

Sophos Cloud Optix

Il potere dell'intelligenza artificiale e l'automazione dei processi uniscono le forze per semplificare la cloud security
Sophos Cloud Optix è una soluzione agentless e basata su SaaS che offre la combinazione ottimale tra le nostre conoscenze approfondite sulla sicurezza e il potere dell'intelligenza artificiale. Offre monitoraggio della sicurezza nel cloud, analisi e automatizzazione dei processi di conformità, tutto tramite un'interfaccia semplice da utilizzare e un sistema che garantisce la massima efficienza dei processi.

Funzionalità principali

- Una soluzione SaaS agentless, che può essere impostata in pochi minuti
- Visualizzazione completa della topologia e del flusso di traffico della rete
- Rilevamento dei comportamenti degli utenti e delle anomalie del traffico, con tecnologie di intelligenza artificiale
- Valutazione continua della conformità
- Una vasta scelta di policy di conformità subito utilizzabili
- Correlazione degli alert, per maggiore rapidità di correzione dei problemi
- Rilevamento delle modifiche alle impostazioni più critiche
- Scansione continua dei modelli Infrastructure-as-Code

See everything, secure everything

Il rilevamento automatico degli asset dell'organizzazione in ambienti Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP) garantisce al personale tecnico il potere di rispondere e risolvere i rischi di sicurezza nel giro di pochi minuti. Questo sistema è reso possibile grazie al monitoraggio continuo degli asset e della topologia completa della rete, nonché alla visualizzazione del traffico, incluso il traffico in ingresso, in uscita e interno.

Conformità proattiva in ambito cloud

Man mano che i workload vengono trasferiti sul cloud, identificare i processi di conformità (e naturalmente anche il modo per implementarli) diventa sempre più difficile. Cloud Optix riduce i costi e la complessità associati a governance, gestione dei rischi e conformità, implementando modelli subito pronti per l'uso, policy personalizzate e strumenti di collaborazione.

Un processo di conformità più rapido

Monitoraggio continuo della conformità e allineamento a standard quali CIS, GDPR, SOC2, HIPAA, ISO 27001 e PCI DSS, grazie a modelli personalizzabili, oppure preimpostati e pronti per l'uso.

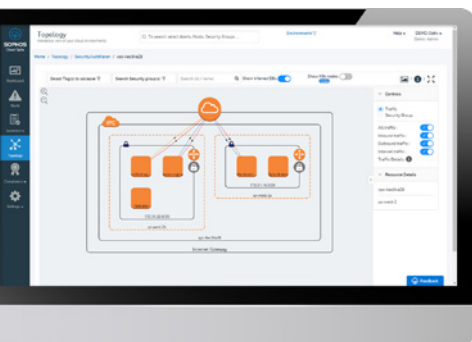
Collaborazione semplificata

Gestione e monitoraggio delle policy di conformità, per non rischiare di perdere nessuna delle operazioni essenziali, anche in caso di nuovi rilasci, grazie all'integrazione con software di terze parti e strumenti quali JIRA e ServiceNow.

Analisi e monitoraggio della sicurezza con tecnologie di IA

Cloud Optix monitora costantemente l'inventario degli asset, le configurazioni e il traffico di rete, apprendendo dalle informazioni ottenute. Gli alert basati sull'IA riducono i tempi di risposta e aiutano a intraprendere più rapidamente azioni correttive per i rischi di sicurezza, grazie alla classificazione automatica del livello di gravità degli avvisi e alle informazioni contestuali.

- Monitoraggio continuo dell'inventario degli asset (Amazon Simple Storage Service (S3), gruppi di sicurezza, chiavi di accesso per gli utenti, ecc.), delle configurazioni e dei log dei gruppi di sicurezza
- Identificazione dei pattern tipici di comportamenti anomali degli utenti, per rilevare gli attacchi avanzati e automatizzati, causati dal furto delle chiavi di accesso degli utenti, o da dipendenti con intenzioni malevole
- Previsione del potenziale andamento del traffico di rete, in base alle impostazioni di sicurezza, per evitare potenziali punti di violazione prima che vengano sferrati attacchi
- Impostazione di barriere protettive per prevenire, rilevare e correggere le modifiche accidentali o malevole alle configurazioni della rete



Una metodologia DevSecOps più intelligente

La rapidità con cui vengono effettuate le modifiche di tipo Infrastructure-as-Code, per via delle continue distribuzioni e delle pratiche DevOps, consente di rilasciare nuovi software più volte al giorno. Di conseguenza, i responsabili della sicurezza sono costretti a lavorare sotto pressione e questo potrebbe esporre i sistemi a potenziali rischi. L'architettura basata su API di Cloud Optix permette ai responsabili DevOps di integrare completamente la protezione ai processi DevOps, per una distribuzione rapida e sicura.

