Forcepoint

Sintesi della soluzione

Forcepoint Next Generation Firewall con Amazon Web Services

Il firewall di fascia enterprise più sicuro ed efficiente, a gestione centralizzata, sempre attivo e vigile

Sfida

- Aziende e organizzazioni devono proteggere i loro ambienti cloud e ibridi con lo stesso livello di sicurezza che avevano nelle tradizionali infrastrutture on-premise
- Lo sviluppo e la manutenzione di un'infrastruttura cloud o ibrida sicura possono essere costosi e tecnicamente complessi
- La conformità alle normative può richiedere molto impegno e tempo

Soluzione

- Forcepoint Next Generation Firewall (NGFW) offre soluzioni basate su software, studiate per offrire il massimo della sicurezza con costi e complessità ridotti al minimo
- Forcepoint NGFW Security Management Center (SMC) è una piattaforma unificata che snellisce i processi e offre visibilità e controllo
- Con Forcepoint NGFW SMC gli amministratori IT possono snellire il lavoro necessario per raggiungere la conformità su reti fisiche e virtuali, incluso l'accesso agevole ai report di controllo

Risultato

- Massima sicurezza in ambienti cloud e ibridi e minima complessità
- Risposta più rapida agli incidenti
- Processi semplificati di gestione, implementazione e conformità alle normative
- Costo inferiore per la sicurezza e l'infrastruttura di rete

Forcepoint Next Generation Firewall (NGFW) collega e protegge le persone e i dati che utilizzano in tutta la rete aziendale ibrida o nel cloud, con la massima efficienza, disponibilità e sicurezza. Scelte da migliaia di clienti in tutto il mondo e disponibili in AWS Marketplace, le soluzioni per la sicurezza di rete Forcepoint permettono ad aziende e organizzazioni di affrontare e risolvere le criticità con efficienza e a costo conveniente.

Sicurezza Forcepoint per ambienti cloud pubblici

I servizi basati su cloud e le distribuzioni virtuali stanno trasformando le aziende di ogni tipo e dimensione. Le apparecchiature hardware tradizionali stanno scomparendo rapidamente dalle sedi locali perché, per restare competitive, le organizzazioni hanno bisogno di maggiore efficienza, agilità e controllo dei costi, senza oneri amministrativi e di manutenzione. Questa diffusa adozione delle architetture cloud aumenta le responsabilità che gravano sui professionisti della sicurezza e sui responsabili IT, chiamati a garantire che questi nuovi ambienti siano sicuri tanto quanto i precedenti ambienti fisici.

Forcepoint Next Generation Firewall (NGFW) offre soluzioni basate su software, studiate per offrire il massimo della sicurezza con costi e complessità ridotti al minimo. Forcepoint NGFW Security Management Center (SMC) è una piattaforma unificata che offre funzioni di visibilità e controllo ineguagliate e applicazione uniforme delle policy, per aiutare a garantire la conformità alle normative sia nell'infrastruttura fisica sia negli ambienti cloud e virtuali.

Sicurezza cloud di AWS

Per proteggere gli ambienti cloud, Forcepoint introduce in AWS la sua tecnologia firewall di ultima generazione, con caratteristiche di scalabilità ed efficienza comprovate e una solida funzionalità di protezione. Amplia facilmente e in sicurezza la rete della tua organizzazione, dai data center e dal perimetro di rete fino alle filiali e alle sedi remote, nell'ambiente cloud di AWS tramite un gateway VPN (Virtual Private Network) sicuro. La nostra gestione centralizzata ti consente di creare e distribuire le policy velocemente e in modo omogeneo in tutti i tuoi sistemi. Potrai vedere rapidamente nel dettaglio che cosa succede sia nel tuo ambiente AWS sia sulla tua rete fisica.

I clienti che passano a Forcepoint NGFW segnalano un calo dell'86% negli attacchi IT, un alleggerimento del 53% (in termini di tempo) del carico di lavoro che grava sull'IT e una riduzione del 70% nelle attività di manutenzione programmata.

