Sophos Workload Protection Lizenz-Guide

SOPHOS
Cybersecurity delivered.

Übersicht über Intercept X for Server, XDR, Cloud Native Security und MTR

Verwaltung über Sophos Central

Funktionen	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud-native Sicherheit	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Verwaltung						
Mehrere Richtlinien		✓	✓	✓	✓	✓
Gesteuerte Updates		✓	✓	✓	✓	✓
Reduzierung der Angriffsfläche						
Application Control		✓	✓	✓	✓	✓
Peripheral Control		✓	✓	✓	✓	✓
Web Control/Kategoriebasierte URL-Blockierung		✓	✓	✓	✓	✓
Application Whitelisting (Server Lockdown)		✓	✓	✓	✓	✓
Download Reputation	✓	✓	✓	✓	✓	✓
Web Security	✓	✓	✓	✓	✓	✓
Vor Ausführung auf einem Gerät						
Deep-Learning-Malware-Erkennung	✓	✓	✓	✓	✓	✓
Anti-Malware-Dateiscans	✓	✓	✓	✓	✓	✓
Live Protection	✓	✓	✓	✓	✓	✓
Verhaltensanalysen vor Ausführung (HIPS)	✓	✓	✓	✓	✓	✓
Blockierung pot. unerwünschter Anwendungen (PUAs)	✓	✓	✓	✓	✓	✓
Intrusion Prevention System (IPS)	✓	✓	✓	✓	✓	✓
Stoppen von Bedrohungen bei Ausführung						
Data Loss Prevention		✓	✓	✓	✓	✓
Laufzeit-Verhaltensanalyse (HIPS)	✓	✓	✓	✓	✓	✓
Antimalware Scan Interface (AMSI)	✓	✓	✓	✓	✓	✓

Funktionen	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud-native Sicherheit	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Malicious Traffic Detection (MTD)	✓	✓	✓	✓	✓	✓
Exploit Prevention (Details auf Seite 5)	✓	✓	✓	✓	✓	✓
Active Adversary Mitigations (Details auf Seite 5)	✓	✓	✓	✓	✓	✓
Ransomware File Protection (CryptoGuard)	✓	✓	✓	✓	✓	✓
Disk and Boot Record Protection (WipeGuard)	✓	✓	✓	✓	✓	✓
Man-in-the-Browser Protection (Safe Browsing)	✓	✓	✓	✓	✓	✓
Enhanced Application Lockdown	✓	✓	✓	✓	✓	✓
Erkennung						
Live Discover (umgebungsübergreifende SQL-Abfragen zum Threat Hunting und zur Einhaltung von Sicherheitsvorgaben)			✓	✓	✓	✓
SQL-Abfragen-Library (vorformulierte, individuell anpassbare Abfragen)			✓	✓	✓	✓
Datenspeicherung auf Festplatte (bis zu 90 Tage) mit schnellem Datenzugriff			✓	✓	✓	✓
Produktübergreifende Datenquellen (z. B. Firewall, E-Mail)			✓	✓	✓	✓
Liste mit nach Priorität geordneten Erkennungen			✓	✓	✓	✓
Sophos Data Lake (Cloud-Datenspeicher)			30 Tage	30 Tage	30 Tage	30 Tage
Geplante Abfragen			✓	✓	✓	✓
Laufzeitbasierte Container-Transparenz und -Erkennungen			✓	✓	✓	✓
Analyse						
Bedrohungsfälle (Ursachenanalyse)		✓	✓	✓	✓	✓
Deep Learning-Malware-Analyse			✓	✓	✓	✓
Erweiterte Bedrohungsdaten aus den SophosLabs auf Abruf			✓	✓	✓	✓
Export forensischer Daten			✓	✓	✓	✓
KI-gesteuerte Analysen			✓	✓	✓	✓

