Guida Alle Licenze Sophos Workload Protection

SOPHOS
Cybersecurity delivered.

Panoramica di Intercept X for Server, XDR, Cloud Native Security e MTR

Con gestione da Sophos Central

Funzionalità	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Sicurezza Nativa Del Cloud	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Gestione						
Criteri multipli		✓	✓	✓	✓	✓
Aggiornamenti controllati		✓	✓	✓	✓	✓
Riduzione della superficie di attacco						
Controllo delle applicazioni		✓	✓	✓	✓	✓
Controllo delle periferiche		✓	✓	✓	✓	✓
Controllo web / Blocco degli URL in base alla categoria di appartenenza		✓	✓	✓	✓	✓
Whitelisting delle applicazioni (Server Lockdown)		✓	✓	✓	✓	✓
Download Reputation	✓	✓	✓	✓	✓	✓
Web Security	✓	✓	✓	✓	✓	✓
Prima dell'esecuzione sul dispositivo						
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)	✓	✓	✓	✓	✓	✓
Blocco delle minacce in esecuzione						
Data Loss Prevention (prevenzione della perdita di dati)		✓	✓	✓	✓	✓

Funzionalità	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Sicurezza Nativa Del Cloud	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
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)			✓	✓	✓	✓
Accesso rapido, archiviazione dei dati su disco (fino a 90 giorni)			✓	✓	✓	✓
Origini dati che coinvolgono prodotti multipli, ad es. Firewall, Email			✓	✓	✓	✓
Elenco dei rilevamenti in ordine di priorità			✓	✓	✓	✓
Sophos Data Lake (archiviazione dati nel cloud)			30 giorni	30 giorni	30 giorni	30 giorni
Query pianificate			✓	✓	✓	✓
Visibilità e rilevamenti dei runtime dei container			✓	✓	✓	✓
Indagine						
Casi di minacce (Root Cause Analysis)		✓	✓	✓	✓	✓
Analisi antimalware con Deep Learning			✓	✓	✓	✓

Funzionalità	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Sicurezza Nativa Del Cloud	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Dati di intelligence avanzata sulle minacce disponibili su richiesta, forniti direttamente dai SophosLabs			✓	✓	✓	✓
Esportazione dei dati attraverso analisi approfondite			✓	✓	✓	✓
Indagini guidate dall'intelligenza artificiale			✓	✓	✓	✓
Correzione						
Rimozione automatizzata del malware	✓	✓	✓	✓	✓	✓
Synchronized Security Heartbeat	✓	✓	✓	✓	✓	✓
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 e rilevamenti dei runtime dei container			✓	✓	✓	✓
Applicazioni						
Synchronized Application Control (visibilità sulle applicazioni)	✓	✓	✓	✓	✓	✓
Cache degli aggiornamenti e relay dei messaggi	✓	✓	✓	✓	✓	✓
Esclusioni automatiche alla scansione	✓	✓	✓	✓	✓	✓
Monitoraggio dell'integrità dei file			✓	✓	✓	✓
Ambienti cloud						
Monitoraggio degli ambienti cloud: AWS, Azure, GCP, Kubernetes, IaC e registri Docker Hub		Una per provider	Una per provider	Illimitate	Una per provider	Una per provider
Monitoraggio della sicurezza (Regole di best practice per la gestione del profilo di sicurezza sul cloud, CSPM)		Scansioni quotidiane	Scansioni quotidiane	Scansioni quotidiane pianificate e scansioni su richiesta	Scansioni quotidiane	Scansioni quotidiane
Inventario delle risorse		✓	✓	✓	✓	✓
Opzioni di ricerca avanzata		✓	✓	✓	✓	✓
Rilevamento delle anomalie basato sull'intelligenza artificiale		✓	✓	✓	✓	✓
Avvisi dei SophosLabs per il traffico dannoso rilevato da Intelix		✓	✓	✓	✓	✓
Avvisi e-mail		✓	✓	✓	✓	✓

