Intercept X Advanced for Server with EDR

Innovativ. Umfassend. Stark.

Schützen Sie Ihre Cloud, Ihre lokalen und virtuellen Server vor Malware, Ransomware und dateilosen Angriffen und erhalten Sie maximale Transparenz über Ihre gesamte Umgebung – mit EDR, das Threat Hunting- und IT-Operations-Aufgaben optimiert.

Umfassender Schutz vor neuesten Bedrohungen

Sophos Intercept X for Server nutzt einen umfassenden Ansatz zum Schutz Ihrer Server und verlässt sich nicht auf eine einzelne Sicherheitstechnik.

Moderne Techniken nutzen signaturlose KI mit Deep Learning: Diese blockiert zuverlässig neue, bisher unbekannte Malware. Anti-Ransomware-Funktionen erkennen und stoppen schädliche Verschlüsselungsprozesse und versetzen betroffene Dateien zurück in einen sicheren Zustand. So werden negative Auswirkungen auf den Geschäftsbetrieb deutlich minimiert. Anti-Exploit-Techniken neutralisieren dateilose Angriffe und Exploits wie verschleierte PowerShell-Skripts, die häufig von Angreifern verwendet werden. Grundlegende Techniken beinhalten u. a. signaturbasierte Malware Erkennung, Verhaltensanalysen, Erkennung von schädlichem Datenverkehr, Device Control, Application Control, Webfilterung sowie Data Loss Prevention.

Maximale Transparenz

Intercept X Advanced for Server ist die erste EDR-Lösung, die speziell für IT Operations und Threat Hunting entwickelt wurde. Suchen Sie z. B. nach Servern, bei denen unnötigerweise Remote Desktop Protocol (RDP) aktiviert ist, und schließen Sie diese Sicherheitslücke. Finden Sie verdächtige Prozesse, die versuchen, eine Verbindung über einen Nicht-Standardport herzustellen, und beenden Sie diese.

Sie können Ihr gesamtes Multi-Cloud Inventory sehen und schützen, Ihre Cloud Workloads sowie kritische Cloud Services wie S3 Buckets, Datenbanken und serverlose Funktionen erfassen, verdächtige Aktivitäten oder unsichere Bereitstellungen erkennen und Sicherheitslücken schließen.

Volle Kontrolle über Ihre Server

Sie können schnell Richtlinien zum Schutz vor Bedrohungen, für Application, Peripheral und Web Control erstellen und diese mit wenigen Klicks für Ihre Cloud sowie für Ihre lokalen und virtuellen Bereitstellungen aktivieren. Bei Bedarf können auch individuelle Richtlinien für einzelne Server konfiguriert werden. Mit einem Klick aktivieren Sie einen Lockdown für Ihre Server und schützen diese so vor nicht autorisierten Änderungen, sodass nur Ihre genehmigten Anwendungen ausgeführt werden können – ohne ServerAusfallzeiten. Überwachen Sie wichtige Dateien und Ordner, und erhalten Sie eine Benachrichtigung, wenn versucht wird, diese zu manipulieren.

Schutz für Ihre gesamte Umgebung

Intercept X for Server schützt Ihre Server unabhängig vom Standort und erleichtert die Verwaltung aller Server über eine zentrale Konsole. Schützen Sie physische Server vor Ort, Cloud-Amazon-EC2-Instanzen, virtuelle MicrosoftAzure- und Google-Cloud-Maschinen sowie virtuelle Bereitstellungen und gemischte Umgebungen.

SOPHOS

INTERCEPT X

Lösung

Security & Identity

Produkt

Intercept X

Highlights

- Schutz Ihrer lokalen Server und Cloud Workloads
- Branchenführender Malware-Schutz mit leistungsstarkem Deep Learning
- Active Adversary Protection, Schutz vor Exploits und Ransomware
- Endpoint Detection and Response (EDR) mit leistungsstarken Funktionen zur Sicherstellung der Durchsetzung von Sicherheitsvorgaben und zum Threat Hunting für IT-Administratoren und Sicherheitsanalysten
- Transparenz und Sicherheit für Ihre gesamte Cloud Umgebung, inklusive S3- Buckets und Datenbanken
- Schutz Ihrer Server Konfigurationen vor nichtautorisierten Änderungen

BERGT working it-services

Features

Features	
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	✓
Anti-Ransomeware	
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	✓
Reaktion/Analyse/Beseitigung	
False Positive Suppression	✓
Bedrohungsfälle (Ursachenanalyse)	✓
Sophos Clean	✓
Synchronized Security Heartbeat	✓

