CHECK POINT

# CloudGuard Intelligence

*Cloud Intelligence e Threat Hunting*


## Approfondimenti

Le aziende migrano ed espandono le loro applicazioni e i loro servizi in ambienti multi-cloud a un ritmo senza precedenti. Nonostante i numerosi vantaggi del multi-cloud, ciò crea anche problemi di sicurezza. Ciò è dovuto al fatto che le distribuzioni locali sono diverse da quelle offerte dai provider di servizi cloud come Amazon Web Services o Microsoft Azure.

La visibilità e l'indagine sugli incidenti in un ambiente multi-cloud rappresentano una crescente sfida. Le indagini e le analisi forensi cloud diventano costose e inefficaci quando ci sono troppi dati di sicurezza da analizzare; a volte è quasi impossibile distinguere i veri avvisi di sicurezza da quelli irrilevanti. L'accumulo e l'interpretazione dei dati raccolti durante le operazioni quotidiane sul cloud prima di un incidente rivestono un ruolo fondamentale. Ciò ha un impatto diretto sulla sicurezza, in quanto tali informazioni possono essere rilevanti per indagini successive. Le organizzazioni che eseguono migrazioni sul cloud devono comprendere l'importanza dell'analisi dei dati, della visualizzazione contestuale e dell'intelligence sulle minacce per proteggere i dati sensibili e prevenire le minacce.

### CASI D'USO

- Semplificazione delle operazioni di sicurezza di rete
- Riduzione dei tempi di rilevamento delle minacce
- Rilevamento e correzione degli attacchi orientati al cloud e dell'utilizzo anomalo delle risorse cloud, delle attività di rete e degli accessi
- Verifica di conformità rapida e assistita

CloudGuard Intelligence

### CARATTERISTICHE E VANTAGGI PRINCIPALI DEL PRODOTTO

- Si integra facilmente con Amazon AWS, Microsoft Azure e Google GCP per unificare la tua soluzione nativa del cloud.
- Fornisce una visibilità semplificata dell'intero ambiente multi-cloud con il nostro strumento di esplorazione visiva unificata.
- Offre analisi avanzata e analisi forense con tecnologia ThreatCloud e apprendimento automatico.
- Consente di arricchire i registri di traffico con informazioni contestualizzate che forniscono avvisi pertinenti, isolano le minacce e minimizzano i falsi positivi.
- Grazie a CloudBots è possibile accelerare i processi di indagine sulla sicurezza, rilevare le anomalie delle attività e correggere automaticamente gli errori di configurazione.
- Si integra perfettamente con i SIEM utilizzando il connettore Firehose in formato JSON per ulteriori informazioni.

© 2021 Check Point Software Technologies Ltd. Tutti i diritti riservati.

# CloudGuard Intelligence

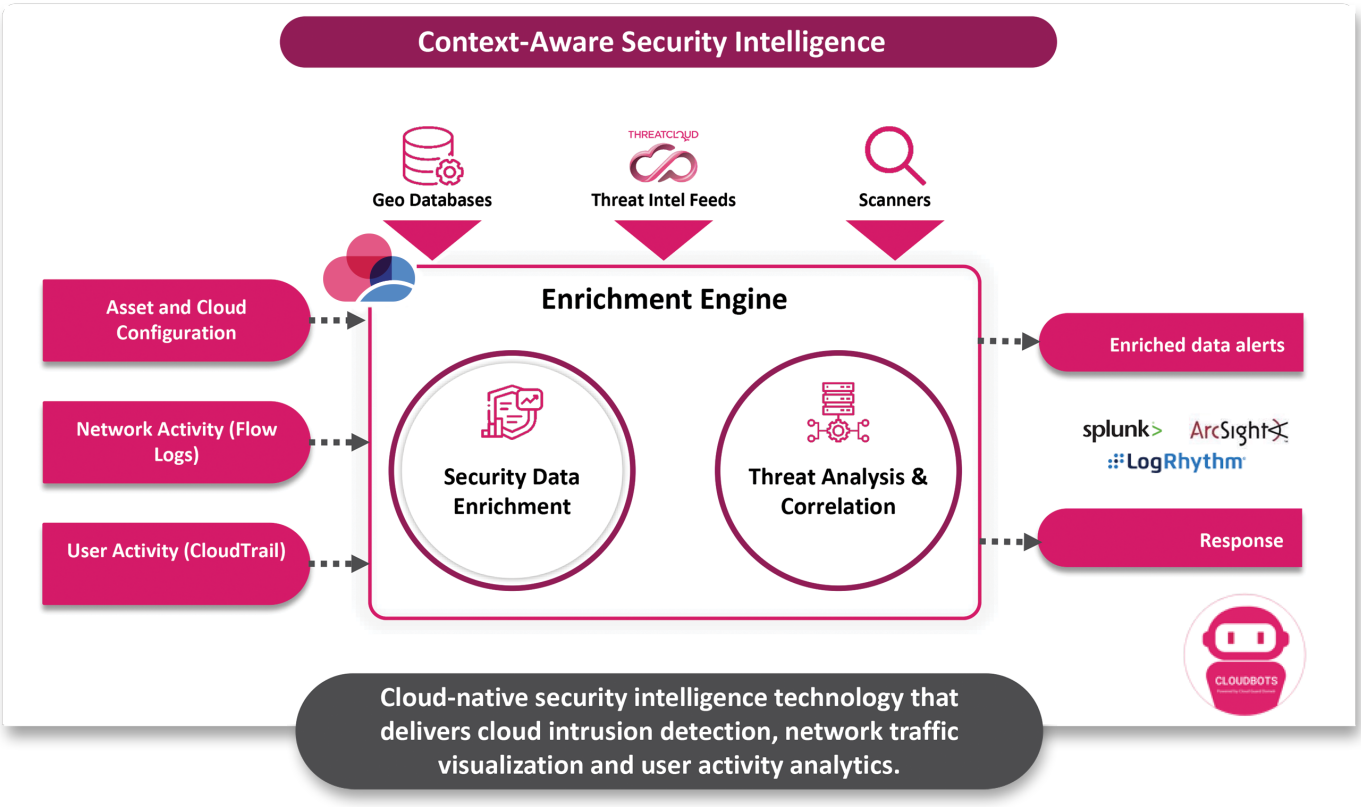
Le funzioni avanzate di intelligence sulla sicurezza cloud e ricerca delle minacce offrono una visualizzazione contestualizzata delle minacce e informazioni in tempo reale in ambienti multi-cloud per rispondere agli incidenti degli ambienti multi-cloud in modo più rapido ed efficiente.

