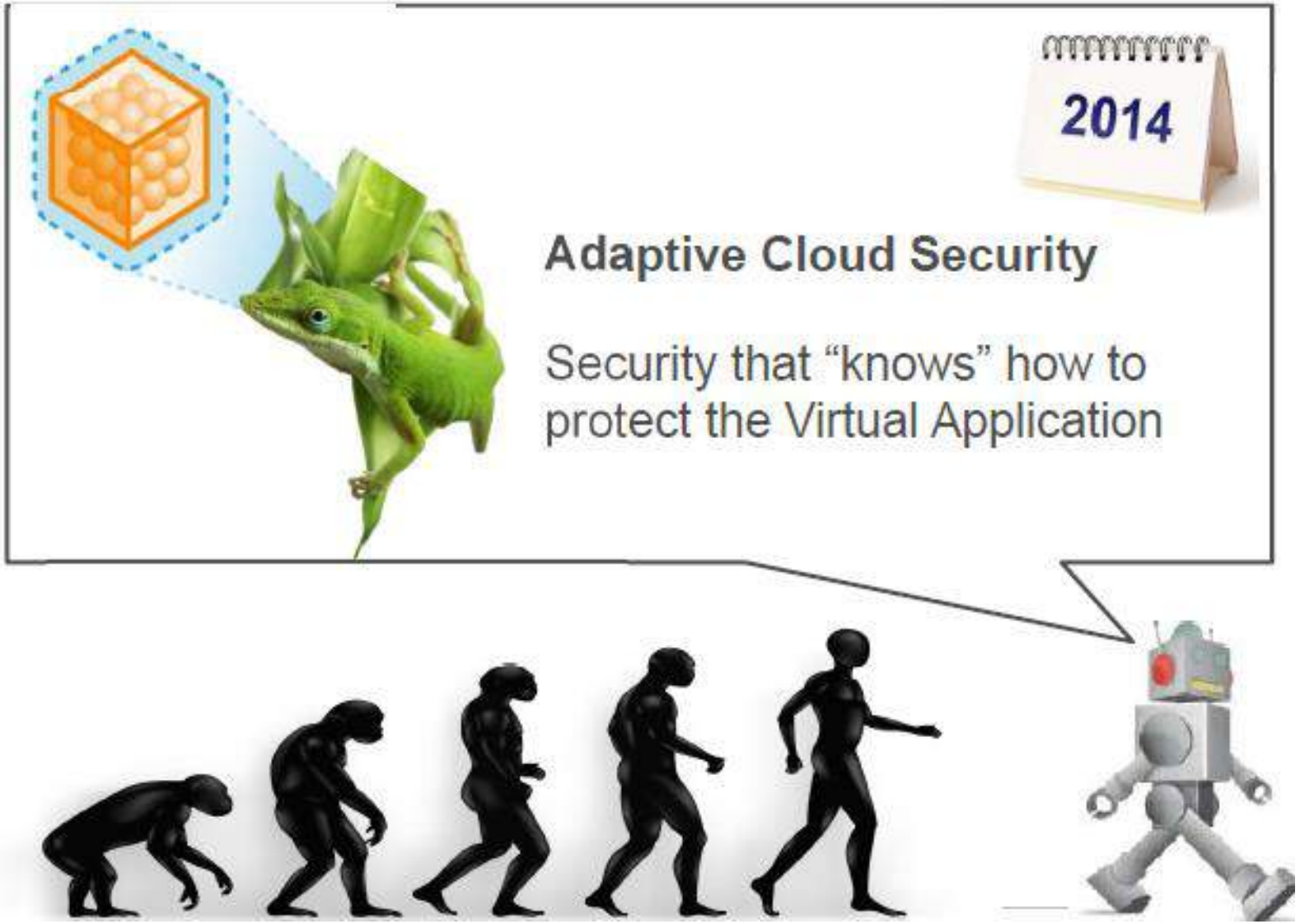


Evoluzione della sicurezza IT





Evoluzione della sicurezza IT



Evoluzione della sicurezza IT

A causa del cambiamento dei target del cyber crime, dello spionaggio e dell'hacktivism, gli attacchi diventano sempre più vari, come ad esempio l'hackeraggio di un sito di news dove è stata riportata la notizia falsa di bombe alla Casa Bianca: **la borsa è crollata** in pochi minuti.

