SOPHOS

SYNCHROWORKS CONSULTING

Intercept X Advanced for Server with EDR

Unmatched Server Protection

Secure your cloud, on-premises and virtual servers from never-seen-before malware, ransomware and fileless attacks and get unparalleled visibility across your entire estate with EDR that streamlines threat hunting and IT operations tasks.

Highlights

- Secure your on-premises servers and cloud workloads
- Top-rated malware protection driven by deep learning
- Active adversary, exploit, and ransomware protection
- Endpoint Detection and Response (EDR) that delivers powerful IT security operations hygiene and threat hunting for both IT admins and security analysts
- See and secure your wider cloud environment such as S3 buckets and databases
- Protect your server configurations from unauthorized changes

Stop the Latest Threats

Sophos Intercept X for Server employs a comprehensive defense-in-depth approach to server protection, rather than simply relying on one primary security technique.

Modern techniques include signatureless deep learning AI which excels at blocking malware that has never been seen before. Anti-ransomware capabilities detect and stop malicious encryption processes and return affected files to a safe state, minimizing business disruption. Anti-exploit techniques neutralize fileless attacks and exploits such as obfuscated PowerShell scripts that are commonly used by attackers. Foundational techniques include signature-based malware detection, behavior analysis, malicious traffic detection, device control, application control, web filtering, data loss prevention, and more.

Get Unparalleled Visibility

Intercept X Advanced for Server is the first EDR solution designed for IT administrators and security analysts to solve IT operations and threat hunting use cases. For example, find servers that have remote desktop protocol (RDP) unnecessarily enabled and close the security gap and hunt down suspicious processes that are attempting to connect on a non-standard port and terminate them.

See and secure your entire multi-cloud inventory. You can detect your cloud workloads as well as critical cloud services including S3 buckets, databases and serverless functions, identify suspicious activity or insecure deployments, and close security gaps.

Take Control of Your Servers

Quickly create policies for threat protection, application, peripheral, and web control and apply them across your cloud, on-premises and virtual deployments. Policies can also be configured individually for servers that require them. Lockdown servers with a single click preventing any unauthorized changes so that only apps approved by you can run – with no server downtime. Monitor critical files and folders, receiving notification if attempts are made to tamper with them.

Simplify Management and Deployment

Sophos Central makes managing your servers easy. Policy management, alerts, and reporting are all accessed from the same screen. Sophos Central also provides default policies and recommended configurations to ensure that you get the most effective protection from day one. And the license policy and agent deployed is the same for physical, virtual, cloud, and mixed deployments.

Secure Your Entire Estate

Intercept X for Server protects your servers wherever they are and makes it easy to manage them all from the same console. Secure servers physically on-premises, cloud Amazon EC2 instances, Microsoft Azure and Google Cloud virtual machines as well as virtual deployments and mixed estates.

Managed Threat Response (MTR)

24/7 threat hunting, detection and response delivered by a team of Sophos experts as a fully managed service. Utilizing the intelligent EDR found in Intercept X Advanced for Server with EDR, Sophos analysts respond to potential threats, look for indicators of compromise and provide detailed analysis on events including what happened, where, when, how and why.

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	✓
Dynamic Shellcode Protection	✓
EFS Guard	✓
CTF Guard	✓
ApiSetGuard	✓

FEATURES	
ACTIVE ADVERSARY MITIGATIONS	
Credential Theft Protection	✓
Code Cave Mitigation	✓
Man-in-the-Browser Protection (Safe Browsing)	✓
Malicious Traffic Detection	✓
Meterpreter Shell Detection	✓
ANTI-RANSOMWARE	
Ransomware File Protection (CryptoGuard)	✓
Automatic file recovery (CryptoGuard)	✓
Disk and Boot Record Protection (WipeGuard)	✓
APPLICATION LOCKDOWN	
Web Browsers (including HTA)	✓
Web Browser Plugins	✓
Java	✓
Media Applications	✓
Office Applications	✓
DEEP LEARNING PROTECTION	
Deep Learning Malware Detection	✓
Deep Learning Potentially Unwanted Applications (PUA) Blocking	✓
RESPOND/INVESTIGATE/REMOVE	
False Positive Suppression	✓
Threat Cases (Root Cause Analysis)	✓
Sophos Clean	✓
Synchronized Security Heartbeat	✓

Try it now for free

Register for a free 30-day evaluation at sophos.com/server

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

20-07-21 DS-EN (DD)

SYNCHROWORKS CONSULTING

SOPHOS