SOPHOS
Cybersecurity made simple.

CLOUD READY

Intercept X for Server

无论是云端还是预置，您都需要保护企业核心的关键应用和数据。Intercept X for Server 利用深度学习恶意软件侦测、漏洞利用预防、防勒索软件技术、应用程序白名单、主动攻击防护和深度根本原因分析，提供全面深度防御方法。

主要优势

- 发现并保护 Microsoft Azure 和 Amazon Web Services 中的工作负荷
- 防范服务器上的勒索软件，包括恶意端点的远程攻击
- 服务器锁定白名单应用程序
- 阻止高级黑客技术和漏洞利用攻击
- 根本原因分析详细说明攻击原因和感染路径
- Synchronized Security 在多个 Sophos 产品之间共享威胁、运行状况和安全信息
- Sophos Central 简化管理
- 针对 Windows 和 Linux 系统的威胁防护

功能强大的服务器特定防护

Intercept X for Server 利用多种防护措施阻止零日攻击、漏洞利用攻击和黑客。首先，这些防护阻止攻击进入服务器，在运行前侦测攻击，或者如果攻击绕过防护，则阻止攻击并进行彻底清理。持续更新的人工智能模型经过训练，可以查找服务器上的潜在恶意代码的可疑属性。此外，服务器特定功能，如服务器锁定(Server Lockdown)和云负荷发现(Cloud Workload Discovery)，可以确保服务器配置安全。

Intercept X for Server 发现并保护云中的工作负荷，包括 Microsoft Azure 和 Amazon Web Services。将 Sophos Central 连接到 AWS 和 Azure 后，Intercept X for Server 在 Sophos Central 中显示相关信息向您确认服务器受保护，更加方便管理。

阻止基于服务器的勒索软件

CryptoGuard 防御勒索软件，在文件系统层面工作，以侦测和拦截服务器，或与服务器连接的远程端点上主动提供的文件加密。WipeGuard 同样可以保护主引导记录免受恶意加密。

Sophos Intercept X for Server 支持单击锁定服务器，将应用程序列入白名单以确保服务器安全，阻止未经授权的应用程序运行。Sophos 自动扫描系统，建立已知的好应用程序清单（白名单），无需手动创建规则。Sophos 在应用程序和关联文件（如 DLL、数据文件和脚本）之间创建不可打破的关联。

破坏攻击：拒绝黑客访问服务器

漏洞出现的速度令人警惕，要在不影响用户工作的情况下给服务器打补丁有困难。漏洞利用攻击可能带来巨大破坏，而传统的服务器保护技术通常侦测不到。Intercept X for Server 的目的是阻止最顽固的黑客利用漏洞利用攻击技术获取凭证，无论他们是尝试保持隐藏和持久，还是横向移动，Intercept X 都可以对其进行阻止。

根本原因分析

Intercept X for Server 还加入侦测和响应技术，使整个攻击过程完全可见，这样管理员就会知道攻击进入方式，到达的位置，接触内容，以及下一步应采取的措施。Intercept X for Server 无需额外代理或管理控制台即可实现此功能。

Synchronized Security

Synchronized Security 是业界同类的最佳安全系统，能按照要抵御的攻击去协调防御措施。直观化的安全平台和获奖的安全产品能够共同拦截高级网络威胁，给予您无与伦比的安全防护。

Sophos Central 易于管理

从 Sophos Central 管理安全意味着您无需部署服务器来确保系统安全。Sophos 的 Sophos Central 可即时访问，无需设置控制台服务器。Sophos Central 为服务器提供现成的政策，并管理其他 Sophos 产品，包括 Sophos Intercept X、Mobile、Wireless、Email 和 Web — 都是通过一个单一管理平台进行操作的。

Intercept X for Server 的产品亮点

操作系统平台		Windows Server	✓
		Linux[1]	✓
		Public Cloud (Microsoft Azure and Amazon AWS)	✓
预防	减少攻击表面	Application Whitelisting [Server Lockdown]	✓
		Web Security	✓
		Windows Firewall Control	✓
		Download Reputation	✓
		Web Control (URL Blocking)	✓
		Peripheral Control (e.g., USB)	✓
		Application Control	✓
	在设备上运行前	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	✓
侦测	阻止运行威胁	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	✓
回应	调查并移除	Sophos Clean Automated Malware Removal	✓
		Root Cause Analysis	✓
管理	控制	Server-specific policy management	✓
		Update Cache and Message Relay	✓
		Automatic Scanning Exclusions	✓
		Synchronized Application Control[4]	✓
	可见性	Azure Workload Discovery and Protection	✓
		AWS Workload 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	✓

1Windows 上提供所有功能；Linux 上提供选择的功能
2 参见虚拟环境、超瘦代理部署用 的Sophos 许可指南
3 对于 Sophos Enterprise Console 管理的 Windows 服务器，CryptoGuard 随 Endpoint Exploit Prevention (EXP) 附加程序许可证提供
4 与 Sophos XG Firewall 一同使用时

Azure

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

立即免费试用

30天免费试用
sophos.com/server。

中国销售（北京）
电话：400 650 6598
电子邮件：salescn@sophos.com

中国销售（上海）
电话：+86 21 3251 7160
电子邮件：salescn@sophos.com

中国销售（广州）
电话：+86 136 0241 6506
电子邮件：salescn@sophos.com

2018/6/28 DS-ZHCN (MP)

SOPHOS