CheckPoint ha eseguito nel 2013 uno studio sulle maggiori minacce alla sicurezza, attraverso l'analisi dei dati reali rilevati su 888 aziende clienti.

L'analisi ha evidenziato che:

- Il 61% delle aziende aveva traffico peer to peer
- Il 53% era vulnerabile ad attacchi sulle postazioni di lavoro
- Il 54% avevano dipendenti che hanno perso informazioni
- Il 63% aveva postazioni di lavoro infettate da BOT
- Il 43% presentava l'uso di anonymizers

Evoluzione della sicurezza IT

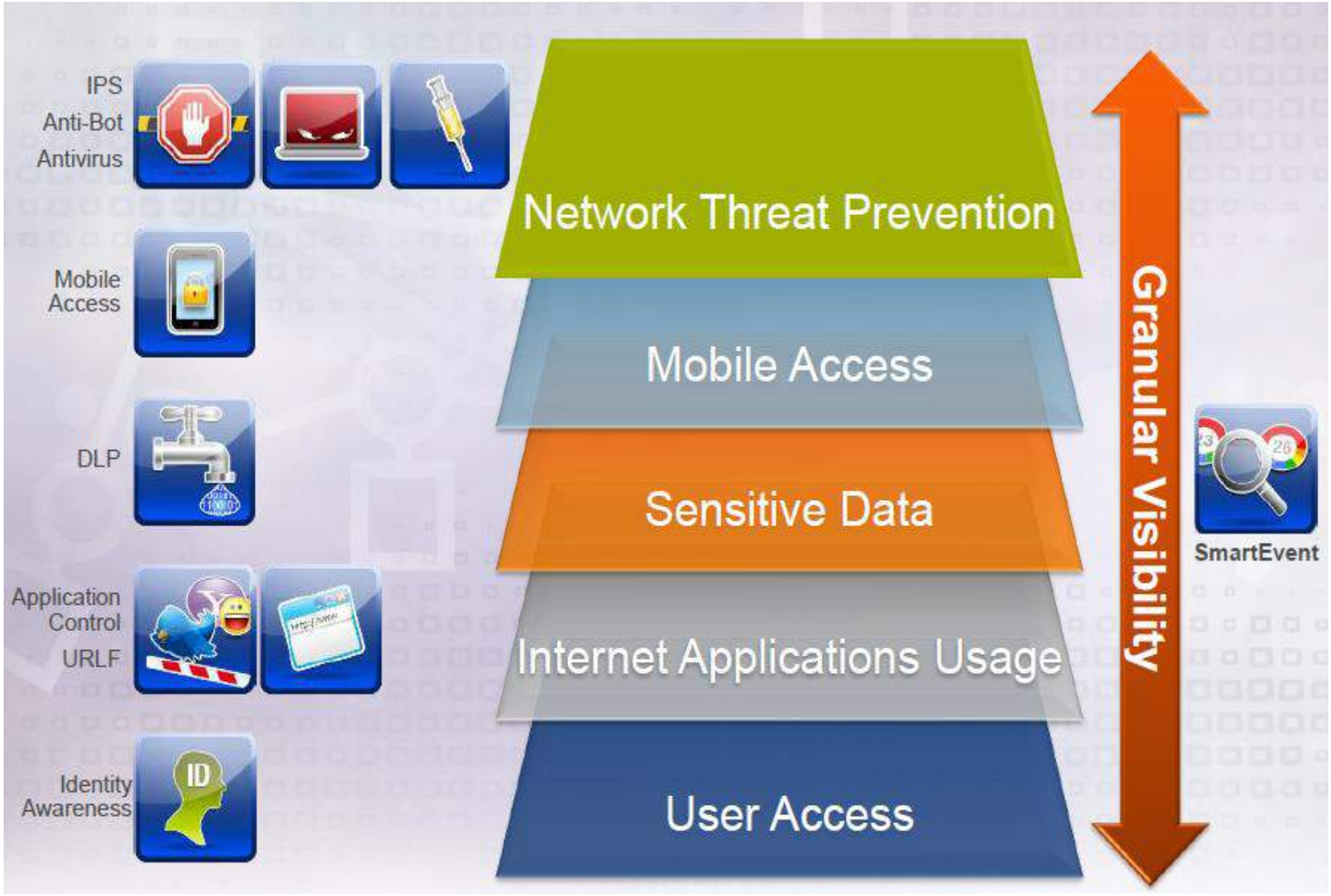
Le soluzioni tecnologiche per affrontare queste minacce sono:

