Protezione Per I Workload Dei Server

Protezione Windows

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

Sophos Intercept X for Server è la soluzione leader di settore che riduce la superficie di attacco e impedisce l'esecuzione delle minacce informatiche. Offre la combinazione ottimale tra tecnologie antiexploit e antiransomware, deep learning, intelligenza artificiale e opzioni di controllo, per bloccare gli attacchi prima che possano compromettere i sistemi. Intercept X for Server adotta un approccio alla protezione dei server a 360 gradi, basato sulla difesa in profondità e si differenzia dai sistemi tradizionali che si affidano a un'unica tecnica principale.

Blocco delle minacce sconosciute

L'intelligenza artificiale basata sul deep learning contenuta in Intercept X for Server primeggia nel rilevare e bloccare i malware, anche quelli mai visti prima. Agisce analizzando gli attributi dei file di centinaia di milioni di campioni per identificare le minacce senza doversi affidare alle firme.

Blocco del ransomware

Intercept X for Server include opzioni antiransomware avanzate, in grado di rilevare e bloccare i processi di cifratura dannosi utilizzati negli attacchi. I file cifrati vengono ripristinati ad uno stato sicuro, riducendo l'impatto sulla produttività aziendale.

Prevenzione degli exploit

Le tecnologie antiexploit bloccano le tecniche di exploit utilizzate dagli hacker per compromettere i dispositivi, prelevare illecitamente le credenziali e distribuire malware. Bloccando le tecniche utilizzate nel corso della catena di attacco, Intercept X for Server protegge le organizzazioni dagli attacchi fileless e dagli exploit zero-day.

Pieno controllo sui server

È possibile garantire che vengano eseguiti solamente gli elementi desiderati. Con Server Lockdown (elenco di elementi consentiti) è possibile assicurarsi che vengano eseguite su un server solo le applicazioni esplicitamente approvate. Il monitoraggio dell'integrità dei file invia notifiche se rileva tentativi non autorizzati di modificare file critici.

Visibilità sull'ambiente cloud esteso

Visibilità e protezione dell'intero inventario di asset multicloud. Consente di rilevare i workload nel cloud e i servizi cloud critici, inclusi bucket di S3, database e funzionalità indipendenti dai server per identificare attività sospette o distribuzioni non protette e per colmare eventuali lacune di sicurezza.

Caratteristiche principali

- Protezione delle distribuzioni server nel cloud, on-premise e virtuali
- Blocco di minacce mai viste prima, grazie all'intelligenza Artificiale basata sul deep learning
- Blocco dei ransomware e ripristino dei file a uno stato sicuro
- Prevenzione delle tecniche di exploit utilizzate nell'intera catena di attacco
- Threat hunting e protezione attiva delle IT operations con XDR
- Visibilità e protezione dell'ambiente cloud esteso, come ad es. bucket di S3 e database
- Sicurezza 24/7 con un servizio completamente gestito

SOPHOS

Extended Detection and Response (XDR)

Sophos XDR offre rilevamenti più accurati e riduce il carico di lavoro per le organizzazioni che svolgono attività di threat hunting e protezione attiva delle IT operations. L'utilizzo della migliore protezione disponibile nel settore come punto di partenza aiuta a ridurre la quantità di informazioni superflue, mentre l'elenco dei rilevamenti in ordine di priorità e le indagini guidate dall'intelligenza artificiale aiutano a capire da dove cominciare, per agire più rapidamente. Sono disponibili integrazioni nel data lake native per endpoint, server, firewall, e-mail, cloud, dispositivi mobili e O365; in alternativa, puoi passare facilmente al dispositivo per visualizzarne lo stato in tempo reale e per consultare fino a 90 giorni di storico dei dati.

Dati raccolti dall'intelligenza artificiale e forniti dagli esperti

Grazie alla combinazione esclusiva tra i dati raccolti dall'intelligenza artificiale e le competenze tecniche degli esperti dei SophosLabs, Intercept X for Server offre alle organizzazioni il meglio su entrambi i fronti, per un'intelligence sulle minacce che non ha rivali in questo settore.

Managed Threat Response (MTR)

Un servizio di rilevamento e risposta alle minacce basato sul threat hunting e operativo 24/7, a cura di un team di esperti Sophos. 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.

Massima semplicità di gestione

Intercept X for Server è gestito in Sophos Central, la piattaforma di gestione nel cloud per tutte le soluzioni Sophos. Offre una finestra unica per tutti i server, i dispositivi e i prodotti, semplificando l'implementazione, la configurazione e la gestione delle distribuzioni nel cloud, on-premise e virtuali.

Specifiche tecniche

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

Caratteristiche	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Advanced
Protezione essenziale (incl. controllo delle app, rilevamento basato sul comportamento e altro)	✓	✓	✓
Protezione next-gen (incl. deep learning, antiransomware, protezione contro attacchi indipendenti dai file e altro)	✓	✓	✓
Controlli per i server (incl. Server Lockdown, monitoraggio dell'integrità dei file e altro)	✓	✓	✓
CSPM (gestione del profilo di sicurezza sul cloud: visibilità e protezione dell'intero inventario di asset nel cloud)	✓	✓	✓
XDR (Extended Detection and Response)		✓	✓
Managed Threat Response (MTR: 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

22-04-07 DS-IT (PC)

SOPHOS