Security Summit

Milano 17-18-19 marzo 2026

WatchGuard Technologies

Zero Trust: perché per molti è ancora una difficoltà operativa

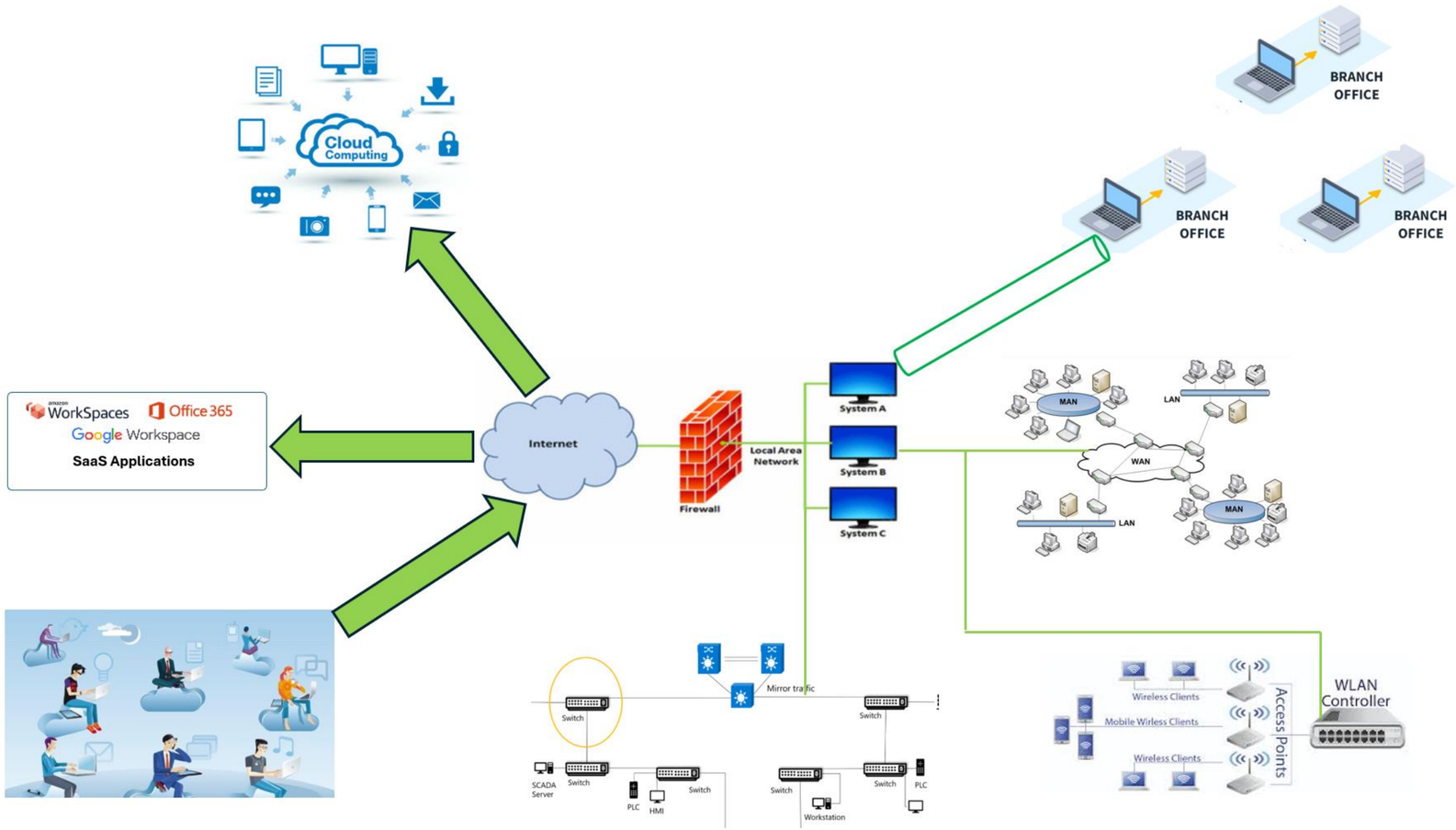
Gianluca Pucci
Manager Sales Engineering - Italy
WatchGuard Technologies

....Perchè difficoltà?.....