Rilevamento delle deviazioni e barriere protettive

Monitoraggio continuo e drift detection rispetto agli standard di configurazione, con prevenzione delle modifiche alle impostazioni critiche che potrebbero esporre l'organizzazione a rischi di sicurezza dovuti a vulnerabilità di sicurezza.

Analisi proattiva dei modelli delle infrastrutture

Analisi continua dei modelli Infrastructure-as-Code distribuiti da soluzioni quali Terraform, Github o Bitbucket. Identificazione delle configurazioni errate, che potrebbero causare il provisioning di un'infrastruttura vulnerabile.

Integrazione di strumenti SIEM e DevOps

Semplificazione delle operazioni di sicurezza, grazie all'integrazione con strumenti di sicurezza di altri vendor quali SIEM e strumenti DevOps per CI/CD.

Maggiore semplicità di gestione e distribuzione

Il servizio SaaS agentless Cloud Optix è perfettamente compatibile con gli strumenti aziendali già presenti nei sistemi.

Connettersi agli account cloud in AWS, Azure o GCP è un processo semplicissimo, grazie alle istruzioni e agli script forniti, che creano un accesso di sola lettura tramite le API native del cloud. Le connessioni possono essere impostate nel giro di pochi minuti e, una volta distribuita, Cloud Optix è subito in grado di cominciare a valutare l'ambiente cloud e offrire informazioni preziose.

La cloud security è una responsabilità condivisa

I provider di servizi di cloud pubblico offrono una flessibilità incredibile per quanto riguarda le piattaforme. Tuttavia, sebbene abbiano la responsabilità di garantire la protezione fisica a livello di datacenter e la separazione virtuale tra dati e ambienti, la responsabilità dei contenuti caricati sul cloud ricade sull'utente.

Cloud Optix offre visibilità continua, nonché rispetto della conformità e risposta alle minacce. Per informazioni sulla gamma completa di firewall next-gen e soluzioni Sophos per la protezione dei workload nel cloud pubblico, visitare: sophos.it/public-cloud.

Le funzionalità di Sophos Cloud Optix

Un unico riquadro trasparente per cloud multipli	✓
Visualizzazione della topologia	✓
Visualizzazione sovrapposta del traffico di rete	✓
Visualizzazione sovrapposta dei gruppi di sicurezza	✓
Rilevamento delle anomalie: traffico di rete	✓
Rilevamento delle anomalie: comportamento in accesso degli utenti	✓
Inventario: host, reti, archiviazione, IAM	✓
Inventario: AWS CloudTrail	✓
Inventario: serverless	✓
Valutazione continua della conformità	✓
Policy di conformità (CIS, FEDRAMP, FFIEC, GDPR, HIPAA, ISO 27001, PCI DSS 3.2, SOC2, EBU R 143)	✓
Policy benchmark CIS	✓
Policy personalizzate	✓
Avvisi e reportistica sulla conformità e sulle best practice	✓
Correzione dei problemi e barriere protettive	✓
Valutazione degli script DevSecOps	✓

Demo o prova gratuita

Tutte le funzionalità di Cloud Optix gratis per 30 giorni
sophos.it/cloud-optix.

Vendite per Regno Unito e resto del mondo:
Tel: +44 (0)8447 671131
E-mail: sales@sophos.com

Vendite per l'Italia:
Tel: [+39] 02 94 75 98 00
E-mail: sales@sophos.it

Vendite per Australia e Nuova Zelanda:
Tel: +61 2 9409 9100
E-mail: sales@sophos.com.au

Vendite per Asia:
Tel: +65 62244168
E-mail: salesasia@sophos.com