Intercept X、XDR 和 MTR 概述

由 Sophos Central 管理

SOPHOS
Cybersecurity evolved.

		功能	INTERCEPT X ESSENTIALS	INTERCEPT X wADVANCED	INTERCEPT X ADVANCED WITH XDR	INTERCEPT X WITH MTR STANDARD	INTERCEPT X WITH MTR ADVANCED
	管理	多种策略		✓	✓	✓	✓
		可控更新		✓	✓	✓	✓
防止	ATTACK SURFACE REDUCTION 减少攻击表面	Application Control		✓	✓	✓	✓
		Peripheral Control		✓	✓	✓	✓
		Web 控制/基于类别的 URL 拦截		✓	✓	✓	✓
		Download Reputation	✓	✓	✓	✓	✓
		Web Security	✓	✓	✓	✓	✓
	在设备上运行前	Deep Learning Malware Detection	✓	✓	✓	✓	✓
		Anti-Malware File Scanning	✓	✓	✓	✓	✓
		Live Protection	✓	✓	✓	✓	✓
		Pre-execution Behavior Analysis (HIPS)	✓	✓	✓	✓	✓
		Potentially Unwanted Application (PUA) Blocking	✓	✓	✓	✓	✓
		入侵防御系统 (IPS)	✓	✓	✓	✓	✓
	阻止威胁运行	Data Loss Prevention	✓	✓	✓	✓	✓
		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)	✓	✓	✓	✓	✓
		防漏洞攻击 (第 5 页详细信息)	✓	✓	✓	✓	✓
		活跃对手减轻 (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	✓	✓	✓	✓	✓

下页继续

Intercept X、XDR 和 MTR 概述

由 Sophos Central 管理（继续）

SOPHOS
Cybersecurity evolved.

		功能	INTERCEPT X ESSENTIALS	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH XDR	INTERCEPT X WITH MTR STANDARD	INTERCEPT X WITH MTR ADVANCED
侦测和调查	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			✓	✓	✓
		跨产品查询			✓	✓	✓
		Sophos Data Lake（云数据存储）			30 天	30 天	30 天
		计划查询			✓	✓	✓
	调查	Threat Cases (Root Cause Analysis)		✓	✓	✓	✓
		Deep Learning Malware Analysis			✓	✓	✓
		Advanced On-demand SophosLabs Threat Intelligence			✓	✓	✓
		Forensic Data Export			✓	✓	✓
响应	解决	Automated Malware Removal	✓	✓	✓	✓	✓
		Synchronized Security Heartbeat	✓	✓	✓	✓	✓
		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）			✓	✓	✓
		On-demand Endpoint Isolation			✓	✓	✓
		Single-click “Clean and Block”			✓	✓	✓
托管服务	人为领导的威胁追踪和响应	24/7 全天候负责人推动的威胁搜捕				✓	✓
		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					✓

Intercept X、XDR 和 MTR 概述

操作系统对比

		功能	WINDOWS	macOS
防止	ATTACK SURFACE REDUCTION 减少攻击表面	Web Security	✓	✓
		Download Reputation	✓	
		Web 控制/基于类别的 URL 拦截	✓	✓
		Peripheral Control	✓	✓
		Application Control	✓	✓
	在设备上运行前	Deep Learning Malware Detection	✓	
		Anti-Malware File Scanning	✓	✓
		Live Protection	✓	✓
		Pre-execution Behavior Analysis (HIPS)	✓	
		Potentially Unwanted Application (PUA) Blocking	✓	✓
		入侵防御系统 (IPS)	✓	
	阻止运行的威胁	数据丢失保护	✓	
		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)	✓	✓
		防漏洞攻击 (第 5 页详细信息)	✓	
		活跃对手减轻 (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	✓	

下页继续

Intercept X、XDR 和 MTR 概述

操作系统对比（继续）

		功能	WINDOWS	macOS
侦测和调查	侦测	在线发现（跨资产 SQL 查询，实现威胁追踪和 IT 安全运行状况）	✓	✓
		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）	✓	仅限实时数据
		跨产品数据来源，如 Firewall、Email	✓	✓
		跨产品查询	✓	✓
		Sophos Data Lake（云数据存储）	30 天	30 天
		排程查询	✓	✓
	调查	Threat Cases (Root Cause Analysis)	✓	✓
		Deep Learning Malware Analysis	✓	
		Advanced On-demand SophosLabs Threat Intelligence	✓	
		Forensic Data Export	✓	
响应	纠正	恶意程式自动移除	✓	✓
		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）	✓	✓
		On-demand Endpoint Isolation	✓	
		Single-click “Clean and Block”	✓	✓
托管服务	人为领导的威胁追踪和响应	24/7 全天候负责人推动的威胁搜捕	✓	✓
		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	✓	✓

Sophos Intercept X 功能

Intercept X 包含的功能详细信息

SOPHOS
Cybersecurity evolved.

	功能	
EXPLOIT PREVENTION 漏洞利用防御	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 减轻（调用方）	✓
	基于分支的 ROP 减轻（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 保护 (Double Pulsar / AtomBombing)	✓
	进程权限提升	✓
	动态 Shellcode 防护	✓
	EFS 防护	✓
	CTF 防护	✓
	ApiSetGuard	✓
活跃对手减轻	凭据盗窃保护	✓
	代码洞减轻	✓
	Man-in-the-Browser 保护（安全浏览）	✓
	恶意流量监测	✓
	Meterpreter Shell 检测	✓

	功能	
反勒索软件	勒索软件文件保护 (CryptoGuard)	✓
	Automatic file recovery (CryptoGuard)	✓
	Disk and Boot Record Protection (WipeGuard)	✓
APPLICATION LOCKDOWN 应用程序锁定	Web 浏览器（包括 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	深度学习恶意软件侦测	✓
	深入学习阻止潜在不需要的应用程序 (PUA)	✓
	误报禁止	✓
响应 调查 移除	Threat Cases (Root Cause Analysis)	✓
	Sophos Clean 清理方案	✓
	Synchronized Security Heartbeat	✓

托管威胁响应 (MTR)

SOPHOS
Cybersecurity evolved.

Sophos 托管威胁响应 (MTR) 提供由专家团队以全托管服务形式带来的 24/7 全天候威胁追踪、侦测和响应功能。MTR 客户还接收 Intercept X Advanced with EDR。

Sophos MTR：Standard

全天候专人引导的威胁搜寻

自动阻挡或终止经确认的恶意人为对象或活动 (强讯号)，让威胁处理专家有时间进行人工引导的威胁搜寻。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 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侦测到的威胁，以及采取的响应操作。

对手侦测

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 Standard 版本功能，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、漏洞) 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。