E’ molto probabile che la ricerca dello «zero trust» da parte delle aziende si traduca nella ricerca di un prodotto specifico, o di una funzione legata a una soluzione già implementata.....

Lo Zero Trust è un Framework, un approccio alla cybersecurity che si adegua alla trasformazione che la superficie di attacco ha subito

....Trasformazione.....



....Il rischio.....

Il rischio concreto legato a questa difficoltà è il «trascurare», dare per scontato che questa trasformazione, fondamentale per accrescere il proprio Business, non abbia riflessi negativi sugli aspetti di sicurezza e che basti avere qualche prodotto specifico installato storicamente a garanzia

.....Il giusto approccio....

.....viene facile dire non lasciare nulla al caso e non trascurare nulla....

..Digitalmente parlando questo vuol dire tutelare al meglio: Identità, utenti mobili/accessi esterni, perimetro, segmentazione, sedi remote, infrastruttura wireless, singoli device, movimenti interni di rete, Cloud, OT/IoT...

….WatchGuard mi aiuta…..

- **Soluzioni e visione aziendale coerenti ed in linea con la mutabilità della superficie di attacco**

- **Piattaforma unica di gestione, correlazione eventi di sicurezza e autoremediation**

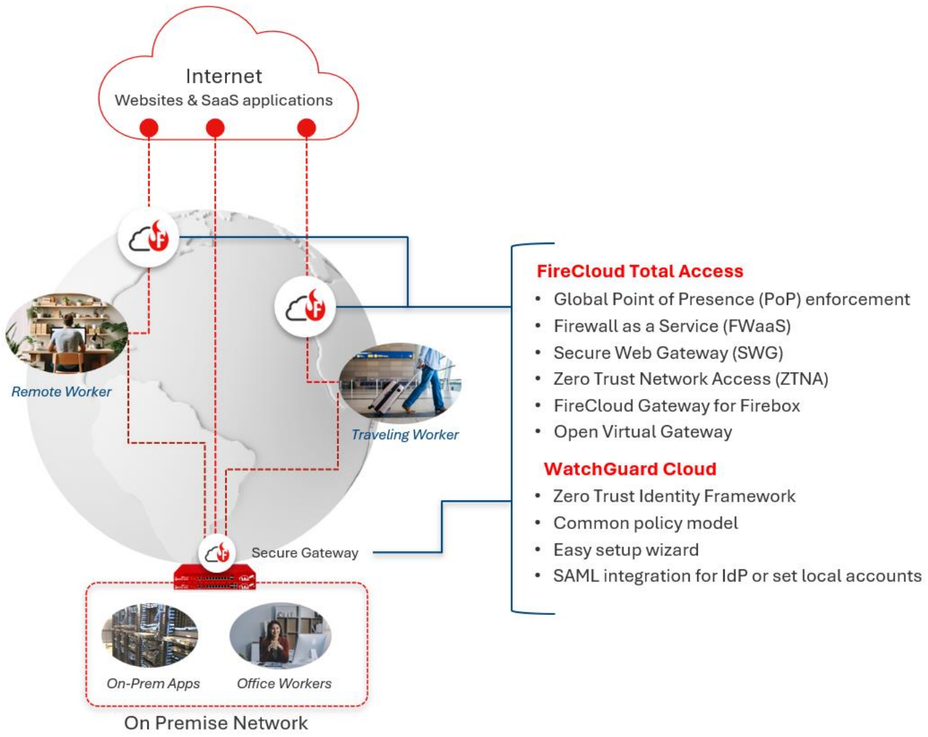
- **Orientamento al Framework Zero Trust unico semplificando le integrazioni tecnologiche fra soluzioni WatchGuard e terze parti**