Massima sicurezza, minima complessità

L'architettura basata su software della sicurezza di Forcepoint per soluzioni come la protezione dalle minacce avanzate, l'ispezione approfondita dei pacchetti e il controllo a livello di applicazione, è studiata per facilitare la distribuzione e aiutare ad assicurare la massima sicurezza senza incrementare la complessità e i costi. La piattaforma di sicurezza Forcepoint basata su software offre una protezione defense-in-depth integrata e completa, personalizzabile in base alla specifiche esigenze di ogni utente, luogo o asset, e include firewall, VPN, IPS e protezione con URL Filtering. Questa piattaforma software offre tutte le funzionalità tipiche delle appliance hardware, inclusi ispezione stateful, controllo granulare delle policy e degli accessi e connessioni ISP ridondanti, ma senza l'ingombro fisico.

Visibilità e controllo in tempo reale

Diversamente dalle console di gestione tradizionali, Forcepoint NGFW offre visibilità e controllo completi sul flusso del traffico nell'ambiente sia virtuale che cloud. SMC crea rapidamente report sulla quantità di traffico in transito tra i sistemi virtuali e avvisa gli amministratori di imminenti malfunzionamenti di un sistema. Puoi gestire qualsiasi numero o combinazione di cluster o dispositivi Forcepoint fisici o virtuali, nonché le versioni software in esecuzione su hardware x86 standard. SMC rafforza anche la sicurezza dei sistemi virtuali tramite un dashboard per il monitoraggio olistico con un controllo granulare e una visibilità su tutto lo stack di applicazioni.

Semplifica la conformità alle normative

Rispettare i requisiti normativi più recenti, come PCI DSS, HIPAA, Sarbanes-Oxley e FISMA nel mondo fisico non è facile, ma assicurare la conformità nel mondo virtuale lo è ancor meno. Nell'ambiente virtuale, infatti, mancano i controlli tradizionali che sorvegliano ogni applicazione. Di conseguenza è pressoché impossibile sapere quali dati sono stati utilizzati, da chi e quando e, probabilmente, questa mancanza di trasparenza mette in allarme i revisori. SMC ti offre il livello di monitoraggio, analisi e reportistica necessario per facilitare la conformità nelle reti fisiche e virtuali. Raccoglie dati completi su tutti gli eventi di rete e li presenta in log di controllo chiari e di facile leggibilità. SMC elenca, inoltre, le impostazioni di sicurezza e segnala le modifiche apportate al sistema, offrendo report di controllo accurati e completi alla semplice pressione di un pulsante.

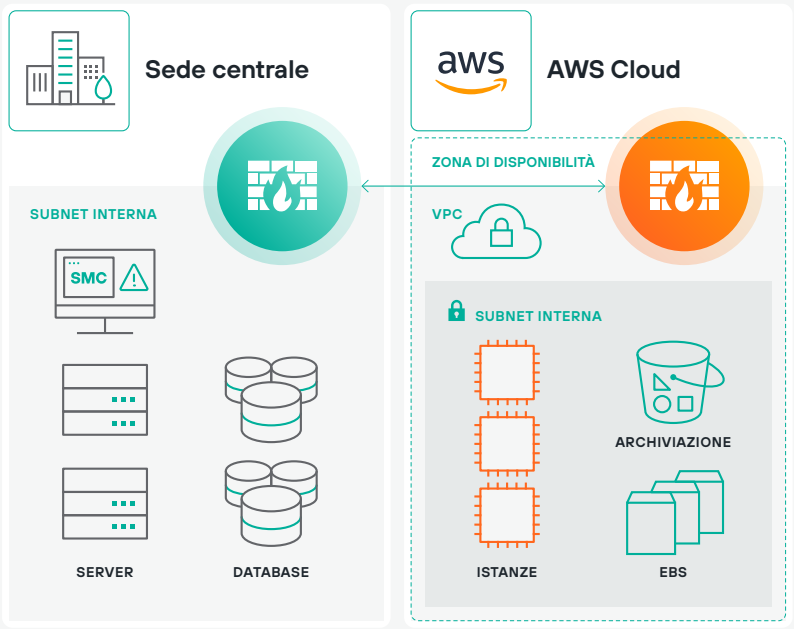
Distribuzione veloce ed elastica

Per distribuire rapidamente la sicurezza dell'architettura Forcepoint basata su software nel tuo ambiente AWS, basta scegliere una delle opzioni disponibili in AWS Marketplace

