

Sophos Workload Protection

工作负荷保护许可指南

SOPHOS
Cybersecurity delivered.

Intercept X for Server、XDR、Cloud Native Security 和 MTR 概述

由 Sophos Central 管理

功能	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	云原生安全	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
管理						
多种政策		✓	✓	✓	✓	✓
可控更新		✓	✓	✓	✓	✓
减少攻击面						
应用程序控制		✓	✓	✓	✓	✓
Peripheral Control		✓	✓	✓	✓	✓
Web 控制/基于类别的 URL 拦截		✓	✓	✓	✓	✓
应用程序白名单 (服务器锁定)		✓	✓	✓	✓	✓
Download Reputation	✓	✓	✓	✓	✓	✓
Web Security	✓	✓	✓	✓	✓	✓
在设备上运行之前						
深度学习恶意软件侦测	✓	✓	✓	✓	✓	✓
反恶意程式文件扫描	✓	✓	✓	✓	✓	✓
实时保护	✓	✓	✓	✓	✓	✓
执行前行为分析 (HIPS)	✓	✓	✓	✓	✓	✓
潜在不想要的应用程序 (PUA) 拦截	✓	✓	✓	✓	✓	✓
入侵防御系统 (IPS)	✓	✓	✓	✓	✓	✓
阻止威胁运行						
数据丢失预防		✓	✓	✓	✓	✓
运行时行为分析 (HIPS)	✓	✓	✓	✓	✓	✓
防恶意软件扫描接口 (AMSI)	✓	✓	✓	✓	✓	✓

功能	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	云原生安全	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
恶意流量监测 (MTD)	✓	✓	✓	✓	✓	✓
防漏洞利用攻击 (第 5 页详细信息)	✓	✓	✓	✓	✓	✓
活跃对手缓解 (第 5 页详细信息)	✓	✓	✓	✓	✓	✓
勒索软件文件保护 (CryptoGuard)	✓	✓	✓	✓	✓	✓
磁盘和引导记录保护 (WipeGuard)	✓	✓	✓	✓	✓	✓
Man-in-the-Browser 保护 (安全浏览)	✓	✓	✓	✓	✓	✓
Enhanced Application Lockdown	✓	✓	✓	✓	✓	✓
侦测						
Live Discover 实时发现 (跨资产 SQL 查询实现威胁追踪 & IT 安全操作保健)			✓	✓	✓	✓
SQL 查询库 (预先编写, 完全可自定义的查询)			✓	✓	✓	✓
快速访问, 磁盘数据存储 (最多 90 天)			✓	✓	✓	✓
跨产品数据来源, 如 Firewall、Email			✓	✓	✓	✓
按照优先级排列的侦测列表			✓	✓	✓	✓
Sophos Data Lake (云数据存储)			30 天	30 天	30 天	30 天
计划查询			✓	✓	✓	✓
容器运行时可见性和侦测			✓	✓	✓	✓
调查						
Threat Cases (Root Cause Analysis)		✓	✓	✓	✓	✓
Deep Learning Malware Analysis			✓	✓	✓	✓
Advanced On-demand SophosLabs Threat Intelligence			✓	✓	✓	✓
Forensic Data Export			✓	✓	✓	✓
人工智能引导调查			✓	✓	✓	✓

功能	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	云原生安全	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
解决						
Automated Malware Removal	✓	✓	✓	✓	✓	✓
Synchronized Security Heartbeat 同步安全心跳	✓	✓	✓	✓	✓	✓
Sophos Clean 清理方案	✓	✓	✓	✓	✓	✓
在线响应 (远程终端访问, 进行进一步调查和响应)			✓	✓	✓	✓
按需服务器隔离			✓	✓	✓	✓
Single-click “Clean and Block”			✓	✓	✓	✓
容器运行时可见性和侦测			✓	✓	✓	✓
控制						
同步应用程序控制 (应用程序可见性)	✓	✓	✓	✓	✓	✓
Update Cache and Message Relay	✓	✓	✓	✓	✓	✓
Automatic Scanning Exclusions	✓	✓	✓	✓	✓	✓
文件完整性监测			✓	✓	✓	✓
云环境						
云环境监测: AWS、Azure、GCP、Kubernetes、IaC 和 Docker Hub 注册表		每个提供商一个	每个提供商一个	无限制	每个提供商一个	每个提供商一个
安全监测 (CSPM 最佳做法规则)		每日扫描	每日扫描	排程、每日和按需扫描	每日扫描	每日扫描
资产安全		✓	✓	✓	✓	✓
高级搜索功能		✓	✓	✓	✓	✓
人工智能支持的异常侦测		✓	✓	✓	✓	✓
SophosLabs Intelix 恶意流量警示		✓	✓	✓	✓	✓
电子邮件提醒		✓	✓	✓	✓	✓
AWS 原生服务集成 (Amazon GuardDuty、AWS Security Hub、Amazon Inspector 等)		✓	✓	✓	✓	✓
Azure 原生服务集成 (Azure Sentinel 和 Advisor)		✓	✓	✓	✓	✓
Cloud Workload Protection: Sophos Intercept X Server 代理发现		✓	✓	✓	✓	✓
Cloud Workload Protection: 自动 Sophos Intercept X Server 代理移除		✓	✓	✓	✓	✓

