SOPHOS

# Panoramica di Intercept X for Server e Central Server Endpoint Protection

## Con gestione da Sophos Central

| | Funzionalità | Central Server Protection | Intercept X Advanced per Server | Intercept X Advanced for Server with EDR |
|---|---|---|---|---|
| RIDUZIONE DELLA SUPERFICIE DI ATTACCO | Web Security | ✓ | ✓ | ✓ |
| | Download Reputation | ✓ | ✓ | ✓ |
| | Controllo web / Blocco degli URL in base alla categoria di appartenenza | ✓ | ✓ | ✓ |
| | Controllo periferiche | ✓ | ✓ | ✓ |
| | Controllo delle applicazioni | ✓ | ✓ | ✓ |
| | Whitelisting delle applicazioni (Server Lockdown) | | ✓ | ✓ |
| PRIMA DELL'ESECUZIONE NEI DISPOSITIVI | Rilevamento antimalware con tecnologie di deep learning | | ✓ | ✓ |
| | Scansione antimalware dei file | ✓ | ✓ | ✓ |
| | Live Protection | ✓ | ✓ | ✓ |
| | Analisi del comportamento in pre-esecuzione (HIPS) | ✓ | ✓ | ✓ |
| | Blocco delle applicazioni potenzialmente indesiderate (PUA) | ✓ | ✓ | ✓ |
| | Intrusion Prevention System (IPS, in arrivo nel 2020) | ✓ | ✓ | ✓ |
| BLOCCO DELLE MINACCE IN ESECUZIONE | Data Loss Prevention (prevenzione della perdita di dati) | ✓ | ✓ | ✓ |
| | Analisi del comportamento in fase di esecuzione (HIPS) | ✓ | ✓ | ✓ |
| | Antimalware Scan Interface (AMSI) | ✓ | ✓ | ✓ |
| | Rilevamento del traffico malevolo (Malicious Traffic Detection, MTD) | ✓ | ✓ | ✓ |
| | Prevenzione degli exploit (dettagli a pag. 5) | | ✓ | ✓ |
| | Mitigazione degli antagonisti attivi (dettagli a pag. 5) | | ✓ | ✓ |
| | Protezione antiransomware per i file (CryptoGuard) | | ✓ | ✓ |
| | Protezione del disco e del record di avvio (WipeGuard) | | ✓ | ✓ |
| | Protezione contro gli attacchi man-in-the-browser (Safe Browsing) | | ✓ | ✓ |
| | Ottimizzazione del lockdown delle applicazioni | | ✓ | ✓ |
| RILEVAMENTO | Live Discover (formulazione di query SQL su ambienti diversi per il threat hunting e la protezione dell'integrità delle IT security operation) | | | ✓ |
| | Libreria di query SQL (query pre-compilate e completamente personalizzabili) | | | ✓ |
| | Rilevamento e definizione di priorità per gli eventi sospetti | | | ✓ |
| | Accesso rapido, archiviazione dei dati su disco (fino a 90 giorni) | | | ✓ |

*L'elenco delle funzionalità continua nella pagina successiva*

SOPHOS

# Panoramica di Intercept X for Server e Central Server Endpoint Protection

## Con gestione da Sophos Central

| | Funzionalità | Central Server Protection | Intercept X Advanced per Server | Intercept X Advanced for Server with EDR |
|---|---|---|---|---|
| INDAGINE | Casi di minaccia (Root Cause Analysis) | | ✓ | ✓ |
| | Analisi antimalware con Deep Learning | | | ✓ |
| | Dati di intelligence avanzata sulle minacce disponibili su richiesta, forniti direttamente dai SophosLabs | | | ✓ |
| | Esportazione dei dati attraverso analisi approfondite | | | ✓ |
| CORREZIONE | Rimozione automatizzata del malware | ✓ | ✓ | ✓ |
| | Synchronized Security Heartbeat | ✓ | ✓ | ✓ |
| | Sophos Clean | | ✓ | ✓ |
| | Accesso remoto al terminal (per indagare e intraprendere azioni da remoto) | | | ✓ |
| | Isolamento dei server su richiesta | | | ✓ |
| | Disinfezione e blocco con un solo clic | | | ✓ |
| VISIBILITÀ | Protezione dei workload nel cloud (Amazon Web Services, Microsoft Azure, Google Cloud Platform)* | ✓ | ✓ | ✓ |
| | Mappa di AWS, visualizzazione di aree geografiche multiple | ✓ | ✓ | ✓ |
| | Synchronized Application Control (visibilità sulle applicazioni) | ✓ | ✓ | ✓ |
| | Gestione dello stato di sicurezza sul cloud (monitoraggio e protezione per host cloud, funzionalità serverless, bucket S3 e altro) | | | ✓ |
| CONTROLLO | Gestione delle policy per i server | ✓ | ✓ | ✓ |
| | Cache degli aggiornamenti e relay dei messaggi | ✓ | ✓ | ✓ |
| | Esclusioni automatiche alla scansione | ✓ | ✓ | ✓ |
| | Monitoraggio dell'integrità dei file | ✓ | ✓ | ✓ |