- **Software Blade Architecture**: consente l'implementazione delle policies mediante l'estensione sullo stesso hardware delle componenti software di sicurezza disponibili, gestite centralmente ed in maniera modulare

- **Threat Cloud**: è una rete collaborativa tra gli utenti CheckPoint per la costituzione di una base di conoscenza in tempo reale delle minacce e per il relativo aggiornamento automatico delle protezioni sui singoli apparati

Evoluzione della sicurezza IT

Software Blade: Implementa una architettura di sicurezza multistrato integrando i vari prodotti come indicato nella figura seguente:



Evoluzione della sicurezza IT

Le blade software più interessanti ed innovative sono:

- **Mobile Access**: rende sicuro l'utilizzo privato/aziendale dei dispositivi mobili, creando un ambiente isolato e criptato accessibile solo dietro autenticazione. Implementa inoltre una VPN tra il dispositivo dell'utente ed i servizi Corporate
- **DLP** (data loss prevention): regola l'invio fuori dall'azienda di email (testo ed allegati) con informazioni classificate, come ad esempio numeri di carte di credito, fogli di budget…
- **Threat Emulation**: apre ed esamina il comportamento degli allegati delle email entranti in un'area protetta prima di inviarli all'utente, o bloccarli, nel caso siano dannosi.

- **Application Control**: consente di regolare l'uso di un gran numero di applicazioni che sfuggono ai tradizionali controlli dei firewall (esempio Emule, Torrent, Skype…)
- **URL Filtering** e **Identity Awareness**: prevedono la connessione con Active Directory per identificazione ed autorizzazione alla navigazione, propedeutico a eliminazione proxy

Evoluzione della sicurezza IT

Threat Cloud

Oggi contiene:

