SOPHOS

# Intercept X

## La migliore protezione endpoint in assoluto

Sophos Intercept X blocca la più vasta gamma di attacchi, grazie alla sua esclusiva combinazione di rilevamento antimalware con Deep Learning, exploit prevention, antiransomware e molto altro ancora.

## Caratteristiche principali

- Il numero 1 tra i motori di rilevamento antimalware, basato sulla tecnologia deep learning
- Prevenzione degli exploit, per bloccare le tecniche utilizzate dai cybercriminali per assumere il controllo dei software vulnerabili
- La mitigazione degli active adversary previene la persistenza sui computer
- La Root cause analysis consente di visualizzare le azioni effettuate dal malware e individuarne la provenienza
- Tecnologie di prevenzione appositamente progettate per individuare il ransomware
- Endpoint Detection and Response (EDR) per garantire l'integrità delle IT security operation e opzioni di threat hunting per amministratori IT e analisti di sicurezza

Sophos Intercept X adotta un approccio di difesa in profondità alla protezione endpoint; si differenzia dai sistemi tradizionali, che si basano su un'unica tecnica principale. È la combinazione tra tecniche tradizionali e tecniche moderne, sviluppata da un vendor leader di mercato.

Le tecniche moderne includono il rilevamento antimalware con Deep Learning, la prevenzione degli exploit e funzionalità dedicate all'individuazione del ransomware. Tra le tecniche tradizionali ci sono: rilevamento antimalware basato sulle firme, analisi del comportamento, rilevamento del traffico malevolo, controllo dei dispositivi, controllo delle applicazioni, web filtering, prevenzione contro la perdita dei dati e molto altro ancora.

## Rilevamento antimalware con tecnologie di deep learning

L'intelligenza artificiale integrata in Intercept X è una rete neurale di Deep Learning, ovvero una forma avanzata di Machine Learning in grado di rilevare sia malware noto che sconosciuto, senza utilizzare le firme.

Grazie alla tecnologia Deep Learning, Intercept X vanta il migliore motore di rilevamento antimalware disponibile sul mercato, come dimostrano i test condotti da organismi di valutazione indipendenti. Queste caratteristiche consentono a Intercept X di rilevare il malware che sfugge agli altri strumenti di sicurezza endpoint.

## Bloccare gli exploit per bloccare l'attacco

Le vulnerabilità dei software emergono a una velocità allarmante e i vendor devono rilasciare patch continuamente. D'altro canto, è molto più raro che vengano create nuove tecniche di exploit: i cybercriminali finiscono per continuare a usare sempre le stesse tecniche per ciascuna vulnerabilità scoperta. La prevenzione degli exploit blocca gli strumenti e le tecniche di exploit utilizzati per diffondere malware, prelevare illecitamente le credenziali ed eludere il rilevamento. Queste tecnologie consentono a Sophos di proteggere la rete, bloccando gli hacker e sventando gli attacchi zero-day più elusivi.

## Protezione antiransomware dall'efficacia comprovata

Intercept X sfrutta l'analisi basata sul comportamento per bloccare ransomware e attacchi al boot record mai osservati prima. Questa caratteristica la rende la più avanzata tecnologia antiransomware attualmente disponibile. Anche se dovessero essere file o processi attendibili a venire compromessi o utilizzati in maniera impropria, CryptoGuard bloccherà e ne ripristinerà il corretto funzionamento senza alcuna interazione da parte degli utenti o del personale di supporto IT. CryptoGuard agisce in maniera silenziosa a livello di file system, tenendo traccia dei computer remoti e dei processi locali che cercano di modificare documenti e altri file.

## Endpoint Detection and Response (EDR)

Sophos Intercept X Advanced è la prima soluzione EDR progettata per amministratori IT e analisti di sicurezza. Aiuta a risolvere i problemi relativi alla gestione operativa dei sistemi informatici e ai casi di utilizzo del threat hunting. Consente di rispondere a domande su eventi endpoint passati e attuali. Permette di individuare proattivamente gli active adversary, o di utilizzare la gestione operativa dei sistemi informatici per garantire l'integrità del sistema di IT security. Quando viene identificato un problema in remoto, aiuta a implementare un'azione di risposta precisa e accurata.

## Maggiore semplicità di gestione e distribuzione

Gestire la sicurezza da Sophos Central significa non dover più installare o distribuire server per poter proteggere gli endpoint. Sophos Central offre policy predefinite e configurazioni consigliate, per garantire la massima protezione sin dal primo istante.

| | 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 | ✓ |
| 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)

Threat hunting, rilevamento e risposta alle minacce 24h su 24 e 7gg su 7 come servizio completamente gestito, a cura di un team di esperti Sophos. Sfruttando l'efficacia del sistema intelligente di EDR di Intercept X Advanced with EDR, gli analisti di Sophos rispondono tempestivamente alle potenziali minacce, cercando indicatori di compromissione e fornendo un'analisi dettagliata degli eventi che indica il cosa, dove, quando, come e perché dell'accaduto.

## Specifiche tecniche

Sophos Intercept X supporta Windows 7 e versioni successive, a 32 e a 64 bit. In alternativa, può essere utilizzata con altri prodotti endpoint e antivirus, per aggiungere funzionalità di rilevamento antimalware con Deep Learning, antiexploit, antiransomware, Root Cause Analysis e Sophos Clean.

| | 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 | ✓ |
| DEEP LEARNING | Rilevamento antimalware con tecnologie di deep learning | ✓ |
| | Blocco delle applicazioni potenzialmente indesiderate (PUA) con deep learning | ✓ |
| | Eliminazione dei falsi positivi | ✓ |
| | Live Protection | ✓ |
| RISPOSTA INVESTIGAZIONE RIMOZIONE | Root Cause Analysis | ✓ |
| | Sophos Clean | ✓ |
| | Synchronized Security Heartbeat | ✓ |
| DELIVERY | Esecuzione possibile come agente standalone | ✓ |
| | Esecuzione possibile insieme ad antivirus già esistente | ✓ |
| | Esecuzione possibile come componente di un agente Sophos Endpoint già esistente | ✓ |
| | Windows 7 | ✓ |
| | Windows 8 | ✓ |
| | Windows 8.1 | ✓ |
| | Windows 10 | ✓ |
| | macOS* | ✓ |

* Le funzionalità supportate includono CryptoGuard, Malicious Traffic Detection, Synchronized Security Heartbeat, Root Cause Analysis

## Effettuate subito una prova gratuita

Registratevi per una prova gratuita di 30 giorni su: sophos.it/intercept-x.

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



11/05/2020 DS (PS)

SOPHOS