SOPHOS
Cybersecurity made simple.

CLOUD READY

Intercept X for Server

Ganz gleich ob in der Cloud oder lokal, die kritischen Anwendungen und Daten Ihres Unternehmens müssen zuverlässig geschützt werden. Intercept X for Server bietet umfassenden Schutz mit Deep Learning Malware-Erkennung, Exploit Prevention, Anti-Ransomware-Technologie, Whitelisting von Anwendungen, Active Adversary Protection und fundierter Ursachenanalyse.

Highlights

- Erkennt und schützt Workloads in Microsoft Azure und Amazon Web Services
- Schützt vor Ransomware auf Servern, einschließlich Remote-Angriffen über von Angreifern eingeschleuste oder übernommene Endpoints
- Server Lockdown und Whitelisting von Anwendungen
- Wehrt hochkomplexe Hacking-Techniken und Exploits ab
- Ursachenanalyse mit weiterführenden Informationen zu Ursprung des Angriffs und Infektionsweg
- Synchronized Security ermöglicht den Austausch von Bedrohungs-, Sicherheits- und Schutzdaten zwischen verschiedenen Sophos-Produkten
- Einfache Verwaltung über Sophos Central
- Schutz vor Bedrohungen für Windows- und Linux-Systeme

Leistungsstarker Schutz speziell für Server

Intercept X for Server nutzt ein breites Spektrum verschiedener Schutzmechanismen, um Zero-Day-Angriffe, Exploits und Hacker abzuwehren. Diese Mechanismen verhindern, dass Angriffe überhaupt die Server erreichen, erkennen Angriffe, bevor sie ausgeführt werden oder stoppen sie und führen eine gründliche Bereinigung durch, wenn ein Angriff doch einmal nicht abgefangen wurde. Das KI-Modell wird ständig aktualisiert und darauf trainiert, nach verdächtigen Attributen von potenziell schädlichem Code auf Servern Ausschau zu halten. Darüber hinaus wird mit serverspezifischen Funktionen wie Server Lockdown und Cloud Workload Discovery sichergestellt, dass Serverkonfigurationen geschützt sind.

Intercept X for Server erkennt und schützt Workloads in der Cloud, einschließlich Microsoft Azure und Amazon Web Services. Wird Sophos Central mit AWS und Azure verbunden, bestätigt Intercept X for Server visuell, dass die Server geschützt sind. Durch die Anzeige wichtiger Informationen in Sophos Central wird die Verwaltung erleichtert.

Abwehr serverbasierter Ransomware

CryptoGuard schützt vor Ransomware, indem auf Dateisystemebene unerwünschte Dateiverschlüsselungen erkannt und verhindert werden, sowohl auf dem Server als auch von einem mit dem Server verbundenen Remote-Endpoint. WipeGuard funktioniert ähnlich und schützt den Master Boot Record vor schädlicher Verschlüsselung.

Sophos Intercept X for Server ermöglicht mit einem einzigen Klick einen Server Lockdown. Dabei werden Ihre Anwendungen auf eine Whitelist gesetzt, der Server wird in einem sicheren Zustand „eingefroren" und die Ausführung nicht autorisierter Anwendungen wird verhindert. Sophos überprüft automatisch das System und erstellt ein Verzeichnis (Whitelist) bekannter erwünschter Anwendungen, ohne dass manuell Regeln erstellt werden müssen. Sophos stellt eine feste Verbindung zwischen Anwendungen und zugehörigen Dateien wie DLL, Datendateien und Skripten her.

Schutz vor Exploits: Keine Chance für Hacker

Neue Schwachstellen treten mit alarmierender Häufigkeit auf und oft ist es eine ganz schöne Herausforderung, Server zu patchen, ohne die Nutzer bei ihrer Arbeit zu behindern. Exploit-Angriffe können verheerende Folgen haben und werden von traditionellen Serverschutz-Technologien häufig nicht erkannt. Intercept X for Server hält selbst die hartnäckigsten Hacker davon ab, mithilfe von Exploit-Techniken Zugangsdaten abzugreifen. Ganz gleich, ob diese Techniken verborgen und persistent sind oder sich ausbreiten, Intercept X wehrt sie ab.

Ursachenanalyse

Intercept X for Server beinhaltet auch Erkennungs- und Reaktionstechnologien, damit Administratoren genau wissen, wie ein Angreifer eingedrungen ist, wohin sich der Angriff ausgebreitet hat, wer und was genau betroffen ist und welche Schritte erforderlich sind. Intercept X for Server macht dies möglich, ohne dass ein zusätzlicher Agent oder eine weitere Verwaltungskonsole nötig ist.

