SOPHOS
Security made simple.

# Sophos Intercept X

## „Deep Learning"-Malware-Erkennung, Exploit Prevention, Anti-Ransomware, Ursachenanalyse und Sophos Clean

Sophos Intercept X stoppt Angreifer und Bedrohungen mit der richtigen Technik zur richtigen Zeit. In Kombination mit Ihrer Antivirus-Software oder Sophos Endpoint Protection bietet Sophos Intercept X umfassenden Next-Generation-Schutz.

### Highlights

- „Trainierte" Deep-Learning-Modelle erkennen unbekannte Malware
- Exploit Prevention stoppt Techniken, mit denen Angreifer versuchen, anfällige Software unter ihre Kontrolle zu bringen
- Active Adversary Mitigation verhindert Persistenz auf Systemen
- Ursachenanalyse gibt Aufschluss über Aktivitäten und Ursprung von Malware
- Sophos Clean entfernt Malware rückstandslos
- Wertet Ihre bestehende Antivirus-Software auf

### Maßgeschneiderte Next-Gen Endpoint Security

Die Zeiten einfacher Dateiscans sind schon lange Geschichte. Ein effektiver Schutz muss Bedrohungen daran hindern, auf Ihre Geräte zu gelangen, sie stoppen, bevor sie ausgeführt werden, und sie aufspüren, falls sie die Abwehr überlistet haben. Es genügt nicht, die Malware zu beseitigen – auch alle Aktionen der Malware müssen analysiert und rückgängig gemacht werden. Sophos Intercept X ergänzt Ihre bestehende Antivirus-Software durch modernste Schutztechnologien für umfassenden Next-Gen-Schutz.

### „Deep Learning"-Malware-Erkennung

Intercept X wird in den SophosLabs mit neuronalen Deep-Learning-Netzwerken „trainiert" und kann daher neue, unbekannte Malware-Dateien sehr genau erkennen – ohne Signaturen. Bei anderen Machine-Learning-Methoden ist es häufig erforderlich, dass Datenwissenschaftler Attribute identifizieren, nach denen gesucht werden soll. Das daraus resultierende Modell ist dann durch die Effektivität der Attribut-Auswahl und Trainingsdaten beschränkt. Die „Deep Learning"-Funktion in Intercept X hingegen identifiziert die wichtigen Attribute, um zwischen Malware und unbedenklichen Dateien zu unterscheiden, selbst. Dies, kombiniert mit einem umfangreichen Trainingsdatensatz aus den SophosLabs, ermöglicht das Festlegen einer präzisen Entscheidungsgrenze zwischen schädlichen und unbedenklichen Dateien. Das Trainingsmodell ist kleiner als 20 MB und benötigt nur selten Updates. In der Cloud trainieren die SophosLabs das Modell kontinuierlich weiter und prüfen diese Entscheidungsgrenze mit neuen, unbekannten Malware-Samples.

### Leistungsstarker Schutz für schwachstellenanfällige Software

Neue Schwachstellen treten mit alarmierender Häufigkeit auf. Bis sie von den Software-Herstellern mit Patches behoben werden, bieten sie ein Eintrittstor für Angreifer, die verschiedenste Exploit-Techniken nutzen. Exploit Prevention stoppt diese Techniken und verhindert, dass Angreifer eine noch nicht gepatchte Schwachstelle ausnutzen können.

### Effektive Erkennung von Ransomware

Unsere CryptoGuard-Technologie erkennt spontane, schädliche Datenverschlüsselungen und stoppt Ransomware sofort, bevor sie Schaden anrichtet. Selbst wenn vertrauenswürdige Dateien und Prozesse manipuliert oder zweckentfremdet werden, stoppt CryptoGuard den Vorgang und versetzt die betroffenen Elemente wieder zurück in ihren Ursprungszustand – ohne dass ein Eingreifen des Benutzers oder der IT-Abteilung nötig ist. CryptoGuard arbeitet unauffällig auf Dateisystemebene und behält Remote-Computer und lokale Prozesse im Auge, die versuchen, Ihre Dokumente und andere Dateien zu manipulieren.

## Ursachenanalyse

Durch das Identifizieren, Isolieren und Entfernen von Malware wird das unmittelbare Problem beseitigt. Aber wissen Sie, was die Malware genau gemacht hat, bevor sie entfernt wurde, oder wie sie überhaupt auf dem System Fuß fassen konnte? Unsere Ursachenanalyse informiert Sie über alle Ereignisse, die zur Erkennung geführt haben. Sie sehen, welche Dateien, Prozesse und Registry-Schlüssel mit der Malware in Kontakt gekommen sind, und können eine gründliche Systembereinigung vornehmen.

## Einfache Lizenzierung und Bereitstellung

Bei einer Verwaltung Ihrer Sicherheit über Sophos Central müssen Sie zum Schutz Ihrer Endpoints keine Server installieren oder bereitstellen. Sophos Central ist bereits mit Standard-Richtlinien und empfohlenen Einstellungen vorkonfiguriert, sodass Sie von Anfang an effektiven Schutz erhalten.

## In vier Schritten zu effektivem Schutz

1. Besuchen Sie www.sophos.de/intercept-x, um Sophos Intercept X zu testen.
2. Erstellen Sie einen Sophos Central Admin-Account.
3. Downloaden und installieren Sie den Intercept-X-Agenten.
4. Verwalten Sie Ihren Schutz über Sophos Central.

## Technische Spezifikationen

Sophos Intercept X unterstützt Windows 7 und höher, 32 und 64 Bit. Sophos Intercept X kann gemeinsam mit Sophos Endpoint Protection Standard oder Advanced eingesetzt werden. Alternativ lässt sich Sophos Intercept X auch in Kombination mit Endpoint-/Antivirus-Produkten anderer Hersteller nutzen, um „Deep Learning"-Malware-Erkennung, Schutz vor Exploits und Ransomware, Ursachenanalyse und Sophos Clean hinzuzufügen.

| | 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 | ✓ |
| 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 | „Deep Learning"-Malware-Erkennung | ✓ |
| | Deep Learning Potentially Unwanted Applications (PUA) Blocking | ✓ |
| | False Positive Suppression | ✓ |
| | Live Protection | ✓ |
| REAKTION ANALYSE BESEITIGUNG | Ursachenanalyse | ✓ |
| | Sophos Clean | ✓ |
| | Synchronized Security Heartbeat | ✓ |
| BEREITSTELLUNG | Kann als Standalone-Agent ausgeführt werden | ✓ |
| | Kann mit bestehendem Antivirus ausgeführt werden | ✓ |
| | Kann als Komponente von bestehendem Sophos Endpoint Agent ausgeführt werden | ✓ |
| | Windows 7 | ✓ |
| | Windows 8 | ✓ |
| | Windows 8.1 | ✓ |
| | Windows 10 | ✓ |
| | macOS* | ✓ |

* Unterstützte Funktionen: CryptoGuard, Malicious Traffic Detection,Synchronized Security Heartbeat, Ursachenanalyse

Verwalten Sie Ihre Sophos Endpoint Protection über die Sophos Enterprise Console? Sie können Ihre Endpoints über Sophos Central verwalten und Sophos Intercept X zur automatischen Bereitstellung aktivieren.

## Jetzt kostenfrei testen

Fordern Sie jetzt Ihre kostenlose 30-Tage-Testversion an unter www.sophos.de/intercept-x

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de



2017-09-10-DS-DE (MP)

SOPHOS