Server Workload Protection

Protezione Per Linux

Intercept X Advanced for Server, Intercept X Advanced for Server with XDR e Intercept X Advanced for Server with MTR

Cloud o data center, host e container. Metti in sicurezza la tua infrastruttura attuale e le sue evoluzioni future con la protezione Sophos: una soluzione potentissima e dall'impatto minimo sulla performance.

Abbrevia I Tempi Di Rilevamento E Risposta

Ottieni una visibilità a 360 gradi sui tuoi host e workload dei container, per identificare malware, exploit e comportamenti anomali, prima che i cybercriminali possano fare breccia nei sistemi. Extended Detection and Response (XDR) offre capacità di analisi approfondita per host, container, endpoint, traffico di rete e servizi di sicurezza nativi del cloud.

Le tecnologie di rilevamento in fase di runtime native del cloud individuano comportamenti anomali ed exploit, nonché minacce quali le uscite dai container, gli exploit del kernel e i tentativi di privilege escalation. I flussi di lavoro semplificati per le indagini sulle minacce attribuiscono massima priorità ai rilevamenti di incidenti ad alto rischio e collegano tutti gli eventi correlati per garantire maggiore efficienza e per risparmiare tempo prezioso.

Ottimizza Le Security Operations

Blocca le minacce grazie alla visibilità interattiva in fase di runtime per host e container, disponibile direttamente nella nostra console di gestione centralizzata. In alternativa puoi integrarla nei tuoi strumenti di risposta agli incidenti preferiti, grazie a un'ampia selezione di opzioni di distribuzione.

Gestione con Sophos Central: l'agent Linux a impatto minimo offre ai team di sicurezza tutte le risorse di cui hanno bisogno per svolgere le indagini e rispondere a comportamenti anomali, tentativi di exploit e minacce malware. Grazie al monitoraggio dell'host Linux, questa opzione di distribuzione consente di gestire tutte le soluzioni Sophos da un'unica area di lavoro, per passare liberamente dalle attività di threat hunting a quelle di correzione e gestione, e viceversa, con la massima semplicità.

Integrazione API: Sophos Linux Sensor è un'opzione estremamente flessibile e ottimizzata per garantire massimi livelli di performance. Il sensore Linux utilizza API per integrare negli strumenti di risposta alle minacce che già usi i rilevamenti dettagliati in fase di runtime ottenuti da ambienti host o di container. In questo modo, avrai a disposizione un più ampio spettro di dati di rilevamento, con maggiore controllo sulla creazione di set di regole personalizzate e una vasta scelta di opzioni di configurazione per ottimizzare l'uso delle risorse.

Performance Senza Attrito

La soluzione di sicurezza Intercept X for Server è ottimizzata per i flussi di lavoro delle DevSecOps, in quanto identifica anche gli attacchi più sofisticati in tempo reale, senza bisogno di moduli del kernel, orchestrazione, dati di riferimento o scansioni di sistema. Inoltre, i limiti ottimizzati per le risorse (inclusi i limiti per CPU, memoria e raccolta di dati) aiutano a prevenire il sovraccarico degli host e i problemi di stabilità, evitando così le perdite finanziarie dovute ai tempi di inattività. Questo a sua volta garantisce un'eccellente performance delle applicazioni e tempi di attività ottimali.

Caratteristiche Principali

- Protezione dei workload Linux e dei container nel cloud, on-premise e virtuali
- Riduzione dei tempi di rilevamento e risposta alle minacce
- Ottimizzazione per i workload mission-critical, per i quali la performance è determinante
- Raccolta di dati da endpoint, rete, e-mail, cloud M365 e dispositivi mobili, con Extended Detection and Response (XDR)
- Visibilità e protezione per l'intero ambiente cloud, con gestione del profilo di sicurezza del cloud inclusa
- Sicurezza 24/7 con un servizio completamente gestito

SOPHOS

Automazione Della Checklist Di Cloud Security

Progetta la struttura del tuo ambiente cloud in modo da soddisfare gli standard di best practice di settore, con elevati livelli di visibilità e potentissimi strumenti che aiutano a rispettarli e che includono sia funzionalità di gestione del profilo di sicurezza del cloud, che opzioni per gestire l'intero ambiente cloud pubblico:

- Identifica proattivamente le attività non approvate, le vulnerabilità delle immagini di host e container e gli errori di configurazione su Amazon AWS, Microsoft Azure e Google Cloud Platform (GCP)
- Individua continuamente le risorse nel cloud, con un inventario dettagliato e alti livelli di visibilità sulla protezione Sophos degli host e sulle distribuzioni di Sophos Firewall
- Applica automaticamente standard di best practice multipli per rilevare eventuali lacune del profilo di sicurezza, e per identificare rapidamente sia i problemi facilmente risolvibili che quelli di importanza critica
- Rileva le anomalie ad alto rischio nei comportamenti degli utenti con ruoli IAM, e individua rapidamente la presenza di modelli di accesso insoliti e di comportamenti dannosi, per prevenire le violazioni dei sistemi

Una Partnership Che Estende Il Tuo Team

Gli esperti analisti SOC di Sophos Managed Threat Response collaborano con il tuo team, monitorando il tuo ambiente 24/7, individuando proattivamente le minacce e avviando azioni di correzione per conto tuo. La loro specializzazione nei sistemi Linux garantisce la massima efficienza. Gli analisti di Sophos rispondono alle potenziali minacce, individuano proattivamente eventuali indicatori di compromissione e forniscono analisi dettagliate degli eventi, incluso dove, quando, come e perché si sono verificati.

Specifiche tecniche

Per informazioni aggiornate, leggi i Requisiti di sistema per Linux. Per informazioni specifiche sulla funzionalità su Windows, consulta la scheda tecnica per Windows.

Caratteristiche	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Advanced
Agent della protezione Linux (include scansione antimalware, prevenzione degli exploit, scansione dei file e molto di più)	✓	✓	✓
Sensore Linux (usa API per integrare i rilevamenti in fase di runtime provenienti da sistemi Linux e container con i tuoi strumenti di risposta alle minacce)		✓	✓
Protezione dell'infrastruttura cloud (monitora il profilo di protezione per prevenire i rischi di sicurezza e conformità)	✓	✓	✓
XDR (Extended Detection and Response)		✓	✓
MTR (Managed Threat Response: servizio di threat hunting e risposta alle minacce operativo 24/7)			✓

Effettua subito una prova gratuita

Registrati per ricevere una prova gratuita di 30 giorni su: sophos.it/server

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

22-05-24 DS-IT (MP)

SOPHOS