功能	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	云原生安全	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
合规性政策与报告		CIS 基准	CIS 基准	CIS 基准、ISO 27001、EBU R 143、FEDRAMP、FIEC、GDPR、HIPAA、PCI DSS、SOC2、Sophos 最佳做法	CIS 基准	CIS 基准
定制政策				✓		
网络可视化		✓	✓	✓	✓	✓
IAM 可视化		✓	✓	✓	✓	✓
开支监测		✓	✓	✓	✓	✓
提醒管理集成 (Jira、ServiceNow、Slack、Teams、PagerDuty、Amazon SNS)		✓	✓	✓	✓	✓
SIEM 集成 (Splunk、Azure Sentinel)		✓	✓	✓	✓	✓
Rest API		✓	✓	✓	✓	✓
基础设施即代码模板扫描		✓	✓	✓	✓	✓
环境访问控制		✓	✓	✓	✓	✓
容器镜像扫描 (ECR、ACR、Docker Hub、API)		✓	✓	✓	✓	✓
托管服务						
24/7 全天候负责人推动的威胁追踪					✓	✓
安全运行状况检查					✓	✓
数据保留					✓	✓
活动报告					✓	✓
敌手侦测					✓	✓
威胁消除与补救					✓	✓
24/7 全天候无负责人威胁追踪						✓
威胁响应团队负责人						✓
直接电话支持						✓
主动安全状态管理						✓
勒索软件文件保护 (CryptoGuard)						✓

操作系统功能对比

功能	Windows	Linux*
管理		
多种政策	✓	✓
可控更新	✓	✓
减少攻击面		
Web Security	✓	
Download Reputation	✓	
Web 控制/基于类别的 URL 拦截	✓	
Peripheral Control	✓	
Application Control	✓	
应用程序白名单(服务器锁定)	✓	
在设备上运行之前		
深度学习恶意软件侦测	✓	✓
反恶意程式文件扫描	✓	✓
实时保护	✓	✓
执行前行为分析 (HIPS)	✓	
潜在不想要的应用程序 (PUA)拦截	✓	
入侵防御系统 (IPS)	✓	
阻止威胁运行		
数据丢失预防	✓	
运行时行为分析 (HIPS)	✓	
防恶意软件扫描接口 (AMSI)	✓	
恶意流量监测 (MTD)	✓	参加注释
防漏洞利用攻击(第 5 页详细信息)	✓	
活跃对手缓解(第 5 页详细信息)	✓	
勒索软件文件保护 (CryptoGuard)	✓	
磁盘和引导记录保护 (WipeGuard)	✓	
Man-in-the-Browser 保护 (安全浏览)	✓	
Enhanced Application Lockdown	✓	

功能	Windows	Linux*
侦测		
Live Discover 实时发现 (跨资产 SQL 查询实现威胁追踪 & IT 安全操作保健)	✓	✓
SQL 查询库 (预先编写, 完全可自定义的查询)	✓	✓
快速访问, 磁盘数据存储 (最多 90 天)	✓	✓
跨产品数据来源, 如 Firewall、Email	✓	✓
按照优先级排列的侦测列表	✓	✓
Sophos Data Lake (云数据存储)	✓	✓
计划查询	✓	✓
容器运行时可见性和侦测		✓
调查		
Threat Cases (Root Cause Analysis)	✓	
Deep Learning Malware Analysis	✓	
Advanced On-demand SophosLabs Threat Intelligence	✓	
Forensic Data Export	✓	
人工智能引导调查	✓	✓
解决		
Automated Malware Removal	✓	
Synchronized Security Heartbeat 同步安全心跳	✓	参加注释
Sophos Clean 清理方案	✓	
在线响应 (远程终端访问, 进行进一步调查和响应)	✓	✓
按需服务器隔离	✓	
Single-click “Clean and Block”	✓	
控制		
同步应用程序控制 (应用程序可见性)	✓	
Update Cache and Message Relay	✓	
Automatic Scanning Exclusions	✓	

功能	Windows	Linux*
文件完整性监测	✓	
托管服务		
24/7 全天候负责人推动的威胁追踪	✓	✓
安全运行状况检查	✓	✓
数据保留	✓	✓
活动报告	✓	✓
敌手侦测	✓	✓
威胁消除与补救	✓	✓
24/7 全天候无负责人威胁追踪	✓	✓
威胁响应团队负责人	✓	✓
直接电话支持	✓	✓
主动安全状态改进	✓	✓

