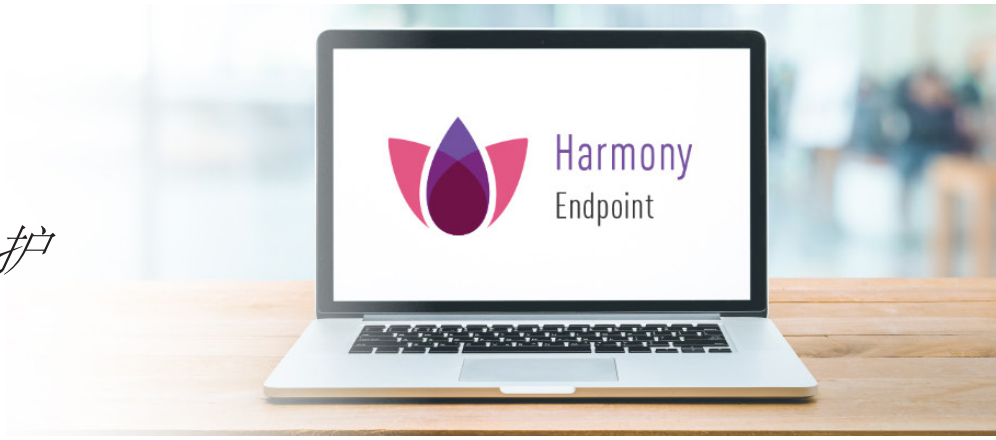
Check Point
SOFTWARE TECHNOLOGIES LTD

Harmony Endpoint

您所需的一切终端保护



Harmony Endpoint 是一款完整的终端安全解决方案，专用于帮助远程办公人员在目前日渐复杂的威胁环境中保持安全。这款解决方案可以防止最迫在眉睫的终端威胁，比如勒索软件、钓鱼攻击或偷渡式恶意软件，同时通过自主检测与响应，快速、最大限度地降低入侵影响。

如此一来，组织只需一款高效且富有成本效益的解决方案即可获得所需的有力终端保护。

主要产品优势

全面终端保护：防止最迫在眉睫的终端威胁

加快恢复速度：自动执行 90% 的攻击检测、调查和修复任务

降低总拥有成本：一款高效且富有成本效益的解决方案为您提供所需的一切终端保护

独特的产品功能

高级行为分析和机器学习算法在恶意软件造成损害之前将其关闭

高捕获率和低误报，确保安全效能和有效防护

自动取证数据分析，提供有关威胁的详细洞察

全面攻击防护和修复，快速恢复任何受感染的系统

市场领先的终端安全解决方案

Harmony Endpoint 被 AV-TEST 评为企业终端保护领域的顶级产品

了解更多

Forrester Wave 将 Check Point 评为终端安全领导者

了解更多

Check Point Harmony Endpoint 在 NSS Labs 2020 年高级终端保护测试中获得 AA 产品评级

了解更多

咨询订购：400-010-8885

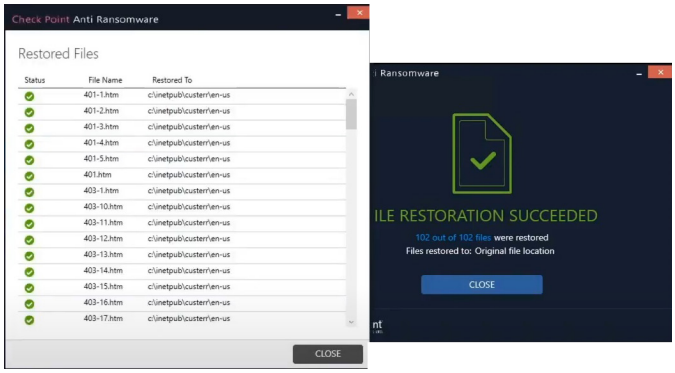
运作方式

全面终端保护

防止最迫在眉睫的终端威胁

- **拦截**来自 Web 浏览或电子邮件附件的**恶意软件**以免其侵入终端，而不会对用户生产力造成任何影响。用户通过电子邮件收到的或者通过 Web 浏览器下载的所有文件都将发送到威胁仿真沙盒进行恶意软件检测。另外，这款解决方案还可利用威胁剥离进程 (内容清除和重建技术) 对这些文件进行净化，在毫秒间交付安全、干净的内容。

- 在脱机模式也可**通过即时全面的修复获得运行时保护，防范勒索软件、恶意软件和无文件攻击。**一旦检测到异常或恶意行为，终端行为守卫就会拦截并修复整个攻击链，而不留任何恶意攻击痕迹。反勒索软件可以识别加密文件或尝试入侵 OS 备份等勒索软件行为，并自动安全恢复被勒索软件加密的文件。Harmony Endpoint 使用仅 Check Point 签名进程可以访问的机器本地独有的保管空间。如果恶意软件试图执行影子复制删除，机器也不会丢失任何数据。