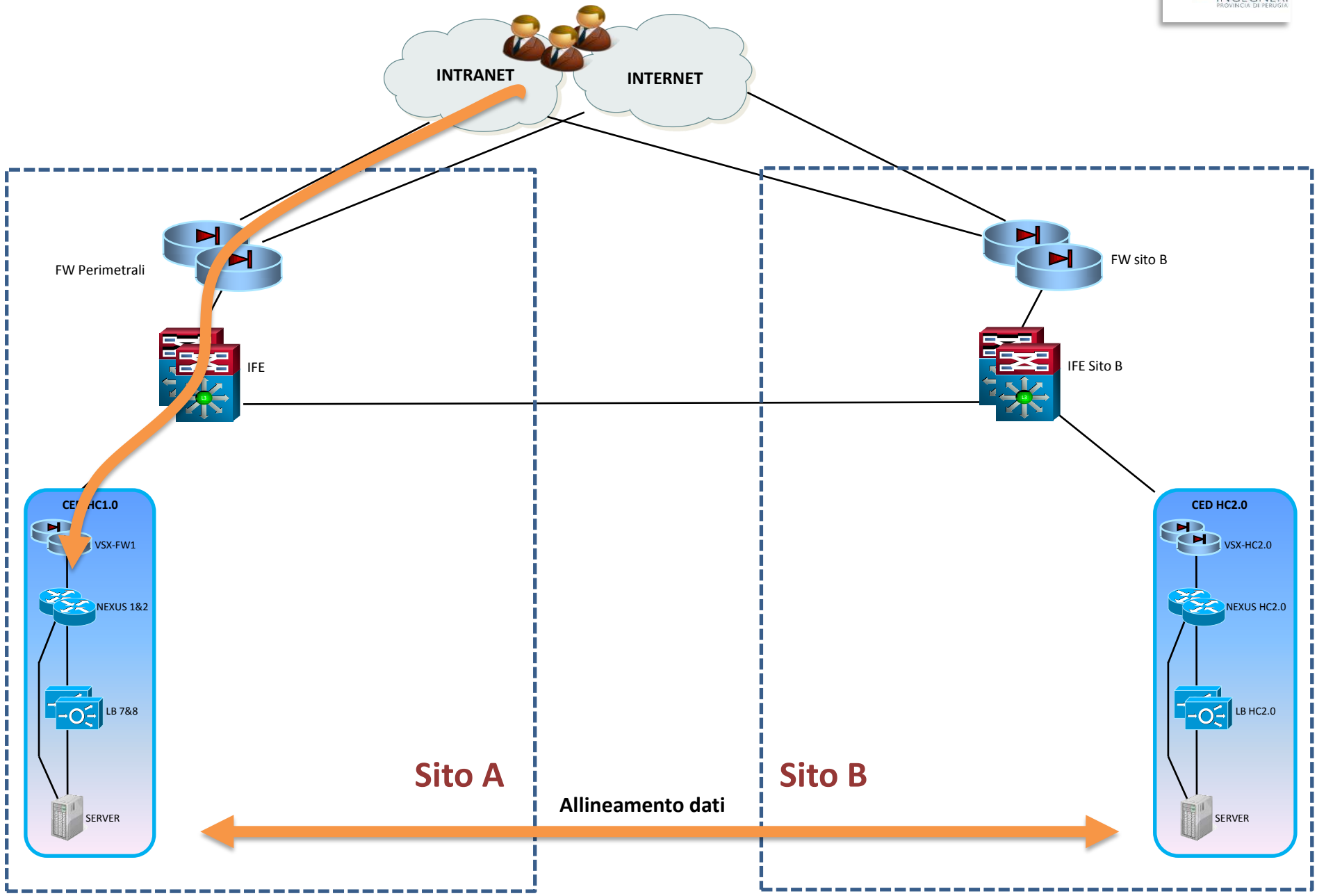
- Oltre 250M di indirizzi analizzati per la BOT discovery
- Oltre 4,5M di firme malware
- Oltre 300k siti affetti da malware

Auto-apprende:

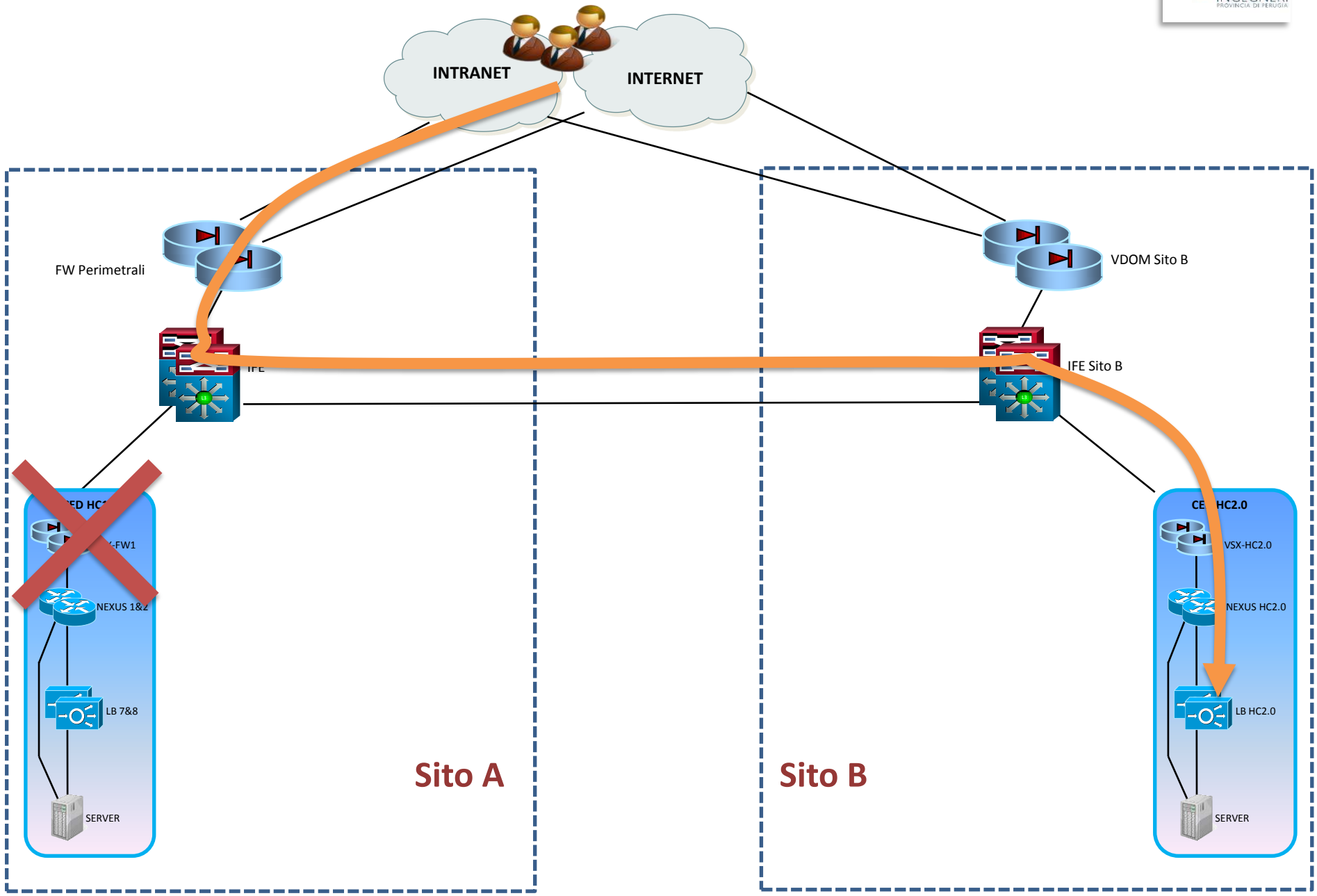
- Dinamicamente dalla rete dei sensori CheckPoint (che sono i dispositivi installati presso i clienti)
- Da analisti CheckPoint
- Da fonti esterne