CloudGuard Intelligence dispone di un sistema automatizzato di rilevamento delle minacce e analisi del traffico di rete (Network Traffic Analysis, NTA), che identifica e esamina le violazioni della sicurezza e le attività non autorizzate. Offre inoltre una visualizzazione contestuale e grafica del traffico di rete e delle attività degli utenti. Gli algoritmi avanzati di mappatura degli oggetti utilizzano le informazioni di configurazione e l'inventario cloud, nonché i dati di monitoraggio in tempo reale provenienti da diverse fonti su Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) e Kubernetes.

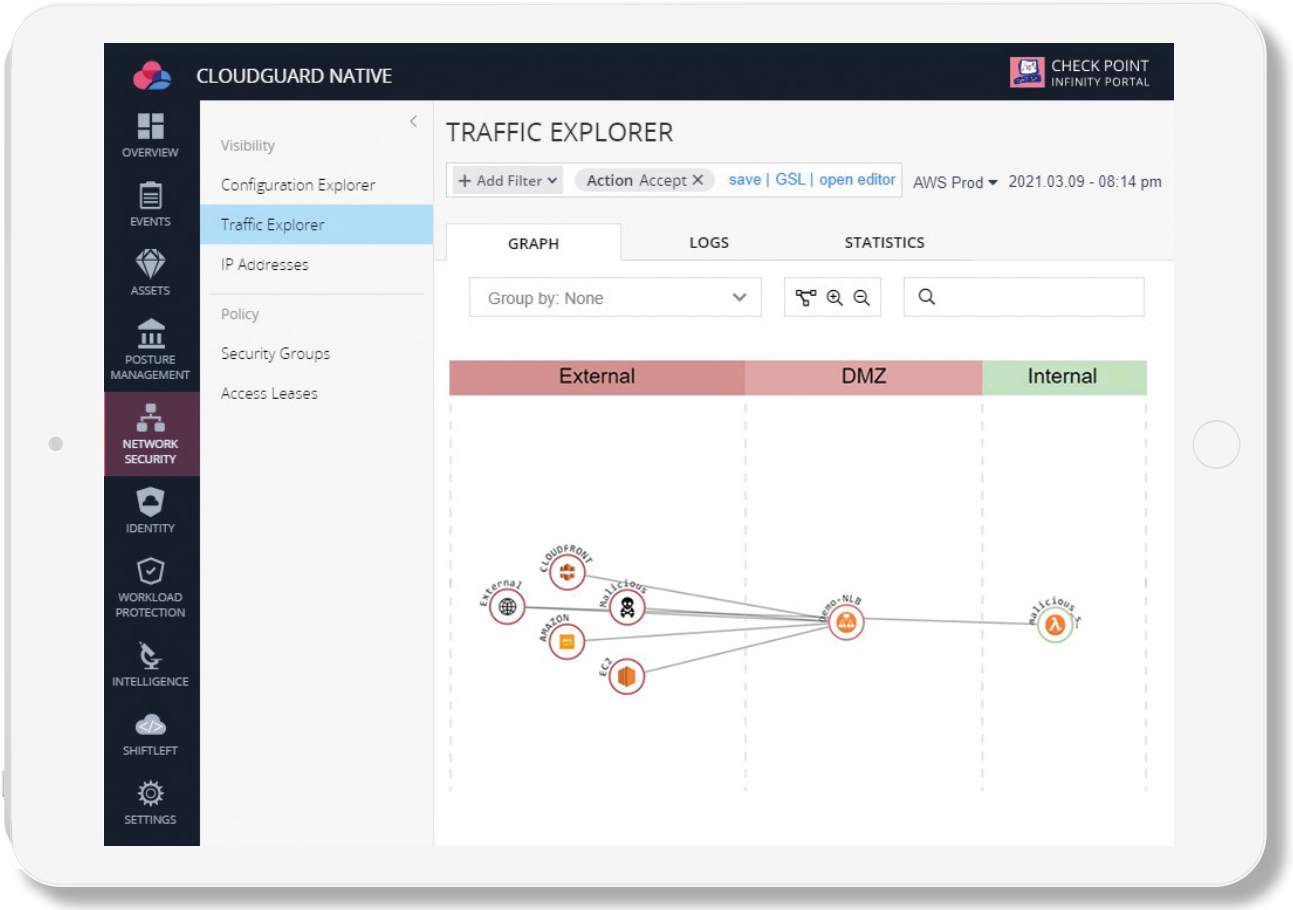
# Trasformazione dei registri in logica di sicurezza

