

# Übersicht über Intercept X for Server und EDR, XDR, MTR

Verwaltung über Sophos Central

	Funktionen	Intercept X Advanced for Server	Intercept X Advanced for Server with EDR	Intercept X Advanced for Server with XDR <sup>1</sup>	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
REDUKTION DER ANGRIFFSFLÄCHE	Web Security	✓	✓	✓	✓	✓
	Download Reputation	✓	✓	✓	✓	✓
	Web Control/Kategoriebasierte URL-Blockierung	✓	✓	✓	✓	✓
	Peripheriekontrolle	✓	✓	✓	✓	✓
	Application Control	✓	✓	✓	✓	✓
	Application Whitelisting (Server Lockdown)	✓	✓	✓	✓	✓
VORAUSFÜHRUNG AUF DEM GERÄT	„Deep Learning“-Malware-Erkennung	✓	✓	✓	✓	✓
	Anti-Malware-Dateiscans	✓	✓	✓	✓	✓
	Live Protection	✓	✓	✓	✓	✓
	Verhaltensanalysen vor Ausführung (HIPS)	✓	✓	✓	✓	✓
	Blockierung pot. unerwünschter Anwendungen (PUAs)	✓	✓	✓	✓	✓
	Intrusion Prevention System	✓	✓	✓	✓	✓
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)	✓	✓	✓	✓	✓
Enhanced Application Lockdown	✓	✓	✓	✓	✓	
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		✓	✓	✓	✓
	Produktübergreifende Datenquellen (z. B. Firewall, E-Mail)			✓		Siehe Fußnote*
	Produktübergreifende Abfragen			✓		Siehe Fußnote*
	Sophos Data Lake (Cloud-Datenspeicher)		7 Tage	30 Tage		Siehe Fußnote*
Geplante Abfragen		✓	✓	✓	✓	

# Übersicht über Intercept X for Server und EDR, XDR, MTR

Verwaltung über Sophos Central

	Funktionen	Intercept X Advanced for Server	Intercept X Advanced for Server with EDR	Intercept X Advanced for Server with XDR <sup>1</sup>	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
ANALYSE	Bedrohungsfälle (Ursachenanalyse)	✓	✓	✓	✓	✓
	Deep Learning-Malware-Analyse		✓	✓	✓	✓
	Erweiterte Bedrohungsdaten aus den SophosLabs auf Abruf		✓	✓	✓	✓
	Export forensischer Daten		✓	✓	✓	✓
BEREINIGUNG	Automatisierte Malware-Entfernung	✓	✓	✓	✓	✓
	Synchronized Security Heartbeat	✓	✓	✓	✓	✓
	Sophos Clean	✓	✓	✓	✓	✓
	Remote-Terminal-Zugriff (Remote-Analyse und -Reaktion)		✓	✓	✓	✓
	On-Demand-Server-Isolation		✓	✓	✓	✓
	Mit einem Klick „Entfernen und blockieren“		✓	✓	✓	✓
VISIBILITY	Cloud Workload Protection (Amazon Web Services, Microsoft Azure, Google Cloud Platform)	✓	✓	✓	✓	✓
	Synchronized Application Control (Transparenz über Anwendungen)	✓	✓	✓	✓	✓
	Verwaltung Ihres Sicherheitsstatus in der Cloud (Cloud Hosts überwachen und schützen, serverlose Funktionen, S3-Buckets etc.)	✓	✓	✓	✓	✓
KONTROLLE	Serverspezifische Richtlinienverwaltung	✓	✓	✓	✓	✓
	Update-Cache und Message-Relay	✓	✓	✓	✓	✓
	Automatische Scan-Ausnahmen	✓	✓	✓	✓	✓
	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					✓

Bitte beachten: Das MTR-Team kann bei Kunden von MTR Advanced auf XDR-Daten und -Funktionen zurückgreifen. MTR-Kunden sind in ihrer Sophos-Central-Konsole jedoch auf EDR-Funktionen beschränkt und müssen für XDR-Funktionen eine XDR-Lizenz erwerben.

<sup>1</sup>Lizenziert als Intercept X Advanced for Server with EDR + Sophos XDR

# Funktionen nach Betriebssystem

	FUNKTIONEN	WINDOWS	LINUX*
REDUKTION DER ANGRIFFSFLÄCHE	Web Security	✓	
	Download Reputation	✓	
	Web Control/Kategoriebasierte URL-Blockierung	✓	
	Peripheriekontrolle	✓	
	Application Control	✓	
	Application Whitelisting (Server Lockdown)	✓	
VORAUSFÜHRUNG AUF DEM GERÄT	„Deep Learning“-Malware-Erkennung	✓	✓
	Anti-Malware-Dateiscans	✓	✓
	Live Protection	✓	✓
	Verhaltensanalysen vor Ausführung (HIPS)	✓	
	Blockierung pot. unerwünschter Anwendungen (PUAs)	✓	
	Intrusion Prevention System	✓	
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)	✓	
Enhanced Application Lockdown	✓		
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	✓	✓
	Produktübergreifende Datenquellen (z. B. Firewall, E-Mail)	✓	✓
	Produktübergreifende Abfragen	✓	✓
	Sophos Data Lake (Cloud-Datenspeicher)	✓	✓
	Geplante Abfragen	✓	✓

# Funktionen nach Betriebssystem

	FUNKTIONEN	WINDOWS	LINUX*
ANALYSE	Bedrohungsfälle (Ursachenanalyse)	✓	
	Deep Learning-Malware-Analyse	✓	
	Erweiterte Bedrohungsdaten aus den SophosLabs auf Abruf	✓	
	Export forensischer Daten	✓	
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“	✓	
VISIBILITY	Cloud Workload Protection (Amazon Web Services, Microsoft Azure, Google Cloud Platform)	✓	✓
	Synchronized Application Control (Transparenz über Anwendungen)	✓	
	Verwaltung Ihres Sicherheitsstatus in der Cloud (Cloud Hosts überwachen und schützen, serverlose Funktionen, S3-Buckets etc.)	✓	✓
KONTROLLE	Serverspezifische Richtlinienverwaltung	✓	
	Update-Cache und Message-Relay	✓	
	Automatische Scan-Ausnahmen	✓	
	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) Sophos Protection for Linux mit den in der Tabelle angehakten Funktionen.

2) 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

## 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 Aplocker 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 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 Bedrohungsuche 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), 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.