SOPHOS

Sophos Intercept X

Einzigartige Endpoint Protection

Sophos Intercept X stoppt mehr Bedrohungen als je zuvor – dank seiner einmaligen Kombination aus Deep-Learning-Malware-Erkennung, Exploit-Abwehr, Anti-Ransomware sowie weiteren modernsten Schutzfunktionen.

Highlights

- Unsere branchenführende Malware-Erkennungsengine mit leistungsstarkem Deep Learning
- 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
- Spezielle Technologie zum Schutz vor Ransomware
- Intercept X wertet Ihre bestehende Antivirus-Software auf. Intercept X Advanced ersetzt Ihre bestehende Endpoint Security durch eine Kombination aus traditionellen und modernen Techniken.

Sophos Intercept X nutzt einen umfassenden Ansatz zum Schutz Ihrer Endpoints und verlässt sich nicht auf einen einzelnen Sicherheitsansatz. Das bezeichnen wir als „Power of the Plus" – eine Kombination führender traditioneller und moderner Techniken.

Zu modernen Techniken gehören Deep-Learning-Malware-Erkennung, Exploit-Abwehr und spezielle Funktionen für Ransomware-Schutz. Zu grundlegenden Techniken gehören signaturbasierte Malware-Erkennung, Verhaltensanalysen, Erkennung von schädlichem Datenverkehr, Device Control, Application Control, Webfilterung, Data Loss Prevention und mehr.

Deep-Learning-Malware-Erkennung

Bei der in Intercept X integrierten künstlichen Intelligenz handelt es sich um ein neuronales Netzwerk – eine erweiterte Form des maschinellen Lernens. Dieses Netzwerk ist in der Lage, sowohl bekannte als auch unbekannte Malware komplett ohne Signaturen zu erkennen.

Intercept X mit leistungsstarkem Deep Learning nutzt die branchenweit beste Malware-Erkennungsengine, wie unabhängige Tests bestätigen. So kann Intercept X auch die Malware erkennen, die andere Endpoint Security Software übersieht.

Effektive Exploit-Abwehr

Neue Schwachstellen treten mit alarmierender Häufigkeit auf und müssen von den Software-Herstellern mit Patches behoben werden. Neue Exploit-Techniken sind dagegen viel seltener und werden von Angreifern für verschiedene Schwachstellen wiederverwendet. Sophos Exploit Prevention blockiert die Exploit-Tools und -Techniken, die zur Verbreitung von Malware, zum Diebstahl von Zugangsdaten und zum Aushebeln von Erkennungsmechanismen genutzt werden. So haben Hacker und Zero-Day-Angriffe keine Chance mehr, in Ihr Netzwerk zu gelangen.

Bewährter Ransomware-Schutz

Durch Verhaltensanalysen stoppt Intercept X unbekannte Ransomware- und Boot-Record-Angriffe und ist damit die branchenweit leistungsstärkste Anti-Ransomware-Technologie. Selbst wenn vertrauenswürdige Dateien und Prozesse manipuliert 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.

Endpoint Detection and Response (EDR)

„Endpoint Detection and Response"-Funktionen sind erforderlich, um über die reine Abwehr hinaus zusätzliche Bedrohungen zu erkennen, weitere Analysen vorzunehmen und versiert reagieren zu können. Sophos Intercept X Advanced with EDR kombiniert intelligente EDR mit branchenweit erstklassiger Endpoint Protection in einer Lösung. Damit erhalten Unternehmen detaillierte Informationen und können kritische Fragen zu Sicherheitsvorfällen beantworten.

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.

Managed Threat Response (MTR)

Managed Detection and Response – 24/7 Fully-Managed-Service von einem Sophos-Expertenteam. Mit der intelligenten EDR von Intercept X Advanced with EDR reagieren Sophos-Analysten auf potenzielle Bedrohungen, suchen nach „Indicators of Compromise" und liefern detaillierte Analysen der Ereignisse – was ist wo, wann, wie und warum passiert?

Technische Spezifikationen

Sophos Intercept X unterstützt Windows 7 und höher, 32 und 64 Bit. Alternativ lässt sich Sophos Intercept X auch in Kombination mit Endpoint-/Antivirus-Produkten anderer Hersteller nutzen, um Deep-Learning-Malware-Erkennung, Exploit-Abwehr, Anti-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

Kostenlose 30-Tage-Testversion 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

2019-12-13 DSDE (PC)

SOPHOS