Synchronized Security

Synchronized Security ist ein branchenführendes Sicherheitssystem, das dafür sorgt, dass Ihre Abwehrmaßnahmen genauso koordiniert sind wie die Angriffe, vor denen sie schützen. Das System kombiniert eine intuitive Security-Plattform mit preisgekrönten Produkten, die aktiv zusammenarbeiten. Dieser einzigartige Sicherheitsansatz schützt Sie optimal gegen komplexe Bedrohungen.

Highlights von Intercept X for Server

PLATTFORMEN		Windows-Server	✓
		Linux[1]	✓
		Öffentliche Cloud (Microsoft Azure und Amazon AWS)	✓
ABWEHR	REDUKTION DER ANGRIFFSFLÄCHE	Whitelisting von Anwendungen (Server Lockdown)	✓
		Web Security	✓
		Windows Firewall Control	✓
		Download Reputation	✓
		Web Control (Blockieren von URLs)	✓
		Peripheral Control (z. B. USB)	✓
		Application Control	✓
	VOR AUSFÜHRUNG AUF DEM GERÄT	„Deep Learning"-Malware-Erkennung	✓
		Exploit Prevention	✓
		Dateiüberprüfungen auf Malware	✓
		Live Protection	✓
		Verhaltensanalysen vor Ausführung (HIPS)	✓
		Off-Board-Überprüfungen bei VMs (ESXi und Hyper-V)[2]	✓
		Erkennung potenziell unerwünschter Anwendungen (PUAs)	✓
		Data Loss Prevention	✓

Einfache Verwaltung mit Sophos Central

Wenn Sie Ihren Schutz mit Sophos Central verwalten, brauchen Sie keine Server mehr aufzusetzen, um Ihre Systeme zu schützen. Sophos Central wird von Sophos gehostet und ermöglicht sofortigen Zugriff, ohne dass Konsolenserver eingerichtet werden müssen. Sophos Central stellt Standardrichtlinien für Server bereit und ermöglicht auch die Verwaltung anderer Sophos Produkte wie Sophos Intercept X, Mobile, Wireless, Email und Web – alles über eine zentrale transparente Ansicht.

ERKENNUNG	BEDROHUNGEN WERDEN AN DER AUSFÜHRUNG GEHINDERT	Anti-Hacker/Active Adversary Mitigations	✓
		Ransomware File Protection (CryptoGuard) ermöglicht Erkennung von Angriffen auf Server von remote verbundenen Endpoints	✓
		Disk & Boot Record Protection (WipeGuard)	✓
		Malicious Traffic Detection	✓
REAKTION	ANALYSE UND BESEITIGUNG	Sophos Clean Automatisierte Malware-Entfernung	✓
		Ursachenanalyse	✓
VERWALTUNG	KONTROLLE	Serverspezifische Richtlinienverwaltung	✓
		Update-Cache und Message-Relay	✓
		Automatische Scan-Ausnahmen	✓
		Synchronized Application Control[4]	✓
	VISIBILITY	Azure Workload-Erkennung und Schutz	✓
		AWS Workload-Erkennung und Schutz	✓
		AWS Map, regionenübergreifende Visualisierung	✓
		Synchronized Security mit Security Heartbeat™ (Erweiterter Schutz vor Bedrohungen, Positive Source Identification und automatisierte Isolierung)[4]	✓
		Windows Remote Desktop Services (Benutzertransparenz)	✓
	SOPHOS CENTRAL	Cloudbasierte Verwaltung, keine Installation und Pflege eines separaten lokalen Servers erforderlich und Verwaltung der Sicherheit von Servern in einer zentralen Konsole zusammen mit Endpoints, Mobile, Email, Wireless	✓
		Multi-Faktor-Authentifizierung	✓
		Rollenbasierte Administration	✓

1 Alle Funktionen verfügbar unter Windows; ausgewählte Funktionen verfügbar unter Linux.
2 Siehe License Guide for Sophos for Virtual Environments, Ultra-thin Agent Deployment.
3 Bei Windows-Servern, die von Sophos Enterprise Console verwaltet werden, ist CryptoGuard mit der Add-on-Lizenz für Endpoint Exploit Prevention (EXP) erhältlich.
4 In Kombination mit der Sophos XG Firewall.

Azure

aws partner network
Advanced Technology Partner
Security Competency
Public Sector Partner
Marketplace Seller

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion unter www.sophos.de/server.

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

2018-06-28 DS-DE (MP)

SOPHOS