- **钓鱼防护** - 借助 Zero-Phishing® 技术实时识别并阻止使用钓鱼网站，防止凭据盗窃。如果经检测发现网站是恶意网站，将阻止用户输入凭据。Zero-phishing® 甚至还可以防范之前未知的钓鱼网站和企业凭据重复使用。

业内最佳的已知和零日恶意软件捕获率

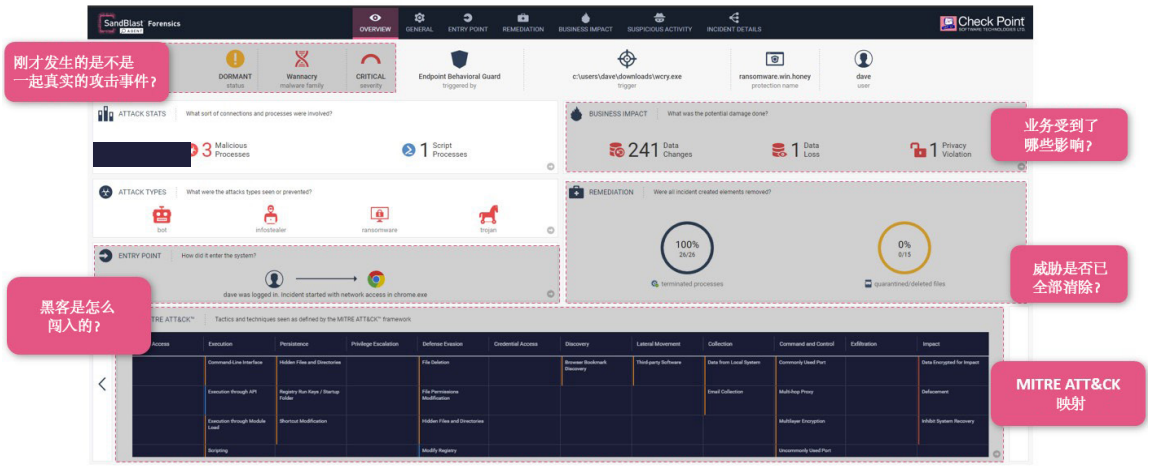
根据 2020 年 AV-TEST 企业终端保护和 NSS 高级终端保护实验室测试的结果，Harmony Endpoint 是公认的行业领导者。Harmony Endpoint 采用 60 多个威胁防护引擎，并搭载全球最强大的威胁情报平台 Check Point ThreatCloud™，可以提供市面上最高的威胁捕获率。

加快恢复速度

自动执行 90% 的攻击检测、调查和修复任务

- **自动化攻击控制和修复:** 唯一一款可自动、全面修复整个网络杀伤链的终端保护解决方案。检测到攻击后，受感染设备会被自动隔离以防止横向感染移动，并恢复至安全状态。