→ Visita il Marketplace

Soluzioni Forcepoint NGFW + AWS

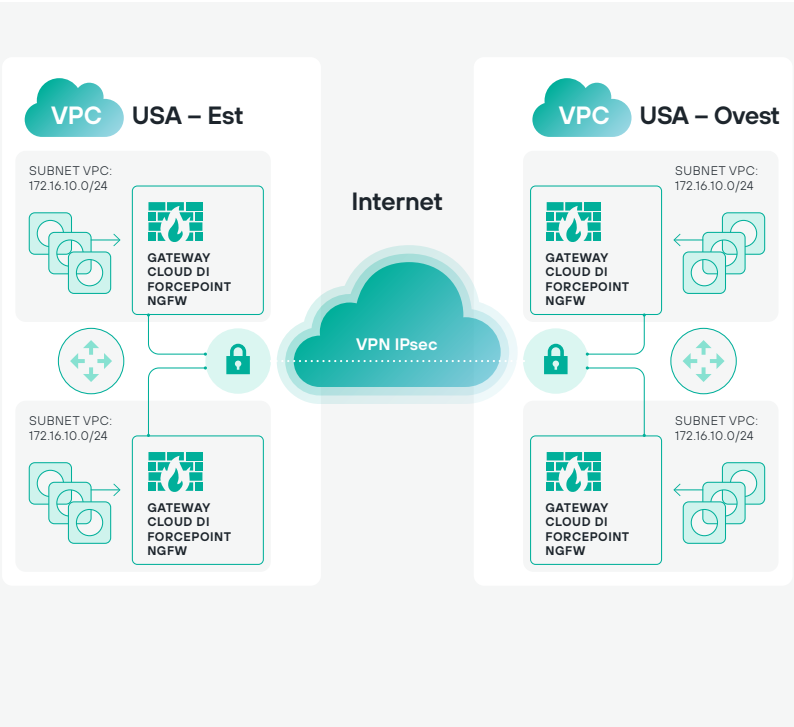
Estendi in modo sicuro le reti aziendali e sfrutta tutta la potenza di AWS, con Forcepoint NGFW



Estendi le reti aziendali negli ambienti AWS

Forcepoint NGFW applica policy di prevenzione delle minacce specifiche per applicazione, in modo da impedire a exploit, malware e vulnerabilità zero-day di compromettere i dati, tentando di esfiltrarli dall'ambiente o dagli ambienti AWS di un'azienda. AWS Security Hub offre visibilità centralizzata sulle azioni e le condizioni che hanno attivato avvisi per l'applicazione delle policy.

- → Estendi la rete della tua organizzazione in AWS
- → Abilita l'IT ibrido con efficienza e semplifica il trasferimento dei dati a/da AWS
- → Gestisci facilmente entrambi i lati di più connessioni VPN da un'unica posizione



Routing da VPC a VPC interregionale

Connetti in sicurezza le VPC tra più regioni AWS. Con la tecnologi adi sicurezza di rete di Forcepoint, leader di settore, puoi gestire, controllare e applicare le policy di sicurezza.