Funktionen	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud-native Sicherheit	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Bereinigung						
Automatisierte Malware-Entfernung	✓	✓	✓	✓	✓	✓
Synchronized Security Heartbeat	✓	✓	✓	✓	✓	✓
Sophos Clean	✓	✓	✓	✓	✓	✓
Live Response (Remote-Terminal-Zugriff für weitere Analysen und Reaktionsmaßnahmen)			✓	✓	✓	✓
On-Demand-Server-Isolation			✓	✓	✓	✓
Mit einem Klick „Entfernen und blockieren“			✓	✓	✓	✓
Laufzeitbasierte Container-Transparenz und -Erkennungen			✓	✓	✓	✓
Zugriff/Berechtigung						
Synchronized Application Control (Transparenz über Anwendungen)	✓	✓	✓	✓	✓	✓
Update Cache und Message Relay	✓	✓	✓	✓	✓	✓
Automatische Scan-Ausnahmen	✓	✓	✓	✓	✓	✓
File Integrity Monitoring			✓	✓	✓	✓
Cloud-Umgebungen						
Überwachung von Cloud-Umgebungen: AWS, Azure, GCP, Kubernetes, IaC und Docker Hub Registries		1 je Anbieter	1 je Anbieter	Unbegrenzt	1 je Anbieter	1 je Anbieter
Security Monitoring (CSPM-Best-Practice-Richtlinien)		Tägliche Scans	Tägliche Scans	Geplante, tägliche und On-Demand-Scans	Tägliche Scans	Tägliche Scans
Asset Inventory		✓	✓	✓	✓	✓
Erweiterte Suchfunktionen		✓	✓	✓	✓	✓
KI-basierte Erkennung von Anomalien		✓	✓	✓	✓	✓
Warnmeldungen zu schädlichem Datenverkehr von SophosLabs Intelix		✓	✓	✓	✓	✓
E-Mail-Warnhinweise		✓	✓	✓	✓	✓
AWS-native Service-Integrationen (Amazon GuardDuty, AWS Security Hub, Amazon Inspector usw.)		✓	✓	✓	✓	✓
Azure-native Service-Integrationen (Azure Sentinel und Advisor)		✓	✓	✓	✓	✓
Cloud Workload Protection: Agent-Erkennung (Sophos Intercept X Server)		✓	✓	✓	✓	✓
Cloud Workload Protection: Automatische Agent-Entfernung (Sophos Intercept X Server)		✓	✓	✓	✓	✓

Funktionen	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud-native Sicherheit	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Compliance-Richtlinien und Reporting		CIS-Bewertungsrichtlinien	CIS-Bewertungsrichtlinien	CIS-Bewertungsrichtlinien, ISO 27001, EBU R 143, FEDRAMP FIEC, GDPR, HIPAA, PCI DSS, SOC2, Sophos Best Practices	CIS-Bewertungsrichtlinien	CIS-Bewertungsrichtlinien
Benutzerdefinierte Richtlinien				✓		
Netzwerkvisualisierung		✓	✓	✓	✓	✓
IAM-Visualisierung		✓	✓	✓	✓	✓
Spend Monitor		✓	✓	✓	✓	✓
Integriertes Alert-Management (Jira, ServiceNow, Slack, Teams, PagerDuty, Amazon SNS)		✓	✓	✓	✓	✓
SIEM-Integrationen (Splunk, Azure Sentinel)		✓	✓	✓	✓	✓
Rest API		✓	✓	✓	✓	✓
Infrastructure-as-Code-Scanvorlagen		✓	✓	✓	✓	✓
Umgebungs-Zugriffskontrolle		✓	✓	✓	✓	✓
Container-Image-Scans (ECR, ACR, Docker Hub, API)		✓	✓	✓	✓	✓
Managed Service						
24/7 indizienbasiertes Threat Hunting					✓	✓
Security Health Checks					✓	✓
Datenspeicherung					✓	✓
Aktivitätsreports					✓	✓
Angriffserkennung					✓	✓
Beseitigung von Bedrohungen und Bereinigung					✓	✓
24/7 indizienloses Threat Hunting						✓
Threat Response Team Lead						✓
Direkter Telefon-Support						✓
Proaktives Security Posture Management						✓
Ransomware File Protection (CryptoGuard)						✓

Funktionen nach Betriebssystem

Funktionen	Windows	Linux*
Verwaltung		
Mehrere Richtlinien	✓	✓
Gesteuerte Updates	✓	✓
Reduzierung der Angriffsfläche		
Web Security	✓	
Download Reputation	✓	
Web Control/Kategoriebasierte URL-Blockierung	✓	
Peripheriekontrolle	✓	
Application Control	✓	
Application Whitelisting (Server Lockdown)	✓	
Vor Ausführung auf einem Gerät		
Deep-Learning-Malware-Erkennung	✓	✓
Anti-Malware-Dateiscans	✓	✓
Live Protection	✓	✓
Verhaltensanalysen vor Ausführung (HIPS)	✓	
Blockierung pot. unerwünschter Anwendungen (PUAs)	✓	
Intrusion Prevention System (IPS)	✓	
Stoppen von Bedrohungen bei Ausführung		
Data Loss Prevention	✓	
Laufzeit-Verhaltensanalyse (HIPS)	✓	
Antimalware Scan Interface (AMSI)	✓	
Malicious Traffic Detection (MTD)	✓	Siehe Fußnote
Exploit Prevention (Details auf Seite 5)	✓	
Active Adversary Mitigations (Details auf Seite 5)	✓	
Ransomware File Protection (CryptoGuard)	✓	
Disk and Boot Record Protection (WipeGuard)	✓	
Man-in-the-Browser Protection (Safe Browsing)	✓	
Enhanced Application Lockdown	✓	