- **Log e reportistica per visibiltà e nel rispetto delle compliances**

- **Proposizione in modalità servizio gestito per rendere più snello il lavoro del partner a favore dei propri clienti**

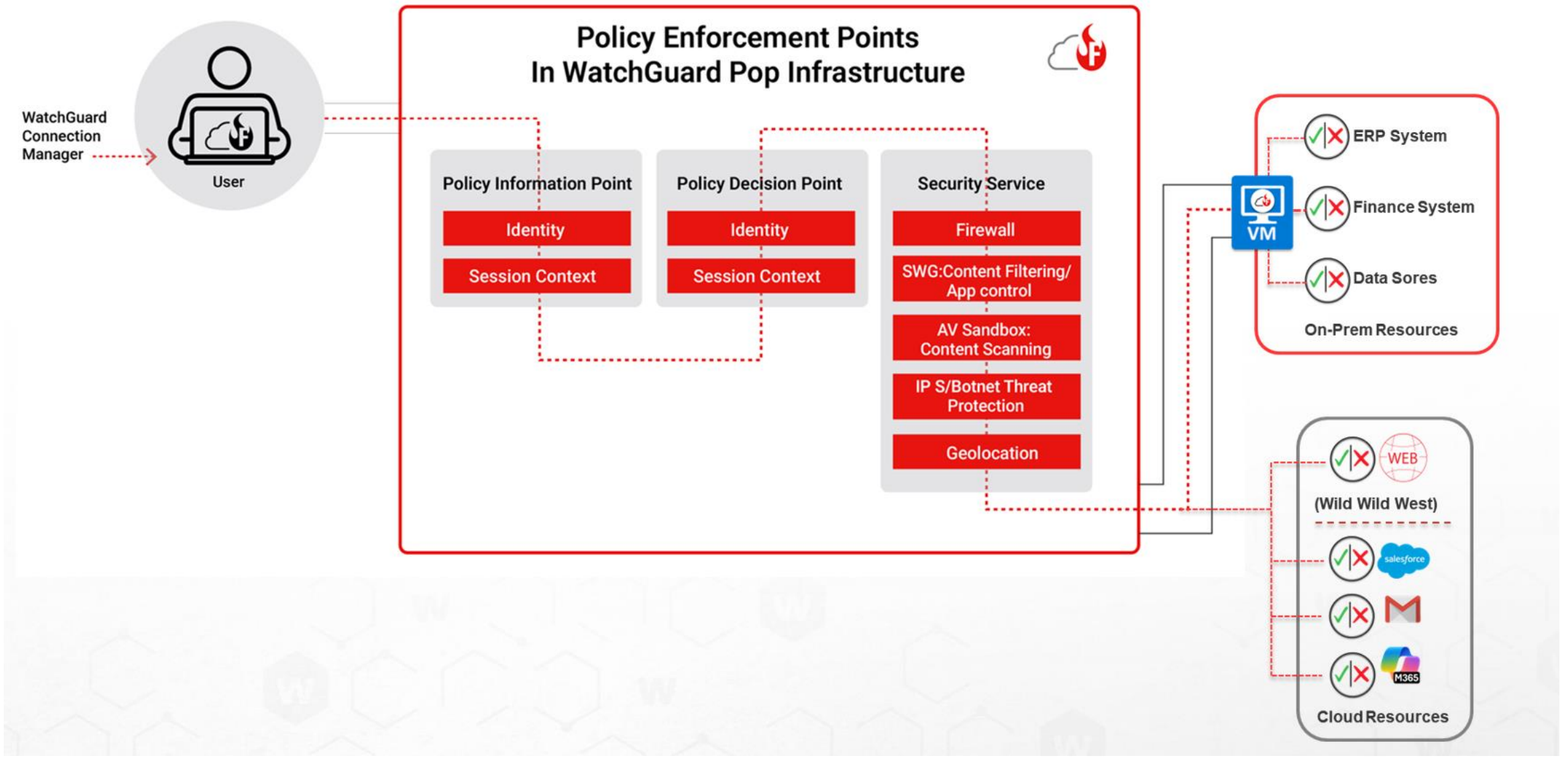
- **Il Team WatchGuard sempre a vostra disposizione…**

....Alcuni esempi.....FireCloud FWaaS & ZTNA....