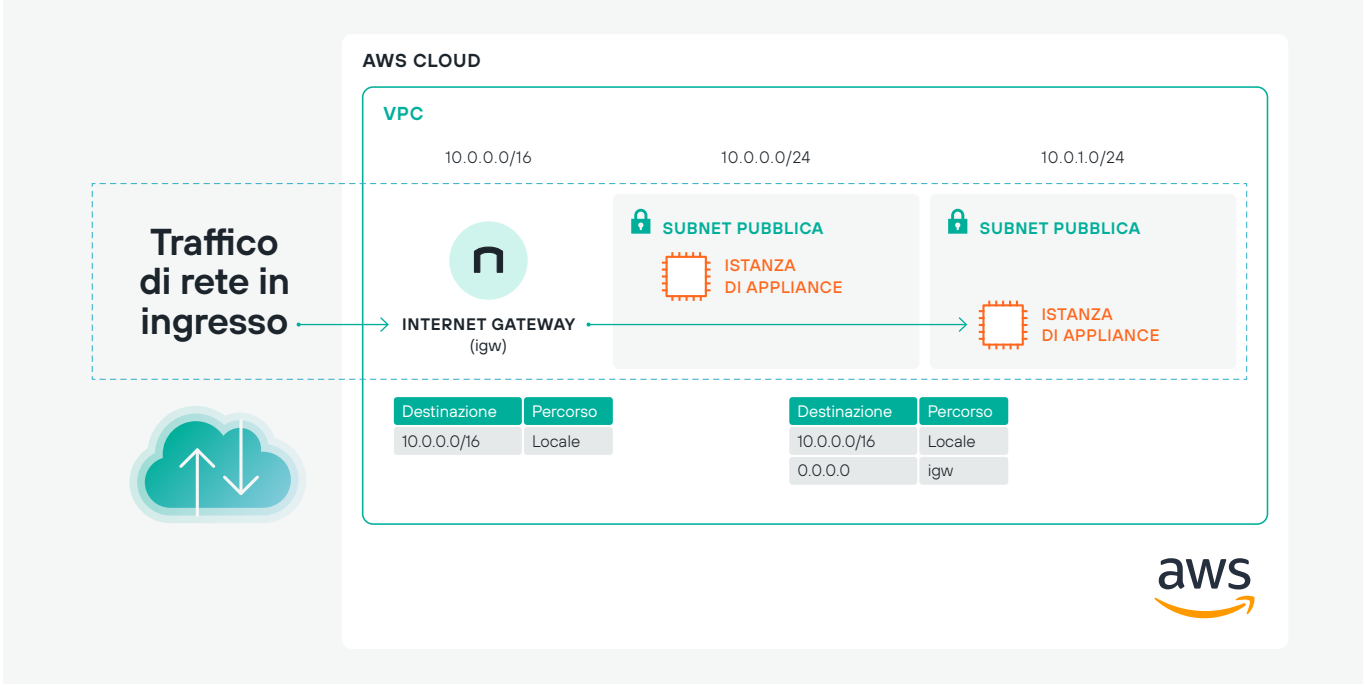
- → Proteggi le informazioni trasferite tra diverse regioni
- → Applica policy di sicurezza coerenti tra regioni

Grazie all'adozione di NGFW con SD-WAN di Forcepoint e al passaggio al cloud, un fornitore di energia ha risparmiato il 90% dei suoi costi WAN, il tutto con una distribuzione zero-touch.

Amazon VPC Ingress Routing

Amazon VPC Ingress Routing semplifica l'integrazione della sicurezza di rete con la tua infrastruttura Amazon Virtual Private Cloud (VPC), semplificando l'applicazione uniforme delle policy di sicurezza su tutta la rete aziendale, sia nel cloud che on-premise, per proteggere efficacemente i tuoi carichi di lavoro AWS.