Funzionalità	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Sicurezza Nativa Del Cloud	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Integrazioni dei servizi nativi di AWS (Amazon GuardDuty, AWS Security Hub, Amazon Inspector ecc.)		✓	✓	✓	✓	✓
Integrazioni dei servizi nativi di Azure (Azure Sentinel e Advisor)		✓	✓	✓	✓	✓
Protezione dei workload del cloud: rilevamento dell'agent Sophos Intercept X Server		✓	✓	✓	✓	✓
Protezione dei workload del cloud: rimozione automatica dell'agent Sophos Intercept X Server		✓	✓	✓	✓	✓
Criteri e reportistica sulla conformità		CIS Benchmarks	CIS Benchmarks	CIS Benchmarks, ISO 27001, EBU R 143, FEDRAMP FIEC, GDPR, HIPAA, PCI DSS, SOC2, best practice di Sophos	CIS Benchmarks	CIS Benchmarks
Criteri personalizzati:				✓		
Visualizzazione della rete		✓	✓	✓	✓	✓
Visualizzazione IAM		✓	✓	✓	✓	✓
Monitoraggio della spesa		✓	✓	✓	✓	✓
Integrazioni per la gestione degli avvisi (Jira, ServiceNow, Slack, Teams, PagerDuty, Amazon SNS)		✓	✓	✓	✓	✓
Integrazioni per SIEM (Splunk, Azure Sentinel)		✓	✓	✓	✓	✓
Rest API		✓	✓	✓	✓	✓
Scansione dei modelli Infrastructure as Code		✓	✓	✓	✓	✓
Controllo degli accessi all'ambiente		✓	✓	✓	✓	✓
Scansione delle immagini dei container (ECR, ACR, Docker Hub, API)		✓	✓	✓	✓	✓
Servizio gestito						
Threat hunting con indizi 24h su 24					✓	✓
Controlli dello stato di integrità della sicurezza					✓	✓
Conservazione dei dati					✓	✓
Report sulle attività					✓	✓
Rilevamento degli active adversary					✓	✓
Neutralizzazione delle minacce e azioni correttive					✓	✓
Threat hunting senza indizi 24h su 24						✓
Contatto dedicato nel team Threat Response						✓
Supporto diretto e dedicato						✓
Gestione proattiva del profilo di sicurezza						✓
Protezione antiransomware per i file (CryptoGuard)						✓

Confronto tra sistemi operativi per le funzionalità

Funzionalità	Windows	Linux*
Gestione		
Criteri multipli	✓	✓
Aggiornamenti controllati	✓	✓
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 sul dispositivo		
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)	✓	
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	✓	

Funzionalità	Windows	Linux*
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)	✓	✓
Accesso rapido, archiviazione dei dati su disco (fino a 90 giorni)	✓	✓
Origini dati che coinvolgono prodotti multipli, ad es. Firewall, Email	✓	✓
Elenco dei rilevamenti in ordine di priorità	✓	✓
Sophos Data Lake (archiviazione dati nel cloud)	✓	✓
Query pianificate	✓	✓
Visibilità e rilevamenti dei runtime dei container		✓
Indagine		
Casi di minacce (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	✓	
Indagini guidate dall'intelligenza artificiale	✓	✓
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	✓	
Applicazioni		
Synchronized Application Control (visibilità sulle applicazioni)	✓	
Cache degli aggiornamenti e relay dei messaggi	✓	
Esclusioni automatiche alla scansione	✓	

Funzionalità	Windows	Linux*
Monitoraggio dell'integrità dei file	✓	
Servizio gestito		
Threat hunting con indizi 24h su 24	✓	✓
Controlli dello stato di integrità della sicurezza	✓	✓
Conservazione dei dati	✓	✓
Report sulle attività	✓	✓
Rilevamento degli active adversary	✓	✓
Neutralizzazione delle minacce e azioni correttive	✓	✓
Threat hunting senza indizi 24h su 24	✓	✓
Contatto dedicato nel team Threat Response	✓	✓
Supporto diretto e dedicato	✓	✓
Miglioramento proattivo del profilo di sicurezza	✓	✓

*Linux include due opzioni di distribuzione. 1) La distribuzione Sophos Protection for Linux 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.

Panoramica Della Protezione Sophos

Dettagli sulle funzionalità di protezione dei workload incluse in Intercept X e Cloud Native Security

Caratteristiche	
Exploit Prevention	
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	✓

Caratteristiche	
EFS Guard	✓
CTF Guard	✓
ApiSetGuard	✓
Mitigazione del comportamento 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	✓
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 (incluse le 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 Indagine Rimozione	
Casi di minacce (Root Cause Analysis)	✓
Sophos Clean	✓
Synchronized Security Heartbeat	✓

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 for Server with XDR.

Sophos MTR: Standard

Threat hunting con indizi 24/7
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.

Security Health Check
Ottimizzazione per garantire massimi livelli di performance nei prodotti della linea Sophos Central, a partire da Intercept X Advanced for Server with XDR, grazie alle analisi proattive delle condizioni operative e ai consigli sull'ottimizzazione della configurazione.

Report sulle attività
I riepiloghi delle attività dei casi rilevati 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 ciascun periodo del report.

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: Funzionalità avanzate

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.

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

22-07-25 IT (DD)

SOPHOS