Funktionen	Windows	Linux*
Erkennung		
Live Discover (umgebungsübergreifende SQL-Abfragen zum Threat Hunting und zur Einhaltung von Sicherheitsvorgaben)	✓	✓
SQL-Abfragen-Library (vorformulierte, individuell anpassbare Abfragen)	✓	✓
Datenspeicherung auf Festplatte (bis zu 90 Tage) mit schnellem Datenzugriff	✓	✓
Produktübergreifende Datenquellen (z. B. Firewall, E-Mail)	✓	✓
Liste mit nach Priorität geordneten Erkennungen	✓	✓
Sophos Data Lake (Cloud-Datenspeicher)	✓	✓
Geplante Abfragen	✓	✓
Laufzeitbasierte Container-Transparenz und -Erkennungen		✓
Analyse		
Bedrohungsfälle (Ursachenanalyse)	✓	
Deep Learning-Malware-Analyse	✓	
Erweiterte Bedrohungsdaten aus den SophosLabs auf Abruf	✓	
Export forensischer Daten	✓	
KI-gesteuerte Analysen	✓	✓
Bereinigung		
Automatisierte Malware-Entfernung	✓	
Synchronized Security Heartbeat	✓	Siehe Fußnote
Sophos Clean	✓	
Live Response (Remote-Terminal-Zugriff für weitere Analysen und Reaktionsmaßnahmen)	✓	✓
On-Demand-Server-Isolation	✓	
Mit einem Klick „Entfernen und blockieren“	✓	
Zugriff/Berechtigung		
Synchronized Application Control (Transparenz über Anwendungen)	✓	
Update-Cache und Message Relay	✓	
Automatische Scan-Ausnahmen	✓	

Funktionen	Windows	Linux*
File Integrity Monitoring	✓	
Managed Service		
24/7 indizienbasiertes Threat Hunting	✓	✓
Security Health Checks	✓	✓
Datenspeicherung	✓	✓
Aktivitätsreports	✓	✓
Angriffserkennung	✓	✓
Beseitigung von Bedrohungen und Bereinigung	✓	✓
24/7 indizienloses Threat Hunting	✓	✓
Threat Response Team Lead	✓	✓
Direkter Telefon-Support	✓	✓
Proaktives Security Posture Improvement	✓	✓

* Für Linux gibt es zwei Bereitstellungs-Optionen: 1) Bereitstellung von Sophos Protection for Linux mit mit den in der Tabelle aufgeführten Funktionen 2) Bereitstellung von Sophos Anti-Virus for Linux mit folgenden Funktionen: Anti-Malware, Live Protection, Malicious Traffic Detection und Synchronized Security. Bitte beachten Sie, dass die beiden Bereitstellungs-Optionen nicht kombiniert werden können.

Sophos-Schutz im Überblick

Details zu den in Intercept X und Cloud Native Security enthaltenen Workload-Schutz-Funktionen

Funktionen	
Exploit Prevention	
Enforce Data Execution Prevention	✓
Mandatory Address Space Layout Randomization	✓
Bottom-up ASLR	✓
Null Page (Null Deference Protection)	✓
Heap Spray Allocation	✓
Dynamic Heap Spray	✓
Stack Pivot	✓
Stack Exec (MemProt)	✓
Stack-based ROP Mitigations (Caller)	✓
Branch-based ROP Mitigations (Hardware Assisted)	✓
Structured Exception Handler Overwrite (SEHOP)	✓
Import Address Table Filtering (IAF)	✓
Load Library	✓
Reflective DLL Injection	✓
Shellcode	✓
VBScript God Mode	✓
Wow64	✓
Syscall	✓
Hollow Process	✓
DLL Hijacking	✓
Squiblydoo Applocker Bypass	✓
APC Protection (Double Pulsar/AtomBombing)	✓
Process Privilege Escalation	✓
Dynamischer Shellcode-Schutz	✓
EFS Guard	✓

