Intercept X for Server

Whether in the cloud or on premises, you need to protect the critical applications and data at the core of your organization. Intercept X for Server offers a comprehensive, defense-in-depth approach using deep learning malware detection, exploit prevention, anti-ransomware technology, application white listing, active adversary protection, and in-depth root cause analysis.

Highlights

‣ Discover and protect workloads on Microsoft Azure and Amazon Web Services, and S3 buckets on AWS

‣ Protect against ransomware on servers, including remote attacks from rogue endpoints

‣ Server Lockdown whitelists applications

‣ Block advanced hacking techniques and exploits

‣ Root cause analysis details the cause of attacks and infection path

‣ Synchronized Security shares threat, health, and security information across multiple Sophos products

‣ Simplified management from Sophos Central

Powerful server-specific protection

Intercept X for Server leverages a broad set of protections to stop zero-day attacks, exploits, and hackers. These protections prevent attacks from reaching servers in the first place, detect attacks before they run, or stop them and provide a thorough cleanup if they manage to evade protection. Its constantly updated artificial intelligence model is trained to look for suspicious attributes of potentially malicious code on servers. Plus, server-specific features such as Server Lockdown and Cloud Workload Discovery ensure that server configurations are safe.

On Microsoft Azure and Amazon Web Services, Intercept X for Server discovers and protects server workloads, and on AWS S3 buckets. By connecting Sophos Central with AWS and Azure, Intercept X for Server visually confirms that servers are protected, and makes management easier by displaying relevant information in Sophos Central.

Stop server-based ransomware

CryptoGuard defends against ransomware, working at the file system level to detect and intercept unsolicited file encryption, both on the server or from a remote endpoint connected to the server. WipeGuard similarly works to protect the master boot record from malicious encryption.

Sophos Intercept X for Server locks down your server with a single click, whitelisting only current applications to secure servers in a safe state, and prevent unauthorized applications from running. Sophos automatically scans the system and establishes an inventory (whitelist) of known good applications without the need for manual rule creation. Sophos creates an unbreakable bond between applications and associated files, such as DLLs, data files, and scripts needed for each application.

Disrupt attacks: Deny hackers access to servers

Vulnerabilities are appearing at an alarming rate, and patching servers without disrupting users can be challenging. Exploit attacks can be devastating and are often undetectable by traditional server protection technologies. Intercept X for Server is designed to stop even the most stubborn hacker from using exploit techniques to harvest credentials, whether they try to remain hidden and persistent, or move laterally, Intercept X is designed to stop them.

Root cause analysis

Intercept X for Server also includes detection and response technology to provide complete visibility so admins will know how an attack got in, where it went, what it touched, and what you should do next. Intercept X for Server provides this without an additional agent or management console.

Synchronized Security

Synchronized Security is a best of breed security system that enables your defenses to be as coordinated as the attacks they protect against. It combines an intuitive security platform with award-winning products that actively work together to block advanced threats to give you unparalleled protection.

Highlights of Intercept X for Server

PLATFORMS		Windows Server	✓
		Linux[1]	✓
		Public Cloud	✓
PREVENT	ATTACK SURFACE REDUCTION	Application Whitelisting [Server Lockdown]	✓
		Web Security	✓
		Windows Firewall Control	✓
		Download Reputation	✓
		Web Control (URL Blocking)	✓
		Peripheral Control (e.g., USB)	✓
		Application Control	✓
	BEFORE IT RUNS ON DEVICE	Deep Learning Malware Detection	✓
		Exploit Prevention	✓
		Anti-malware File Scanning	✓
		Live Protection	✓
		Pre-execution Behavior Analysis [HIPS]	✓
		Off-board scanning for VMs (ESXi and Hyper-V)[2]	✓
		Detect Potentially Unwanted Applications (PUA)	✓
		Data Loss Prevention	✓

1 All features available on Windows; selected features available on Linux
2 See License Guide for Sophos for Virtual Environments, ultra-thin agent deployment
3 For Windows Servers managed by Sophos Enterprise Console, CryptoGuard is
  available with the Endpoint Exploit Prevention [EXP] Add-on license
4 When used in conjunction with the Sophos XG Firewall

Easy to manage with Sophos Central

Managing your security from Sophos Central means you no longer need to deploy a management server to secure your systems. Sophos Central, hosted by Sophos, provides instant access with no console servers to set up. Sophos Central provides out-of-the-box policies for servers while also managing other Sophos products, including Sophos Intercept X, Mobile, Wireless, Email, and Web — all from a single pane of glass.

File Integrity Monitoring

Sophos provides default rules to monitor changes to critical Windows system files, with optional monitoring of additional locations and exclusions via policy.

DETECT	STOP RUNNING THREAT	Anti-Hacker/Active Adversary Mitigations	✓
		Ransomware File Protection [CryptoGuard] includes detection of attacks on the server from remote connected endpoints	✓
		Disk and Boot Record Protection [WipeGuard]	✓
		Malicious Traffic Detection	✓
RESPOND	INVESTIGATE AND REMOVE	Sophos Clean Automated Malware Removal	✓
		Root Cause Analysis	✓
MANAGE	CONTROL	Server-specific policy management	✓
		Update Cache and Message Relay	✓
		Automatic Scanning Exclusions	✓
		File Integrity Monitoring	✓
		Synchronized Application Control[4]	✓
	VISIBILITY	Azure Workload Discovery and Protection	✓
		AWS Workload and S3 bucket Discovery and Protection	✓
		AWS Map, multi-region visualization	✓
		Synchronized Security with Security Heartbeat™ [Enhanced threat protection, positive source identification, and automated isolation][4]	✓
		Windows Remote Desktop Services [user visibility]	✓
	SOPHOS CENTRAL	Cloud-based management, eliminating the need the install and maintain a separate server on premises, and managing security of servers in a single console with endpoints, mobile, email, wireless	✓
		Multi-factor authentication	✓
		Role-based administration	✓

aws partner network

Advanced Technology Partner

Security Competency
Public Sector Partner
Marketplace Seller

Azure

Google Cloud Platform

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

SOPHOS