SOPHOS

INTERCEPT X

Lösung

Security & Identity

Produkt

Intercept X

Highlights

- Schutz Ihrer lokalen Server und Cloud Workloads
- Branchenführender Malware-Schutz mit leistungsstarkem Deep Learning
- Active Adversary Protection, Schutz vor Exploits und Ransomware
- Endpoint Detection and Response (EDR) mit leistungsstarken Funktionen zur Sicherstellung der Durchsetzung von Sicherheitsvorgaben und zum Threat Hunting für IT-Administratoren und Sicherheitsanalysten
- Transparenz und Sicherheit für Ihre gesamte Cloud Umgebung, inklusive S3- Buckets und Datenbanken
- Schutz Ihrer Server Konfigurationen vor nichtautorisierten Änderungen

BERGT working it-services

Features

	Central Server Protection	Intercept X Adv for Server	Intercept X Adv for Server with EDR
Reduktion der Angriffsfläche			
Web Security	✓	✓	✓
Download Reputation	✓	✓	✓
Web Control/Kategorisierbare URL-Filterung	✓	✓	✓
Peripheral Control	✓	✓	✓
Application Control	✓	✓	✓
Application Whitelisting (Server Lockdown)		✓	✓
Vor Ausführung auf dem Gerät			
Deep-Learning-Malware-Erkennung		✓	✓
Anti-Malware-Dateiscans	✓	✓	✓
Live Protection	✓	✓	✓
Verhaltensanalysen vor Ausführung (HIPS)	✓	✓	✓
Blockierung potenziell unerwünschter Anwendungen (PUAs)	✓	✓	✓
Intrusion Prevention System (IPS, ab 2020)	✓	✓	✓
Stoppen von Bedrohung bei Ausführung			
Data Loss Prevention	✓	✓	✓
Laufzeit-Verhaltensanalyse (HIPS)	✓	✓	✓
Antimalware Scan Interface (AMSI)	✓	✓	✓
Malicious Traffic Detection (MTD)	✓	✓	✓
Exploit Prevention		✓	✓
Active Adversary Mitigations		✓	✓
Ransomware File Protection (CryptoGuard)		✓	✓
Disk and Boot Record Protection (WipeGuard)		✓	✓
Man-in-the-Browser Protection (Safe Browsing)		✓	✓
Verbesserter 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			✓
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“			✓

SOPHOS

INTERCEPT X

Lösung

Security & Identity

Produkt

Intercept X

Highlights

- Schutz Ihrer lokalen Server und Cloud Workloads
- Branchenführender Malware-Schutz mit leistungsstarkem Deep Learning
- Active Adversary Protection, Schutz vor Exploits und Ransomware
- ndpoint Detection and Response (EDR) mit leistungsstarken Funktionen zur Sicherstellung der Durchsetzung von Sicherheitsvorgaben und zum Threat Hunting für IT-Administratoren und Sicherheitsanalysten
- Transparenz und Sicherheit für Ihre gesamte Cloud Umgebung, inklusive S3- Buckets und Datenbanken
- Schutz Ihrer Server Konfigurationen vor nichtautorisierten Änderungen

Features

	Central Server Protection	Intercept X Adv for Server	Intercept X Adv for Server with EDR
Visibility			
Cloud Workload Protection (Amazon Web Services, Microsoft Azure, Google Cloud Platform)	✓	✓	✓
AWS Map, regionenübergreifende Visualisierung	✓	✓	✓
Synchronized Application Control (Transparenz über Anwendungen)	✓	✓	✓
Verwaltung Ihres Sicherheitsstatus in der Cloud (Cloud Hosts überwachen und schützen, serverlose Funktionen, Speicherfreigabe etc.)			✓
Kontrolle			
Serverspezifische Richtlinienverwaltung	✓	✓	✓
Update-Cache und Message-Relay	✓	✓	✓
Automatische Scan-Ausnahmen	✓	✓	✓
File Integrity Monitoring	✓	✓	✓

INTERCEPT X

Lösung

Security & Identity

Produkt

Intercept X

Highlights

- Schutz Ihrer lokalen Server und Cloud Workloads
- Branchenführender Malware-Schutz mit leistungsstarkem Deep Learning
- Active Adversary Protection, Schutz vor Exploits und Ransomware
- ndpoint Detection and Response (EDR) mit leistungsstarken Funktionen zur Sicherstellung der Durchsetzung von Sicherheitsvorgaben und zum Threat Hunting für IT-Administratoren und Sicherheitsanalysten
- Transparenz und Sicherheit für Ihre gesamte Cloud Umgebung, inklusive S3- Buckets und Datenbanken
- Schutz Ihrer Server Konfigurationen vor nichtautorisierten Änderungen

SOPHOS