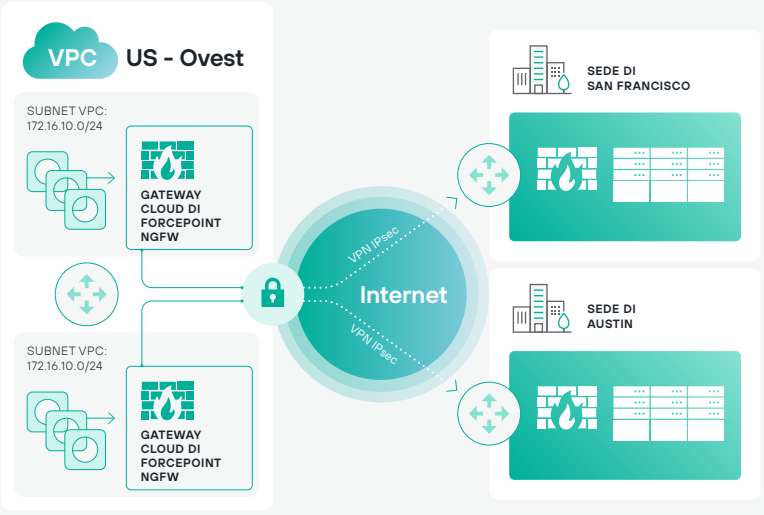
- → Ottieni la flessibilità che ti occorre per trattare il traffico destinato ad Amazon VPC con lo stesso livello di attenzione utilizzato per l'accesso alla rete aziendale
- → Applica le policy per la sicurezza della rete in modo omogeneo sull'intera rete aziendale, senza aggiungere latenza
- → Ottieni il massimo della sicurezza con costi e complessità ridotti al minimo



AWS VPN CloudHub

Connetti in sicurezza le VPC tra più regioni AWS. Con la tecnologi adi sicurezza di rete di Forcepoint, leader di settore, puoi gestire, controllare e applicare le policy di sicurezza.

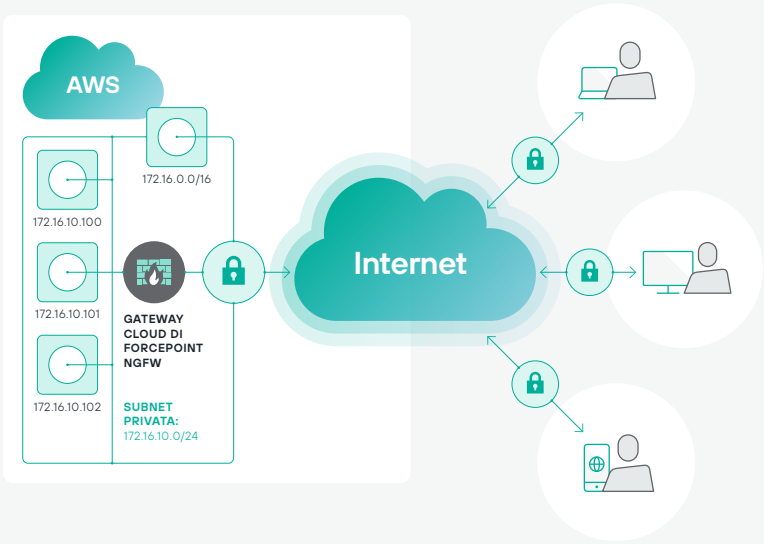
- → Proteggi le informazioni trasferite tra diverse regioni
- → Applica policy di sicurezza coerenti tra regioni