Funktionen	
CTF Guard	✓
ApiSetGuard	✓
Active Adversary Mitigations	
Credential Theft Protection	✓
Code Cave Mitigation	✓
Man-in-the-Browser Protection (Safe Browsing)	✓
Malicious Traffic Detection	✓
Meterpreter Shell Detection	✓
Anti-Ransomware	
Ransomware File Protection (CryptoGuard)	✓
Automatic File Recovery (CryptoGuard)	✓
Disk and Boot Record Protection (WipeGuard)	✓
Application Lockdown	
Web-Browser (einschl. HTA)	✓
Web-Browser-Plugins	✓
Java	✓
Media-Anwendungen	✓
Office-Anwendungen	✓
Deep Learning Protection	
Deep-Learning-Malware-Erkennung	✓
Deep Learning Potentially Unwanted Applications (PUA) Blocking	✓
False Positive Suppression	✓
Reaktion, Analyse, Beseitigung	
Bedrohungsfälle (Ursachenanalyse)	✓
Sophos Clean	✓
Synchronized Security Heartbeat	✓

Managed Threat Response (MTR)

Sophos Managed Threat Response (MTR) bietet 24/7 Managed Detection and Response mit Threat Hunting durch ein Expertenteam, als Fully-Managed-Service. MTR-Kunden erhalten außerdem Intercept X Advanced for Server with XDR.

Sophos MTR: Standard

24/7 indizienbasiertes Threat Hunting
Bestätigte schädliche Artefakte und Aktivitäten (starke Signale) werden automatisch blockiert oder beendet. So können die Bedrohungsexperten ihre Suche auf Bedrohungen konzentrieren, für die Indizien vorliegen. Bei dieser Art der Bedrohungssuche werden kausale und angrenzende Ereignisse (schwache Signale) aggregiert und analysiert, um neue „Indicators of Attack (IoA)" und „Indicators of Compromise (IoC)" zu enttarnen, die bislang nicht erkannt werden konnten.

Security Health Check
Sorgen Sie dafür, dass Ihre Sophos-Central-Produkte – allen voran Intercept X Advanced for Server with XDR – stets mit maximaler Performance arbeiten, indem Sie proaktive Untersuchungen Ihrer Betriebsbedingungen und empfohlene Konfigurations-Verbesserungen durchführen.

Aktivitätsreports
Zusammenfassungen der Aktivitäten jedes Falls ermöglichen eine Priorisierung und Kommunikation. So weiß Ihr Team, welche Bedrohungen erkannt und welche Reaktionsmaßnahmen in den jeweiligen Reporting-Zeiträumen ergriffen wurden.

Angriffserkennung
Die meisten erfolgreichen Angriffe beruhen auf der Ausführung eines Prozesses, der für Überwachungstools seriös erscheinen kann. Mithilfe selbst entwickelter Analyseverfahren ermittelt unser Team den Unterschied zwischen seriösem Verhalten und den Taktiken, Techniken und Prozessen (TTPs) von Angreifern.

Sophos MTR: Advanced

Alle Funktionen der „Standard"-Version, plus:

24/7 indizienloses Threat Hunting
Mithilfe von Data Science, Threat Intelligence und der Intuition erfahrener Bedrohungsexperten kombinieren wir verschiedene Informationen (Ihr Unternehmensprofil, hochwertige Assets und Benutzer mit hohem Risiko), um das Verhalten von Angreifern vorherzusagen und neue Angriffsindikatoren (Indicators of Attack, IoA) zu identifizieren.

Optimierte Telemetriedaten
Bedrohungsanalysen werden um Telemetriedaten von anderen Sophos-Central-Produkten ergänzt, die über die Endpoint-Ebene hinaus ein Gesamtbild der Angriffsaktivitäten liefern.

Proaktive Verbesserung des Sicherheitsstatus
Verbessern Sie Ihren Sicherheitsstatus und Ihre Abwehr proaktiv: Sie erhalten von uns Hilfestellung zur Behebung von Konfigurations- und Architektur-Schwachstellen, die sich negativ auf Ihre gesamte Sicherheit auswirken.

Dedizierter Ansprechpartner
Bei Bestätigung eines Vorfalls wird Ihnen ein dedizierter Ansprechpartner zugewiesen, der direkt mit Ihren internen und externen Mitarbeitern vor Ort zusammenarbeitet, bis die aktive Bedrohung neutralisiert wurde.

Direkter Telefon-Support
Ihr Team kann unser Security Operations Center (SOC) direkt telefonisch kontaktieren. Unser MTR-Team ist 24/7 erreichbar und wird von Support-Teams unterstützt, die weltweit auf 26 Standorte verteilt sind.

Asset-Erkennung
Von Asset-Informationen über Betriebssystem-Versionen, Anwendungen und Schwachstellen bis hin zur Identifizierung verwalteter und nicht verwalteter Assets: Wir liefern Ihnen wertvolle Detail-Informationen bei der Einschätzung von Folgen, während Bedrohungssuchen und als Teil proaktiver Empfehlungen zur Verbesserung des Sicherheitsstatus.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

22-07-25 DE (DD)

SOPHOS