

# Intercept X for Server



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

Sophos Intercept X for Server protegge i server nel cloud, on-premise e virtuali dalle più recenti minacce informatiche.

Sophos Intercept X for Server protegge i server utilizzando un approccio di difesa a 360 gradi. La sua combinazione tra potenti tecniche di difesa e opzioni di visibilità garantisce alle organizzazioni la migliore protezione contro le minacce più recenti.

## **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 multcloud. È possibile 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
- ▶ Risposta alle domande critiche sulle IT operation e sul threat hunting, con EDR
- ▶ Visualizzazione e utilizzo dei dati provenienti da firewall, e-mail e altre origini, 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

*\* L'integrazione di Sophos Cloud Optix e Sophos Mobile XDR sarà presto disponibile*

**SOPHOS**

## Endpoint Detection and Response (EDR)

Progettata per gli amministratori IT e gli esperti di cybersecurity, Sophos EDR aiuta a rispondere alle domande critiche sulle IT operation e sul threat hunting. Permette, ad esempio, di identificare i server con sessioni RDP attive e di analizzare i security group nel cloud, per identificare le risorse esposte all'Internet pubblico.

## Extended Detection and Response (XDR)

Ora è possibile andare oltre i singoli server ed endpoint, raccogliendo dati da firewall, e-mail e altre origini\*. Questa funzionalità fornisce una prospettiva olistica dello stato di cybersecurity complessivo dell'organizzazione, con la possibilità di approfondire le analisi. Ad esempio, offre la possibilità di identificare i problemi di rete di un ufficio specifico e di scoprire qual è l'applicazione che li ha causati.

*\* L'integrazione di Sophos Cloud Optix e Sophos Mobile XDR sarà presto disponibile*

## 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, vedere i requisiti di sistema per [Windows](#) e [Linux](#). Per informazioni specifiche sulla funzionalità su Linux, consultare la [scheda tecnica per Linux](#).

Caratteristiche	Intercept X Advanced for Server	Intercept X Advanced for Server with EDR	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
<b>Protezione essenziale</b> (incl. controllo delle app, rilevamento basato sul comportamento e altro)	✓	✓	✓	✓	✓
<b>Protezione next-gen</b> (incl. deep learning, antiransomware, protezione contro attacchi indipendenti dai file e altro)	✓	✓	✓	✓	✓
<b>Controlli per i server</b> (incl. Server Lockdown, monitoraggio dell'integrità dei file e altro)	✓	✓	✓	✓	✓
<b>CSPM</b> (Gestione dello stato di sicurezza generale sul cloud: visibilità e protezione dell'intero inventario di asset nel cloud)	✓	✓	✓	✓	✓
<b>EDR</b> (Endpoint Detection and Response)		✓	✓	✓	✓
<b>XDR</b> (Extended Detection and Response)			✓		Vedere nota*
<b>Managed Threat Response</b> (MTR: servizio di threat hunting e risposta alle minacce operativo 24/7)				✓	✓
<b>MTR Advanced</b> (Threat hunting senza l'utilizzo di indizi, contatto dedicato e altro)					✓

\* Nota: Il team MTR potrà utilizzare i dati e le funzionalità di XDR per i clienti MTR Advanced. Dalla console di Sophos Central i clienti MTR saranno in grado di accedere solo alle funzionalità di EDR, a meno che non acquistino una licenza XDR.

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

© Copyright 2021. Sophos Ltd. Tutti i diritti riservati.  
Registrazione in Inghilterra e Galles con N° 2096520.

The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito  
Sophos è un marchio registrato da Sophos Ltd. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

Effettuate subito una prova gratuita

Registratevi per ricevere una prova gratuita di 30 giorni su: [sophos.it/server](https://sophos.it/server)