- **Protezione accesso internet con gli stessi paradigmi di sicurezza adottati in azienda**
- **Connessione forzata e persistenze secondo il principio Zero Trust**
- **Soluzione ZTNA per rendere accessibili le risorse locali, limitatamente agli applicativi autorizzati con conseguente diminuzione della superficie di attacco**
- **Inspection SSL nativa**
- **Autenticazione strong con possibile integrazione MFA/PassKey**
- **Strumenti di visibilità continuativa**

....Alcuni esempi.....FireCloud FWaaS & ZTNA....



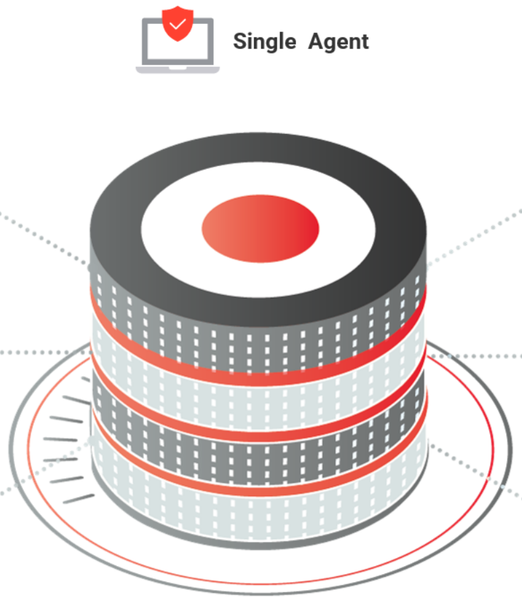
....Alcuni esempi.....EPDR & Zero Trust Application Service....

Prevenzione

Zero Trust Application Service
Le applicazioni sconosciute e non attendibili vengono bloccate per impostazione predefinita, bloccando malware e ransomware prima dell'esecuzione, comprese le minacce zero-day.

Behavior-based attack prevention
Le azioni dannose vengono interrotte automaticamente, anche quando gli aggressori abusano di strumenti legittimi o tecniche senza file.

Attack surface reduction by policy
Script, strumenti e dispositivi vengono controllati in anticipo per eliminare i percorsi di attacco comuni.