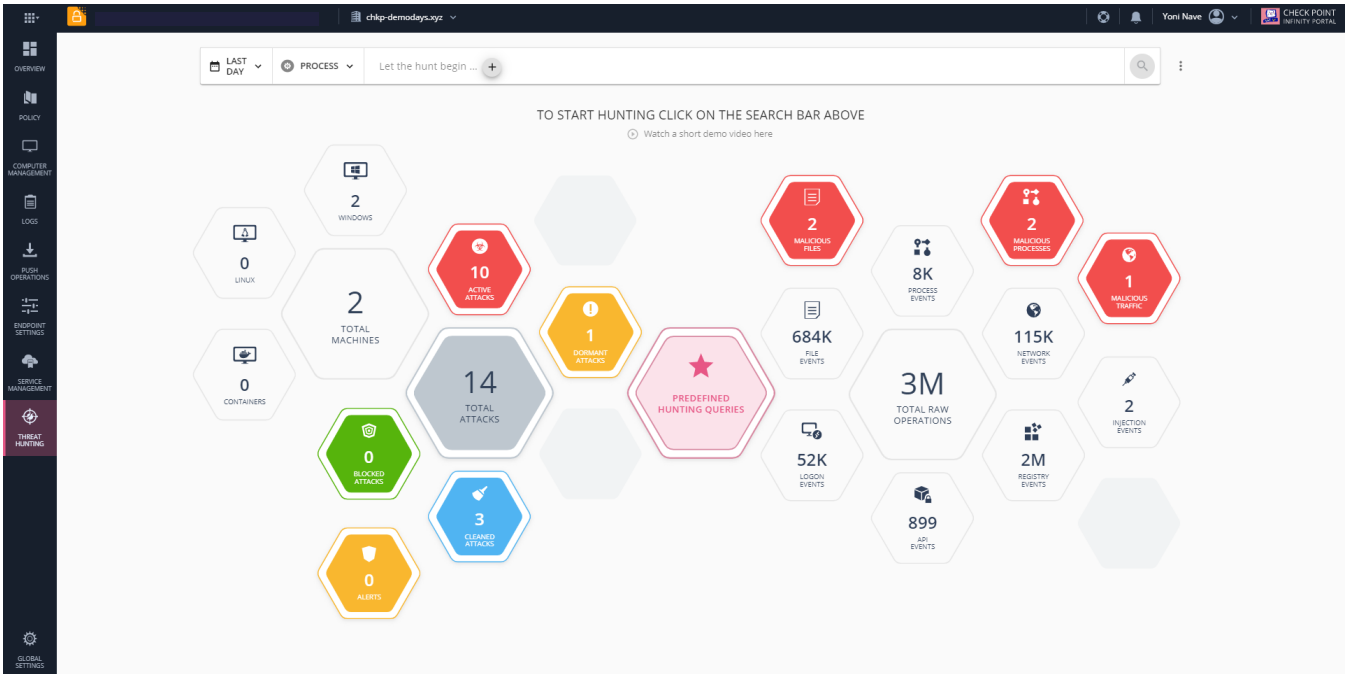
- **自动生成取证报告:** 让您详细了解受影响资产、攻击流以及与 MITRE ATT&CK™ 框架的关联。取证功能可以自动监控和记录终端事件，包括受影响文件、启动的进程、系统注册表变化以及网络活动，并创建详细的取证报告。强大的攻击诊断和可见性有助于采取补救措施，帮助系统管理员和事件响应团队高效地诊断和解决攻击。



Harmony Endpoint 取证报告

> *“使用 Check Point Harmony Endpoint 的最大优势是，我们无需担心对我们环境发起的勒索软件攻击。它可以让我们放心无忧，而这对于我们而言至关重要。我们知道它就在守护着我们的数据的安全。”*
>
> IMC Companies 首席信息安全官 David Ulloa

- **威胁搜寻:** 基于企业范围的可见性, 以及 ThreatCloud™ 从数亿传感器收集的全球共享威胁情报。通过威胁搜寻功能, 您可以设置查询或使用预定义查询识别或深入挖掘可疑事件, 并采取手动修复操作。



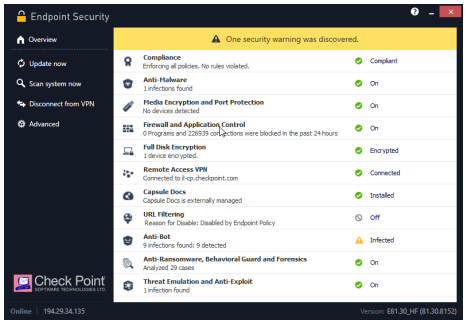
Harmony Endpoint - 威胁搜寻

> *"自从我们部署了 Harmony Endpoint, 将近一年内都没有发生过一起高级恶意软件或勒索软件攻击事件。"*
>
> Mississippi Secretary of State 首席技术官 Russell Walker

最佳总拥有成本

一款高效且富有成本效益的解决方案为您提供所需的一切终端保护

可提供 EPP、EDR、VPN、NGAV、数据和 Web 浏览保护的**单个统一代理**，帮助您的组织简化流程，并降低总拥有成本。



极为灵活，满足您的特定安全和合规要求。

- Harmony Endpoint 托管于本地或通过云服务托管，提供强大易用的功能并且支持快速部署，可以满足您的要求
- 支持 Windows、macOS 和 Linux 操作系统
- VDI 功能 (在远程服务器上的桌面实例仿真) ，支持 VMWare Horizon、Citrix PVS/MCS
- 近期更新的 Harmony Endpoint 安装程序支持无缝升级和回滚，对最终用户而言，无需重启设备，也不会遭受任何中断。
- 开发人员保护支持 - 帮助保护开发人员，无需集成持续集成/持续交付 (CI/CD) 或者集成开发环境 (IDE)。

基于 Check Point Infinity 构建而成，Check Point Infinity 是首个整合式安全架构，旨在解决连通需求增长和安全性不足所带来的复杂问题，跨网络、云、终端、移动设备和物联网提供全面保护和威胁情报。