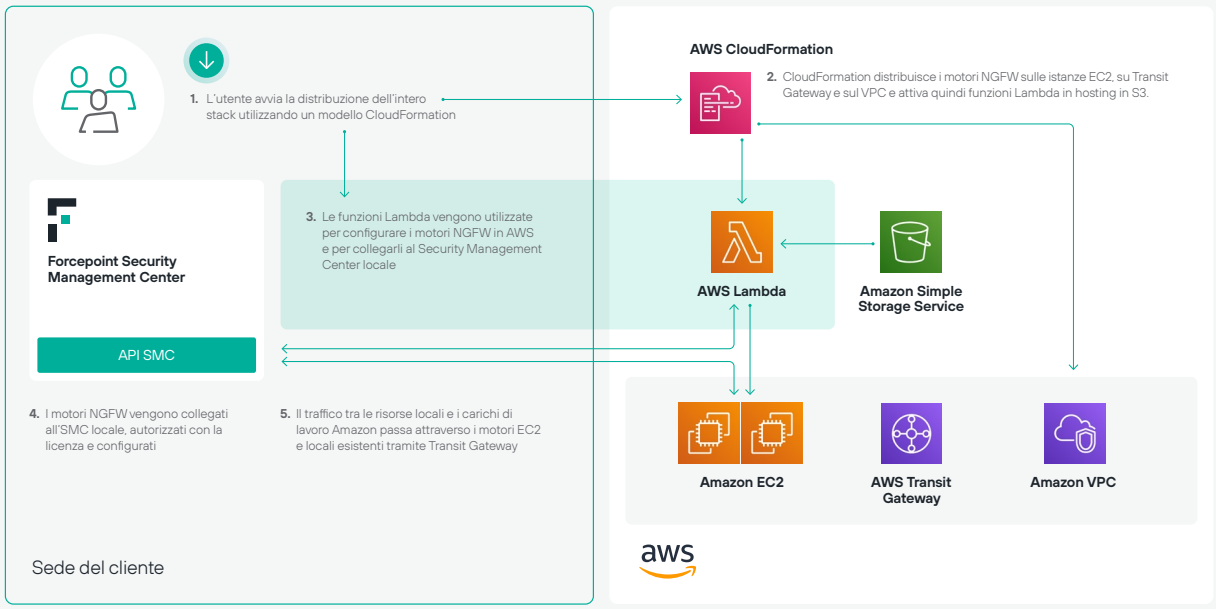
Connettività per accesso remoto

Forcepoint NGFW può essere utilizzato come gateway del perimetro cloud per collegare i tuoi utenti remoti ad Amazon Virtual Private Cloud (VPC). Il gateway cloud di Forcepoint NGFW può essere utilizzato in un'istanza Amazon Elastic Compute Cloud (EC2) per offrire funzionalità avanzate di firewall e proteggere le tue istanze EC2 per tutti gli accessi in ingresso e in uscita, ad esempio:

- → Riconoscimento delle applicazioni
- → Funzionalità di identificazione degli utenti



Forcepoint NGFW + integrazioni dei servizi AWS

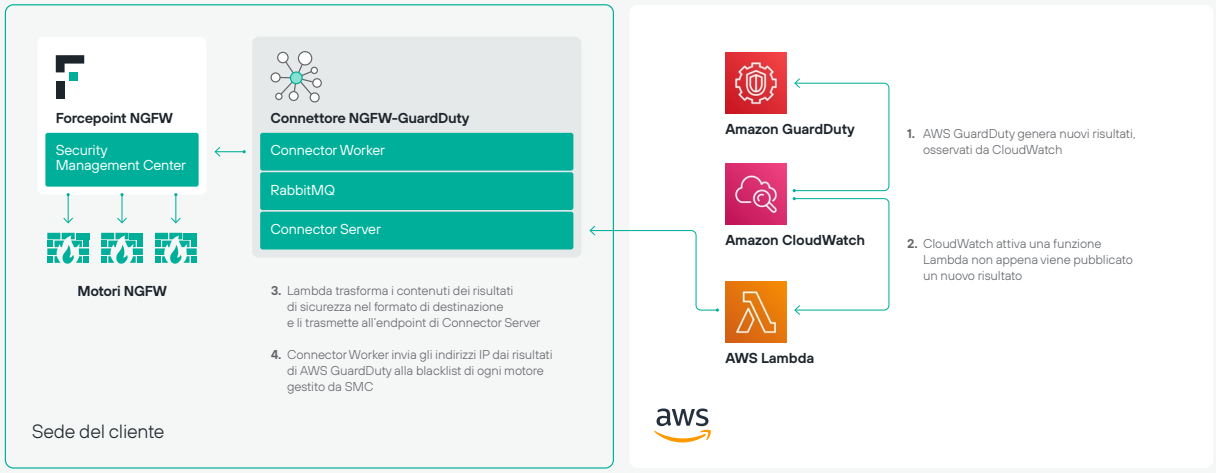


Integrazione di Transit Gateway

Distribuisce un set ridondante di Forcepoint Next Generation Firewall come istanze EC2 e un AWS Transit Gateway e collega i motori NGFW a un Forcepoint Security Management Center esistente, utilizzando funzioni AWS Lambda. Tra i motori NGFW nel cloud e il Transit Gateway vengono configurati tunnel IPSEC ridondanti, e ai motori NGFW in AWS possono essere applicate politiche di sicurezza gestite da Forcepoint Security Management Center per proteggere il flusso del traffico al/dal Transit Gateway.