Archivio dati di investigazione e intelligence arricchito

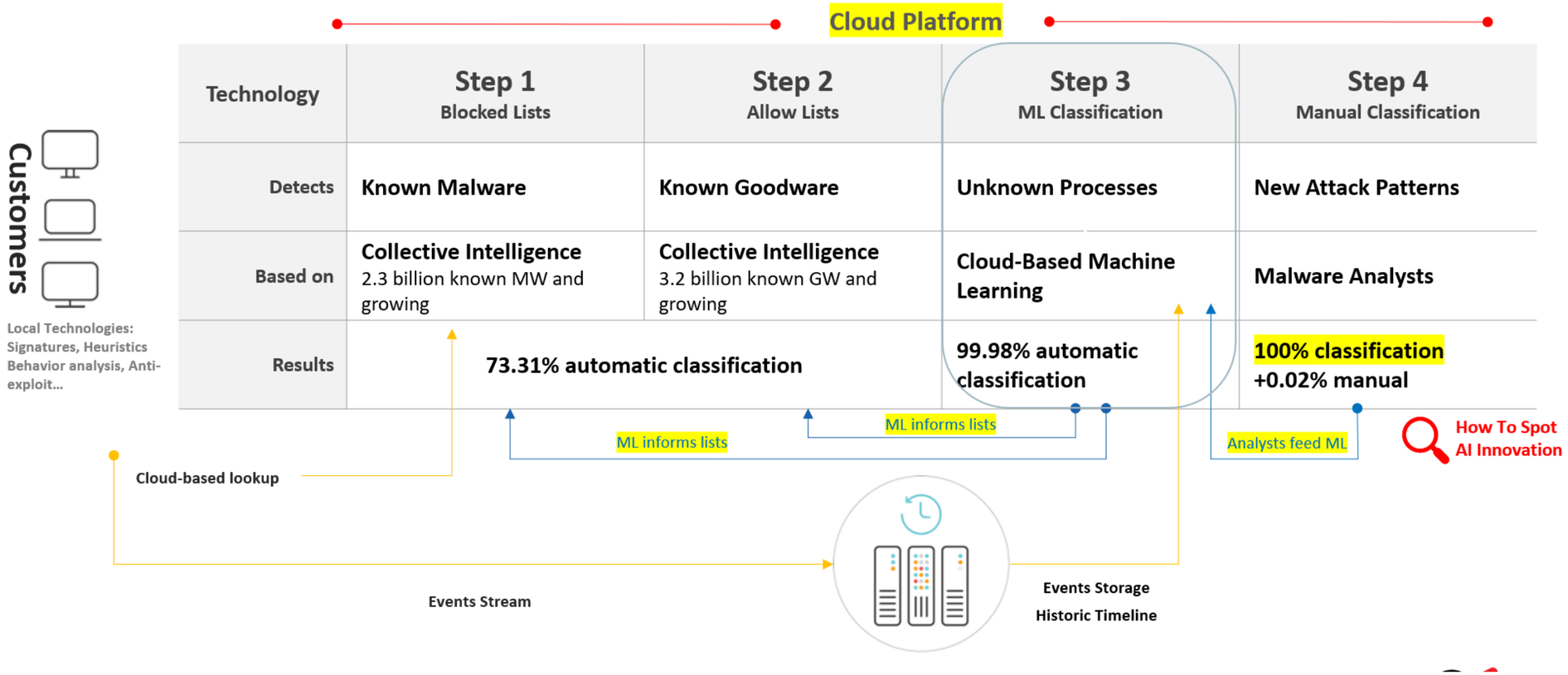
Detection and Response

AI-driven incident detection
L'intelligenza artificiale correla le attività correlate in incidenti ad alta fedeltà, fornendo contesto e chiarezza anziché avvisi rumorosi e isolati.

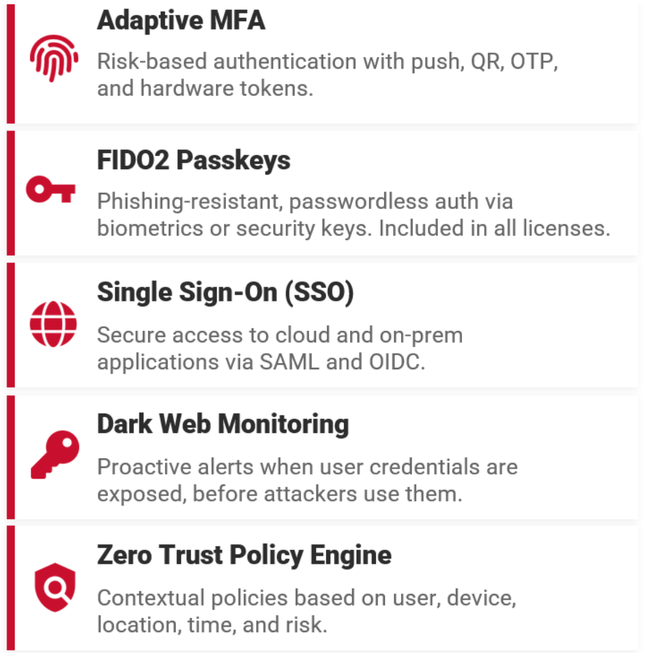
Threat Hunting & Investigation
L'automazione dell'intelligenza artificiale e la telemetria approfondita collegano l'attività in un'unica storia di attacco, consentendo una ricerca proattiva e una comprensione più rapida della portata, dell'impatto e della causa principale.