*Linux 包括两个部署选项。1) Sophos Protection for Linux 部署, 可使用表格中注明的功能。2) Sophos Anti-Virus for Linux 部署包括: Anti-malware、Live Protection、Malicious Traffic Detection 和 Synchronized Security。请注意两个部署选项可以一起使用。

Sophos Protection 概览

随 Intercept X 和 Cloud Native Security 提供的工作负荷保护功能详细信息

产品特点	
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)	✓
基于堆栈的 ROP 缓解(调用方)	✓
基于分支的 ROP 缓解(硬件辅助)	✓
结构化异常句柄覆盖 (SEHOP)	✓
导入地址表过滤 (IAF)	✓
加载库	✓
反射 DLL 注入	✓
Shellcode	✓
VBScript 上帝模式	✓
Wow64	✓
Syscall	✓
Hollow 进程	✓
DLL 劫持	✓
Squiblydoo Applocker 绕过	✓
APC Protection (Double Pulsar / AtomBombing)	✓
进程权限提升	✓
动态 Shellcode 防护	✓
EFS 防护	✓

产品特点	
CTF 防护	✓
ApiSetGuard	✓
Active Adversary Mitigations	
凭据盗窃保护	✓
代码洞缓解	✓
Man-in-the-Browser 保护 (安全浏览)	✓
恶意流量监测	✓
Meterpreter Shell 检测	✓
反勒索软件	
勒索软件文件保护 (CryptoGuard)	✓
Automatic file recovery (CryptoGuard)	✓
Disk and Boot Record Protection (WipeGuard)	✓
应用程序锁定	
Web Browsers (including HTA)	✓
Web 浏览器插件	✓
Java	✓
媒体应用程序	✓
办公应用程序	✓
深度学习防护	
深度学习恶意软件检测	✓
深入学习阻止潜在不需要的应用程序 (PUA)	✓
误报禁止	✓
应对 调查 移除	
Threat Cases (Root Cause Analysis)	✓
Sophos Clean 清理方案	✓
Synchronized Security Heartbeat	✓

Managed Threat Response (MTR)

Sophos Managed Threat Response (托管式威胁回应, MTR) 提供由专家团队以全托管服务形式带来的 24/7 全天候威胁搜捕、检测和响应功能。MTR 客户还获得 Intercept X Advanced for Server with XDR。

Sophos MTR:Standard

24/7 全天候负责人推动的威胁搜捕

自动阻止或终止确认的恶意事件或活动 (强信号), 解放威胁搜捕人员, 开展负责人推动的威胁搜捕。此类威胁搜捕聚集并调查日常和相邻事件 (弱信号), 发现以前可能未检测到的新攻击迹象 (IoA) 和威胁迹象 (IoC)。

安全运行状况检查

保持 Sophos Central 产品--从 Intercept X Advanced for Server with XDR 开始--以最佳性能运行, 主动检查运行状况, 提出配置改进建议。

活动报告

案例活动汇总支持优先级排序和通信功能, 这样, 您的团队了解每个报告期内检测到的威胁, 以及采取的响应操作。

对手检测

大多数成功攻击依赖执行对监测工具来说合法的进程。我们的团队利用独有调查技术, 确定合法行为与攻击者运用的战术、技术和过程 (TTP) 之间的差异。

Sophos MTR:Advanced

包含所有标准功能, 以及:

24/7 全天候无负责人的威胁搜捕

运用数据学、威胁情报和资深威胁搜捕人员的直觉, 将公司档案、高价值资产和高风险用户结合在一起, 预测攻击者行为和识别新攻击迹象 (IoA)。

增强遥测

为威胁调查补充其他 Sophos Central 产品的遥测功能, 超越端点范围, 提供对手活动的全面信息。

主动状态改进

主动改进安全状态, 用规范性指导加固防御, 解决影响整体安全功能的配置和架构弱点。

威胁响应负责人

确认事件后, 提供威胁响应负责人, 直接与您的现场资源 (内部团队或外部合作伙伴) 协作, 直到清除活跃威胁。

直接电话支持

您的团队可以直接致电我们的安全运作中心 (SOC)。我们的 MTR 操作团队随时在线, 遍布全球 26 个地点的支持团队作为其坚强后盾。

资产发现

我们根据资产信息 (包括操作系统版本、应用程序、弱点) 确定托管和非托管资产, 在影响评估时提供宝贵信息, 进行威胁搜捕, 并提出主动状态改进建议。

中国 (大陆地区) 销售咨询
电子邮件: salescn@sophos.com