Distribuisce in real-time le informazioni per l'adeguamento automatico delle configurazioni degli apparati cliente

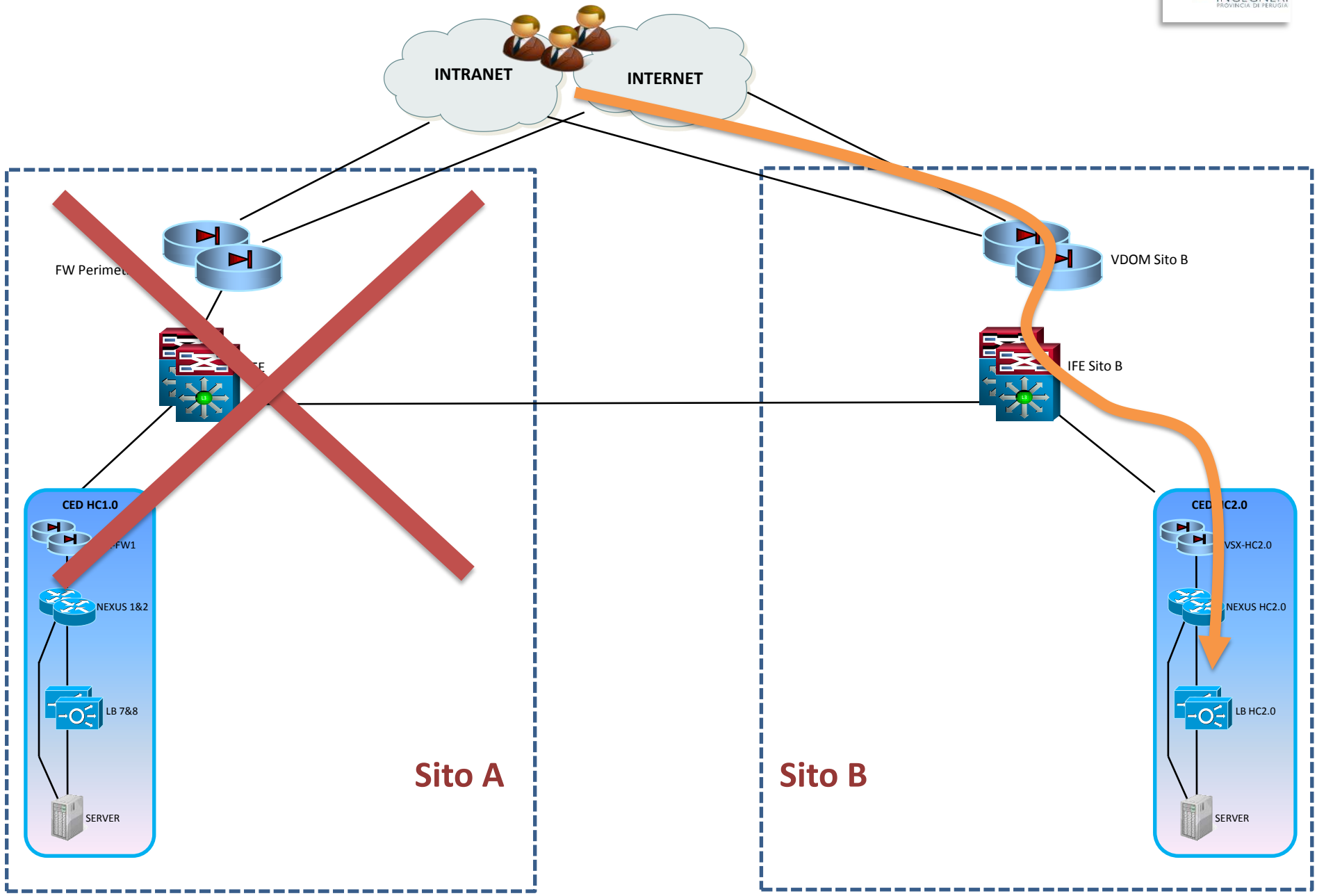
Erogazione del servizio in condizioni normali



