Intercept X und Central Endpoint Protection – Übersicht

SOPHOS
Cybersecurity evolved.

Verwaltung über Sophos Central

		FUNKTIONEN	CENTRAL ENDPOINT PROTECTION	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR
ABWEHR	REDUKTION DER ANGRIFFSFLÄCHE	Web Security	✓	✓	✓
		Download Reputation	✓	✓	✓
		Web Control/Kategoriebasierte URL-Filterung	✓	✓	✓
		Peripheriekontrolle	✓	✓	✓
		Application Control	✓	✓	✓
	VOR AUSFÜHRUNG AUF DEM GERÄT	Deep-Learning-Malware-Erkennung		✓	✓
		Anti-Malware-Dateiscans	✓	✓	✓
		Live Protection	✓	✓	✓
		Verhaltensanalysen vor Ausführung (HIPS)	✓	✓	✓
		Blockierung pot. unerwünschter Anwendungen (PUAs)	✓	✓	✓
		Intrusion Prevention System (IPS, ab 2020)	✓	✓	✓
	STOPPEN VON BEDROHUNGEN BEI AUSFÜHRUNG	Data Loss Prevention	✓	✓	✓
		Laufzeit-Verhaltensanalyse (HIPS)	✓	✓	✓
		Antimalware Scan Interface (AMSI)	✓	✓	✓
		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)		✓	✓
		Verbesserter Application Lockdown		✓	✓

Weitere Funktionen auf der nächsten Seite

Intercept X und Central Endpoint Protection – Übersicht

SOPHOS
Cybersecurity evolved.

Verwaltung über Sophos Central (Fortsetzung)

		FUNKTIONEN	CENTRAL ENDPOINT PROTECTION	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR
ERKENNUNG UND ANALYSE	ERKENNUNG	Live Discover (umgebungsübergreifende SQL-Abfragen zum Threat Hunting und zur Einhaltung von Sicherheitsvorgaben)			✓
		SQL-Abfragen-Library (vorformulierte, individuell anpassbare Abfragen)			✓
		Erkennung verdächtiger Ereignisse und Priorisierung			✓
		Datenspeicherung auf Festplatte (bis zu 90 Tage) mit schnellem Datenzugriff			✓
	ANALYSE	Bedrohungsfälle (Ursachenanalyse)		✓	✓
		Deep Learning-Malware-Analyse			✓
		Erweiterte Bedrohungsdaten aus den SophosLabs auf Abruf			✓
		Export forensischer Daten			✓
REAKTION	BEREINIGUNG	Automatisierte Malware-Entfernung	✓	✓	✓
		Synchronized Security Heartbeat	✓	✓	✓
		Sophos Clean		✓	✓
		Remote-Terminal-Zugriff (Remote-Analyse und -Reaktion)			✓
		On-Demand-Endpoint-Isolation			✓
		Mit einem Klick „Entfernen und blockieren“			✓

Intercept X und Central Endpoint Protection – Übersicht

Betriebssysteme im Vergleich

		FUNKTIONEN	WINDOWS	macOS	LINUX*
ABWEHR	REDUKTION DER ANGRIFFSFLÄCHE	Web Security	✓	✓	
		Download Reputation	✓		
		Web Control/Kategoriebasierte URL-Filterung	✓	✓	
		Peripheriekontrolle	✓	✓	
		Application Control	✓	✓	
	VOR AUSFÜHRUNG AUF DEM GERÄT	Deep-Learning-Malware-Erkennung	✓		
		Anti-Malware-Dateiscans	✓	✓	Siehe Fußnote Seite 4
		Live Protection	✓	✓	Siehe Fußnote Seite 4
		Verhaltensanalysen vor Ausführung (HIPS)	✓		
		Blockierung pot. unerwünschter Anwendungen (PUAs)	✓	✓	
		Intrusion Prevention System (IPS, ab 2020)	✓		
	STOPPEN VON BEDROHUNGEN BEI AUSFÜHRUNG	Data Loss Prevention	✓		
		Laufzeit-Verhaltensanalyse (HIPS)	✓		
		Antimalware Scan Interface (AMSI)	✓		
		Malicious Traffic Detection (MTD)	✓	✓	Siehe Fußnote Seite 4
		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)	✓		
		Verbesserter Application Lockdown	✓		

Weitere Funktionen auf der nächsten Seite

Intercept X und Central Endpoint Protection – Übersicht

SOPHOS
Cybersecurity evolved.

Betriebssysteme im Vergleich (Fortsetzung)

		FUNKTIONEN	WINDOWS	macOS	LINUX*
ERKENNUNG UND ANALYSE	ERKENNUNG	Live Discover (umgebungsübergreifende SQL-Abfragen zum Threat Hunting und zur Einhaltung von Sicherheitsvorgaben)	✓	✓	✓
		SQL-Abfragen-Library (vorformulierte, individuell anpassbare Abfragen)	✓	✓	✓
		Erkennung verdächtiger Ereignisse und Priorisierung	✓		
		Datenspeicherung auf Festplatte (bis zu 90 Tage) mit schnellem Datenzugriff	✓	✓	✓
	ANALYSE	Bedrohungsfälle (Ursachenanalyse)	✓	✓	
		Deep Learning-Malware-Analyse	✓		
		Erweiterte Bedrohungsdaten aus den SophosLabs auf Abruf	✓		
		Export forensischer Daten	✓		
REAKTION	BEREINIGUNG	Automatisierte Malware-Entfernung	✓	✓	
		Synchronized Security Heartbeat	✓	✓	Siehe Fußnote
		Sophos Clean	✓		
		Live Response (Remote-Terminal-Zugriff für weitere Analysen und Reaktionsmaßnahmen)	✓	✓	✓
		On-Demand-Endpoint-Isolation	✓		
		Mit einem Klick „Entfernen und blockieren"	✓	✓	

* Für Linux gibt es zwei Bereitstellungs-Optionen:
1) Bereitstellung von Intercept X Advanced with EDR 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.

Funktionen von Sophos Intercept X

SOPHOS
Cybersecurity evolved.

Details zu den Funktionen von Intercept X

	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	✓
	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	✓

	Funktionen	
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
Cybersecurity evolved.

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

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 with EDR – 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), 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.