Automated Remediation
Le minacce vengono contenute e rimosse automaticamente, con l'intelligenza artificiale che guida la correzione per eliminare la persistenza e ridurre l'MTTR.

....Alcuni esempi.....EPDR & Zero Trust Application Service....

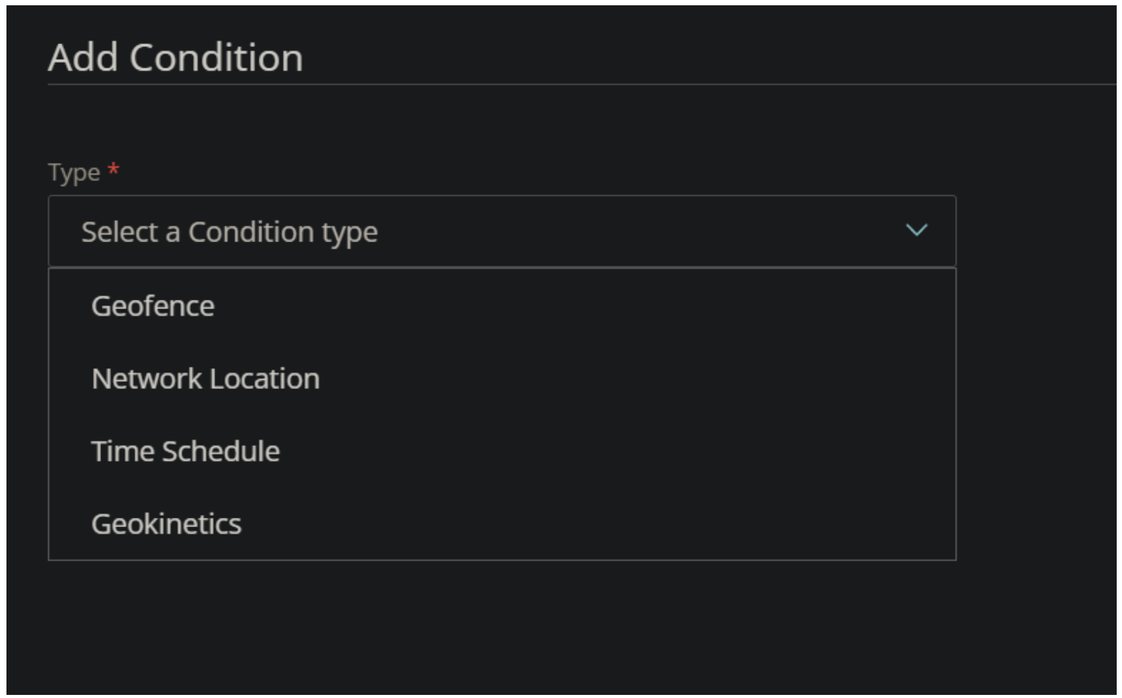


....Alcuni esempi.....AuthPoint MFA....



- **Protezione accessi VPN**
- **Protezione accessi amministrativi PC/Server**
- **Protezione accessi web application SAML/OIDC**
- **Integrazione ADFS/RD Web**
- **Integrazione XDR correlazione eventi e remediation con end-point e gli altri asset WatchGuard**
- **Full Cloud managed solution**
- **Sincronizzazione utenze Entra ID/ Local AD**

….Alcuni esempi…..AuthPoint MFA….



- **Autenticazioni vincolate al contesto**
- **Geolocalizzazione: definizione locazione geografica sulla quale condizionare l'accesso**
- **Network Location: Definizione condizione IP provenienza richiesta**
- **Schedule: Definizione accesso su condizione temporale**
- **Geokinetics: gestione autenticazioni successive basate su discriminante velocità oraria**

Q&A

Contatti:
gianluca.pucci@watchguard.com

Venite a trovarci al nostro Stand!