[1]Per il cloud pubblico, consultare il seguente articolo della knowledge base: https://community.sophos.com/kb/it-it/132540

# Confronto tra sistemi operativi per le funzionalità

SOPHOS

| | FUNZIONALITÀ | WINDOWS | LINUX* |
|---|---|---|---|
| RIDUZIONE DELLA SUPERFICIE DI ATTACCO | Web Security | ✓ | |
| | Download Reputation | ✓ | |
| | Controllo web / Blocco degli URL in base alla categoria di appartenenza | ✓ | |
| | Controllo periferiche | ✓ | |
| | Controllo delle applicazioni | ✓ | |
| | Whitelisting delle applicazioni (Server Lockdown) | ✓ | |
| PRIMA DELL'ESECUZIONE NEI DISPOSITIVI | Rilevamento antimalware con tecnologie di deep learning | ✓ | |
| | Scansione antimalware dei file | ✓ | Vedere nota |
| | Live Protection | ✓ | Vedere nota |
| | Analisi del comportamento in pre-esecuzione (HIPS) | ✓ | |
| | Blocco delle applicazioni potenzialmente indesiderate (PUA) | ✓ | |
| | Intrusion Prevention System (IPS, in arrivo nel 2020) | ✓ | |
| BLOCCO DELLE MINACCE IN ESECUZIONE | Data Loss Prevention (prevenzione della perdita di dati) | ✓ | |
| | Analisi del comportamento in fase di esecuzione (HIPS) | ✓ | |
| | Antimalware Scan Interface (AMSI) | ✓ | |
| | Rilevamento del traffico malevolo (Malicious Traffic Detection, MTD) | ✓ | Vedere nota |
| | Prevenzione degli exploit (dettagli a pag. 5) | ✓ | |
| | Mitigazione degli antagonisti attivi (dettagli a pag. 5) | ✓ | |
| | Protezione antiransomware per i file (CryptoGuard) | ✓ | |
| | Protezione del disco e del record di avvio (WipeGuard) | ✓ | |
| | Protezione contro gli attacchi man-in-the-browser (Safe Browsing) | ✓ | |
| | Ottimizzazione del lockdown delle applicazioni | ✓ | |
| RILEVAMENTO | Live Discover (formulazione di query SQL su ambienti diversi per il threat hunting e la protezione dell'integrità delle IT security operation) | ✓ | ✓ |
| | Libreria di query SQL (query pre-compilate e completamente personalizzabili) | ✓ | ✓ |
| | Rilevamento e definizione di priorità per gli eventi sospetti | ✓ | |
| | Accesso rapido, archiviazione dei dati su disco (fino a 90 giorni) | ✓ | ✓ |