- → Abilita l'applicazione cerente delle policy di sicurezza tra gli ambienti on-premise e AWS
- → Automatizza la distribuzione dell'intero stack di tecnologie utilizzando un singolo modello AWS CloudFormation, con parametri personalizzabili per consentire distribuzioni su misura

Scarica la Guida

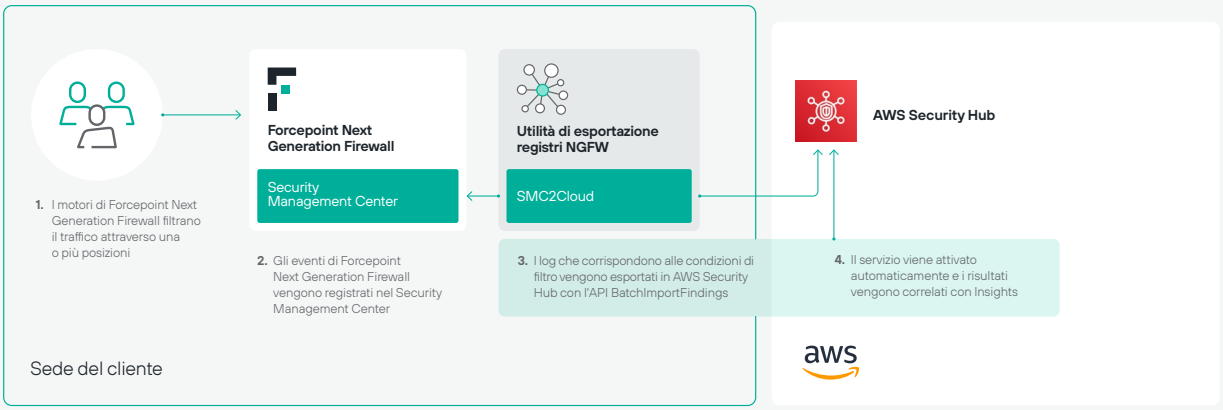


Integrazione di Amazon GuardDuty

GuardDuty offre ai clienti AWS un'opzione intelligente e conveniente per il rilevamento continuo delle minacce in AWS Cloud. Il servizio utilizza l'apprendimento automatico, il rilevamento delle anomalie e la threat intelligence integrata per identificare e stabilire la priorità delle potenziali minacce. L'integrazione di Forcepoint NGFW automatizza l'importazione in tempo reale dei risultati della sicurezza di Amazon GuardDuty.

- → Utenti, applicazioni e servizi ospitati on-premise e protetti da NGFW sfruttano i vantaggi dell'aumentata visibilità degli hacker che attaccano gli ambienti AWS di un'organizzazione
- → Gli indirizzi IP di origini malevole identificati da Amazon GuardDuty vengono inseriti in una blacklist disponibile su un'intera flotta di motori NGFW distribuiti in tutte le sedi aziendali
- → Assicura una protezione avanzata grazie all'intelligence condivisa

Scarica la Guida



Interoperabilità con AWS Security Hub

AWS Security Hub offre una vista unificata del tuo stato di sicurezza sugli account AWS. L'integrazione di Forcepoint con AWS Security Hub offre visibilità sul modo in cui gli utenti interagiscono con i tuoi dati più sensibili, ovunque siano.

- → Esporta automaticamente gli eventi dei log da Forcepoint NGFW ad AWS Security Hub in tempo reale, per accelerare i tempi di risposta
- → Correla i risultati della sicurezza con altre fonti per migliorare la visibilità su tutte le posizioni protette da NGFW
- → Gestisci facilmente i dati raggruppandoli in base a vari campi, ad esempio per gravità e tipo, in modo da dare la priorità a ciò che conta di più per la tua organizzazione

Scarica la Guida Pianifica una demo