CHECK POINT INFINITY

> *"Check Point Harmony Endpoint 是唯一一款高级终端保护解决方案。对我们而言，Harmony Endpoint 是最适合的高级终端保护解决方案。我们很快就在全球组织中部署了这款解决方案。管理控制台有一个非常直观的用户界面，使用起来非常简单。"*
>
> 大型全球基础设施企业高级安全分析师

技术规格

HARMONY ENDPOINT 套件	
套件	• **数据保护** – 包含全磁盘加密和可移动介质加密，包括访问控制和端口保护 • **Harmony Endpoint 基础版** – 包含反恶意软件、反勒索软件、反零日钓鱼攻击、高级威胁防护以及终端检测和响应 (EDR) • **Harmony Endpoint 高级版** – 包含 Harmony Endpoint 基础版，以及威胁仿真和威胁剥离 • **Harmony Endpoint 完整版** – 包含 Harmony Endpoint 高级版，以及数据安全（全磁盘和介质加密） **注：终端合规性**在所有套件中均有提供
操作系统	
操作系统	• Windows 工作站 7、8 和 10 • Windows 服务器 2008 R2、2012、2012 R2、2016 • MacOS Sierra 10.12.6、MacOS High Sierra 10.13.4（威胁仿真、威胁剥离、反勒索软件、Chrome for Mac 浏览器扩展）
跨电子邮件和 Web 进行内容清除和重建 (CDR)	
威胁剥离	移除可被恶意利用的内容，重建文件以消除潜在威胁，并在几秒内向用户提供处理后的安全内容
威胁仿真	• 借助威胁沙盒功能检测并拦截电子邮件附件、已下载文件以及电子邮件内文件的 URL 中发现的未知恶意软件和针对性攻击。 • 跨多种 Windows 操作系统环境为各种不同类型的文件（包括 MS Office、Adobe PDF、Java、Flash、可执行文件和存档等）提供保护。 • 发现 SSL 和 TLS 加密通信中隐藏的威胁。
集中化管理	
云和 本地管理	• Harmony 服务（以 Check Point 云为主机） • Harmony 设备（以本地网络为主机）
NGAV：运行时检测和保护	
反勒索软件	• 威胁防护 - 持续监控勒索软件行为，并识别非法文件加密和无签名情况。 • 检测与隔离 - 通过取证分析识别勒索软件攻击的所有元素，然后予以隔离。 • 数据恢复 - 自动从快照恢复加密文件，确保完整业务连续性。
防漏洞利用	• 提供保护措施，防范旨在侵入合法应用程序的基于漏洞利用的攻击，确保这些漏洞不会被恶意利用。 • 通过在运行时识别可疑的内存操作来检测漏洞利用。 • 关闭检测到的遭恶意利用的进程，修复整个攻击链
行为守卫	• 根据恶意软件的实时行为自适应地检测和阻止其突变。 • 基于最小进程执行树相似性，实时识别、分类和阻止恶意软件突变。
Web 保护	
零日钓鱼	• 实时防御未知的钓鱼网站 • 对需要私人信息的网站中的可疑元素进行静态和启发式检测
公司凭证保护	检测外部网站上的企业凭据重复使用
URL 过滤	• 轻量级浏览器插件，实时允许/阻止访问网站 • 为组织场所内外的用户执行组织安全互联网策略，执行法规合规，提高组织生产力 • 提供 HTTPS 流量的完整可见性
威胁搜寻	
威胁搜寻	收集终端上的所有原始事件和检测到的事件，支持高级查询、深入挖掘和切换，主动进行威胁搜寻并深入调查事件

为何选择 Harmony Endpoint?

现如今, 终端安全在赋能远程办公人员方面的作用日益重要。鉴于 70% 的网络攻击都始于终端, 提供最高安全级别的全面终端保护对于避免安全漏洞攻击和数据泄露至关重要。

Harmony Endpoint 是一款完整的终端安全解决方案, 专用于帮助远程办公人员在目前日渐复杂的威胁环境中保持安全。这款解决方案可以防止最迫在眉睫的终端威胁, 比如勒索软件、钓鱼攻击或偷渡式恶意软件, 同时通过自主检测与响应快速、最大限度地降低入侵影响。

如此一来, 组织只需一款高效且富有成本效益的解决方案即可获得所需的有力终端保护。

Harmony Endpoint 是业内首个专门针对用户、设备和访问打造的统一安全解决方案 Check Point Harmony 产品套件的一部分。Harmony 集六款产品于一身, 可以为所有人提供毫无漏洞的卓越安全性和简便性。它不仅能保护设备和互联网连接免受最复杂的攻击, 还可确保对企业应用程序的零信任访问, 所有这些只需一款易于使用、管理和购买的解决方案即可实现。

了解更多: https://www.checkpoint.com/products/advanced-endpoint-protection/