*L'elenco delle funzionalità continua nella pagina successiva*

# Confronto tra sistemi operativi per le funzionalità

SOPHOS

| | FUNZIONALITÀ | WINDOWS | LINUX* |
|---|---|---|---|
| INDAGINE | Casi di minaccia (Root Cause Analysis) | ✓ | |
| | Analisi antimalware con Deep Learning | ✓ | |
| | Dati di intelligence avanzata sulle minacce disponibili su richiesta, forniti direttamente dai SophosLabs | ✓ | |
| | Esportazione dei dati attraverso analisi approfondite | ✓ | |
| CORREZIONE | Rimozione automatizzata del malware | ✓ | |
| | Synchronized Security Heartbeat | ✓ | Vedere nota |
| | Sophos Clean | ✓ | |
| | Live Response (accesso remoto al terminal a scopo di ulteriore indagine e risposta) | ✓ | ✓ |
| | Isolamento dei server su richiesta | ✓ | |
| | Disinfezione e blocco con un solo clic | ✓ | |
| VISIBILITÀ | Protezione dei workload nel cloud (Amazon Web Services, Microsoft Azure, Google Cloud Platform) | ✓ | |
| | Mappa di AWS, visualizzazione di aree geografiche multiple | ✓ | |
| | Synchronized Application Control (visibilità sulle applicazioni) | ✓ | |
| | Gestione dello stato di sicurezza sul cloud (monitoraggio e protezione per host cloud, funzionalità serverless, bucket S3 e altro) | ✓ | ✓ |
| CONTROLLO | Gestione delle policy per i server | ✓ | |
| | Cache degli aggiornamenti e relay dei messaggi | ✓ | |
| | Esclusioni automatiche alla scansione | ✓ | |
| | Monitoraggio dell'integrità dei file | ✓ | |

*Linux include due opzioni di distribuzione. 1) La distribuzione Intercept X Advanced for Server with EDR offre accesso alle funzionalità elencate nella tabella. 2) Distribuzione Sophos Anti-Virus for Linux, che include: antimalware, Live Protection, Malicious Traffic Detection (rilevamento del traffico malevolo) e Synchronized Security. Si prega di notare che i due tipi di distribuzione non possono essere utilizzati contemporaneamente.

# Funzionalità di Sophos Intercept X

SOPHOS

I dettagli delle funzionalità incluse in Intercept X

| | Funzionalità | |
|---|---|---|
| PREVENZIONE DEGLI EXPLOIT | Implementazione della Data Execution Prevention (DEP) | ✓ |
| | Uso obbligatorio di ASLR (Address Space Layout Randomization) | ✓ |
| | ASLR bottom-up | ✓ |
| | Null Page (protezione contro Null Dereference) | ✓ |
| | Heap Spray Allocation | ✓ |
| | Dynamic Heap Spray | ✓ |
| | Stack Pivot | ✓ |
| | Stack Exec (MemProt) | ✓ |
| | Misure di mitigazione ROP basate su stack (chiamante) | ✓ |
| | Misure di mitigazione ROP branch-based (assistite da hardware) | ✓ |
| | Protezione strutturata contro la sovrascrittura del gestore eccezioni (Structured Exception Handler Overwrite Protection, SEHOP) | ✓ |
| | Filtraggio importazione della tabella indirizzi (Import Address Table Filtering, IAF) | ✓ |
| | Load Library | ✓ |
| | Reflective DLL Injection | ✓ |
| | Shellcode | ✓ |
| | VBScript God Mode | ✓ |
| | WoW64 | ✓ |
| | Syscall | ✓ |
| | Hollow Process | ✓ |
| | DLL Hijacking | ✓ |
| | Squiblydoo Applocker Bypass | ✓ |
| | Protezione contro le APC (Double Pulsar / AtomBombing) | ✓ |
| | Privilege escalation dei processi | ✓ |
| | Protezione dinamica dello shellcode | ✓ |
| | EFS Guard | ✓ |
| | CTF Guard | ✓ |
| | ApiSetGuard | ✓ |

| | Funzionalità | |
|---|---|---|
| ANTIRANSOMWARE | Protezione antiransomware per i file (CryptoGuard) | ✓ |
| | Recupero automatico dei file (CryptoGuard) | ✓ |
| | Protezione del disco e del record di avvio (WipeGuard) | ✓ |
| LOCKDOWN DELLE APPLICAZIONI | Browser web (incluso HTA) | ✓ |
| | Plugin dei browser web | ✓ |
| | Java | ✓ |
| | Applicazioni multimediali | ✓ |
| | Applicazioni Office | ✓ |
| PROTEZIONE CON DEEP LEARNING | Rilevamento antimalware con tecnologie di deep learning | ✓ |
| | Blocco delle applicazioni potenzialmente indesiderate (PUA) con deep learning | ✓ |
| | Eliminazione dei falsi positivi | ✓ |
| RISPOSTA INVESTIGAZIONE RIMOZIONE | Casi di minaccia (Root Cause Analysis) | ✓ |
| | Sophos Clean | ✓ |
| | Synchronized Security Heartbeat | ✓ |
| BLOCCO DEGLI ATTACCHI DEI CYBERCRIMINALI | Protezione contro il furto di credenziali | ✓ |
| | Mitigazione di code cave | ✓ |
| | Protezione contro gli attacchi man-in-the-browser (Safe Browsing) | ✓ |
| | Malicious Traffic Detection (Rilevamento del traffico malevolo) | ✓ |
| | Rilevamento shell Meterpreter | ✓ |