Erogazione del servizio da Sito B



Erogazione del servizio da Sito B in caso di Disastro

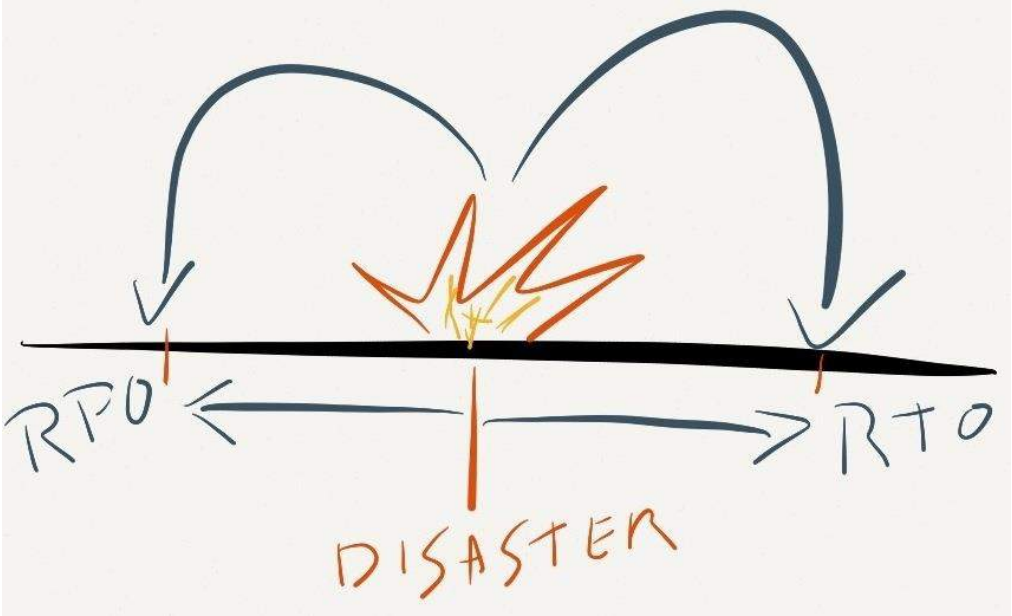


Erogazione del servizio da Sito B in caso di Disastro

Due parametri fondamentali:

RPO: quanti dati ho perso?

RTO: dopo quanto tempo ho di nuovo il servizio?



Erogazione del servizio da Sito B in caso di Disastro

Video Fast DR