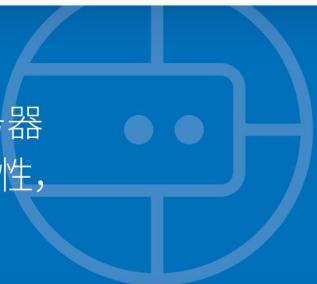


Intercept X Advanced for Server with EDR

无与伦比的服务器防护

Sophos Intercept X for Server 可以保障您的云、内部预置或混合服务器环境不受最新恶意软件威胁影响，为您提供无与伦比的企业资产可见性，让您精确控制服务器上可以运行的内容。



亮点

- 由深度学习驱动的高评价恶意软件防护
- 主动攻击、漏洞利用攻击和勒索软件防护
- 端点侦测与响应 (EDR) 提供资产可见性
- 发现并保护您的 AWS EC2 实例、S3 bucket 以及 Microsoft Azure 工作负荷
- 保护您的服务器配置不受未经授权变动的影响

一体式服务器防护

Intercept X for Server 的防护效果获得业内专家给出的最高评价，结合服务器专属的功能打造综合深度防御解决方案。拦截从未见过的恶意软件，阻止勒索软件攻击，防范危险的漏洞利用攻击技术，杜绝黑客。

在云中，您可以发现并保护您的 Amazon AWS EC2 实例和 Microsoft Azure 工作负荷，对自动缩放组 (Auto Scaling Groups) 和虚拟机 (VM) 实施一致政策。使用 VM 扩展脚本和 CloudFormation 模板，部署和设置工作既简单又快捷。

自动威胁侦测与响应

借助 Intercept X for Server，获得对服务器的无与伦比的可见性。搜寻侵入威胁，查看并精确控制运行中的应用程序，自动响应事件。

端点检测与响应 (EDR) 为您提供企业全部资产的可见性，这样您可以主动检测隐秘攻击，更好地理解安全事件的范围与影响，在短时间内自信地报告企业的安全状态。

将服务器版 Intercept X 和 Sophos XG Firewall 组合使用，可以隔离受威胁的服务器，阻止威胁横向传播，同时自动清理威胁，服务器上运行的应用程序的可见性达到 100%，阻止未知应用程序向外通信。

取得对服务器的控制权

服务器是您企业最重要的资产。利用 Intercept X for Server，您可以精确控制可以运行和不可以运行的应用程序，保证您的服务器配置的安全。

快速创建威胁防护、应用程序、外围设备和 Web 控制的政策，只需几次单击即可在部署中应用。还可以为需要的服务器分别配置策略。

Server Lockdown (服务器锁定) 可以一键锁定服务器配置，防止未经授权改动，这样只有您批准的应用程序可以运行 - 无需服务器停机。

简化管理和部署

Sophos Central 简化服务器的管理工作。从同一个屏幕可以访问政策管理、提醒和报告。Sophos Central 还提供默认策略和建议配置，确保您从一开始就获得最有效的保护。对于实体、虚拟、云和混合部署来说，许可政策和部署的代理相同。

The screenshot displays the Sophos Central interface with several key features highlighted:

- Left Sidebar:** Shows navigation sections like ANALYZE (Dashboard, Logs & Reports), MANAGE PROTECTION (Servers, Servers on AWS), and CONFIGURE (Policies, Settings, Protect Devices). A blue circle labeled **1** points to the "Server Protection" section in the ANALYZE menu.
- Top Header:** Shows the user is "Rohith's · Super Admin".
- Central Content:**
 - Threat Cases:** A table showing the most recent threat cases. One case is highlighted with a blue circle labeled **2**. The table includes columns for Time created, Priority, Name, User, and Device.
 - Servers Summary:** A circular chart showing 200 servers in total, with 175 Active (blue), 1 Inactive 2+ weeks (light blue), 23 Inactive 2+months (grey), and 1 Not Protected (red).
 - Servers on AWS:** A world map showing the distribution of AWS instances across regions, with numbers indicating the count in each region (e.g., 43 in North America, 41 in Europe, 36 in Asia).

1. 立刻检视最新案例、优先级、恶意软件类型和受影响的服务器*
2. 快速访问特定于服务器的政策、设置和部署选项
3. 断定受保护、未受保护或离线的服务器
4. 查看运行的 AWS 实例数量以及区域

*利用 EDR，您可以更进一步了解威胁案例，从 SophosLabs 获取最新恶意软件威胁情报