# Managed Threat Response (MTR)

Sophos Managed Threat Response (MTR) offre un servizio completamente gestito con opzioni di ricerca, rilevamento e risposta alle minacce, disponibile 24h su 24 e 7gg su 7 e gestito direttamente dal nostro team di esperti. Per i clienti MTR è inclusa anche Intercept X Advanced with EDR.

## Sophos MTR: Standard

### Threat hunting con l'utilizzo di indizi, operativo 24h su 24/7gg su 7

Elementi o attività identificate come dannosi (indicatori importanti) vengono automaticamente bloccati o terminati, facendo risparmiare tempo prezioso ai threat hunter, che possono ora dedicarsi all'individuazione delle minacce seguendo gli indizi raccolti. Questo tipo di intercettazione delle minacce prevede l'aggregazione di eventi causali e adiacenti (indicatori minori), per rilevare nuovi indicatori di attacco (IoA) e indicatori di compromissione (IoC), che precedentemente erano impossibili da rilevare.

### Controllo dello stato di integrità della sicurezza

Ottimizzazione della performance di Intercept X, a partire da Intercept X Advanced with EDR, grazie alle analisi proattive delle condizioni operative e ai consigli sull'ottimizzazione della configurazione.

### Report sulle attività

I riepiloghi delle attività dei casi consentono al personale di comunicare e di attribuire la giusta priorità agli eventi, per cui il vostro team saprà esattamente quali sono le minacce individuate e quali azioni di risposta sono state intraprese in ogni periodo di reporting.

### Rilevamento degli active adversary

La maggior parte degli attacchi di successo si basano sull'esecuzione di un processo che, agli strumenti di monitoraggio, può sembrare legittimo. Grazie all'utilizzo di tecniche di indagine sviluppate internamente, il nostro team determina la differenza tra i comportamenti legittimi e le tattiche, tecniche e procedure (TTP) utilizzate dagli autori degli attacchi.

## Sophos MTR: Advanced *Include tutte le funzionalità del servizio Standard, con in più:*

### Threat hunting senza l'utilizzo di indizi, operativa 24h su 24

Utilizzando data science, dati di intelligence sulle minacce e il fenomenale intuito di espertissimi threat hunter, raccogliamo e confrontiamo tutte le informazioni relative al profilo della vostra azienda, alle risorse principali e agli utenti ad alto rischio, per anticipare i comportamenti degli autori degli attacchi e intercettare nuovi indicatori di attacco (Indicators of Attack, IoA).

### Telemetria ottimizzata

Le indagini sulle minacce vengono arricchite dai dati di telemetria provenienti dagli altri prodotti Sophos Central, che vanno oltre la semplice analisi degli endpoint per fornire un quadro completo delle attività degli antagonisti.

### Miglioramento proattivo della condizione generale del sistema

Miglioramento proattivo della condizione di sicurezza generale del sistema con potenziamento della protezione, grazie a indicazioni prescrittive volte a risolvere le vulnerabilità nelle configurazioni e nelle architetture, che possono diminuire le capacità complessive di sicurezza.

### Contatto dedicato per la risposta alle minacce

All'identificazione di un incidente, viene fornito un contatto dedicato per la risposta alle minacce, che collaborerà direttamente con le vostre risorse on-premise (un team interno o un partner esterno), fino alla neutralizzazione completa della minaccia.

### Supporto diretto e dedicato

Il vostro team può usufruire di accesso diretto e dedicato ai nostri Security Operations Center (SOC). Il nostro MTR Operations Team è disponibile 24h su 24 e può contare sull'assistenza di team di supporto situati in 26 località in tutto il mondo.

### Individuazione delle risorse

Da informazioni sulle risorse che includono versioni del sistema operativo, applicazioni e vulnerabilità, fino all'identificazione delle risorse gestite e di quelle non gestite, offriamo importanti analisi approfondite, che sono disponibili per valutare l'impatto di un incidente, per svolgere azioni di threat hunting e per fornire consigli su come migliorare proattivamente lo stato generale del sistema.