CloudGuard analizza e arricchisce i metadati e i registri di traffico degli account cloud con il rispettivo contesto, trasformandoli in una logica di sicurezza leggibile. L'integrazione con Check Point Threat Cloud consente a CloudGuard di inviare avvisi in caso di diverse connessioni sospette, come il traffico in uscita e in entrata verso gli attori dannosi.

Il processo di arricchimento di CloudGuard fornisce funzionalità di indagine avanzate, ad esempio l'esecuzione di query su tutto il traffico per tipo di risorsa, ad esempio EC2, Lambda. Fornisce inoltre analisi avanzata di tecniche di attacco specifiche, rilevamento di anomalie di rete che avvisa in base al comportamento della risorsa e traffico anomalo, ad esempio il traffico DNS non valido.




© 2021 Check Point Software Technologies Ltd. Tutti i diritti riservati.




# Visibilità completa e accelerazione delle indagini grazie all'analisi dei big data

CloudGuard può fornire visualizzazioni quasi in tempo reale dell'attività sul cloud e ha inoltre la capacità di esaminare e analizzare le attività passate. Gli avvisi in tempo reale sono configurati per eventi o tipi di eventi specifici che si verificano nell'ambiente cloud, in modo che l'utente sia consapevole e in grado di rispondere immediatamente. Utilizzando la tecnologia di apprendimento automatico più aggiornata, CloudGuard rileva nuovi attacchi e attività sospette, come l'accesso da posizioni anomale, le modifiche alla rete delle risorse e l'utilizzo della chiave di accesso da una posizione anomala.

CloudGuard offre al cliente la possibilità di vedere ogni flusso di dati e registri di controllo negli elastici ambienti cloud odierni. Basa la sua analisi su due pilastri informativi principali: l'attività 24 ore su 24, 7 giorni su 7 dell'account (API e attività degli utenti) e le connessioni di rete dell'ambiente. CloudGuard combina l'inventario del cloud e le informazioni di configurazione con i dati di monitoraggio in tempo reale provenienti da diverse fonti, feed di intelligence sulle minacce attuali, reputazione IP e database di geolocalizzazione. Ciò si traduce in una visualizzazione migliorata che distingue il traffico sospetto da quello legittimo.  Le funzionalità di rilevamento delle intrusioni, invio di avvisi e indagine in AWS, Azure, GCP e Kubernetes fanno parte della soluzione.

© 2021 Check Point Software Technologies Ltd. Tutti i diritti riservati.

# Integrazione perfetta e arricchimento dell'intelligence di sicurezza in SIEM

Il connettore Firehose di CloudGuard Intelligence trasmette il traffico di registro arricchito in un formato JSON altamente contestualizzato a vari prodotti SIEM, come Splunk, ArcSight, LogRythm per ulteriori indagini. Come mostrato nel diagramma precedente, CloudGuard avvia l'identificazione e l'esecuzione di un'indagine completa delle minacce alla sicurezza, arricchendo i log acquisiti e trasmettendo informazioni più utili alle soluzioni SIEM.

Visita https://www.checkpoint.com/products/cloud-intelligence-threat-hunting/ per saperne di più su CloudGuard Intelligence, richiedi una demo e iscriviti per ottenere una versione di prova gratuita.

Headquarter mondiale
5 Ha'Solelim Street, Tel Aviv 67897, Israele | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | E-mail: info@checkpoint.com
Headquarter Stati Uniti
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233
www.checkpoint.com

© 2021 Check Point Software Technologies Ltd. Tutti i diritti riservati.