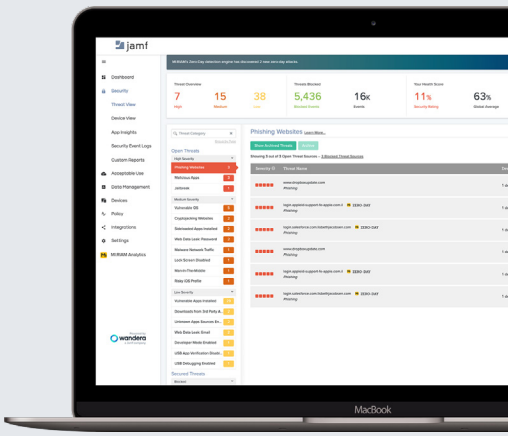
jamf

JAMF THREAT DEFENSE

保护设备、用户和应用程序免受网络威胁



Jamf Threat Defense 提供在设备和网络中运行的云交付安全性

强大的终端安全性

Threat Defense 检测并修复最广泛的终端威胁，包括设备漏洞、恶意软件和有风险的应用程序。持续进行全面的风险评估，以识别威胁，从而实时强制执行安全策略。

Network Defenses 保护用户和数据

借助网络内防御，在攻击开始之前加以制止。内容保护屏蔽恶意网站，包括那些前所未见、设计用于捕获业务凭据的零日网络钓鱼网站。此外，Threat Defense 通过阻断与风险网站的连接，防止命令与控制，以及数据泄漏。一旦检测到中间人攻击，就会自动对连接进行保护。

自适应访问您的应用程序

仅允许安全、可信的设备访问业务应用程序，以加强您的安全态势。Threat Defense 持续监控广泛的遥测和相关输入，可用于在终端遭到破解或者处于高风险状态时防止对应用程序的访问。自适应访问策略可以通过零信任网络访问解决方案，或者 Jamf 的管理解决方案 Jamf Pro 在本地强制执行。

jamf

全面的威胁检测和预防

零日网络保护

Threat Defense 可以识别并阻止甚至是最复杂的网络攻击，包括零日网络钓鱼攻击企图、命令和控制通信以及加密劫持。该服务适用于任何应用程序，包括网络浏览器、电子邮件、社交媒体和短信。

实时风险评估

Threat Defense 持续评估终端风险，从有漏洞的操作系统到恶意配置文件，让组织能够迅速识别不合规的设备，并强制执行真正的零信任访问策略。

详细的应用程序分析洞察

Threat Defense 提供先进的应用程序情报，可用于应用程序审查工作流程和安全调查。为每个应用程序提供风险分数和详细的报告，其中列出给用户和组织数据带来风险的权限和嵌入的 URL。

动态数据加密

Threat Defense 使用实时加密，可防止遭破解的 Wi-Fi 基础设施暴露敏感数据。该服务在后台静默运行，不需要任何用户交互。

领先的安全特性与功能

永远在线的终端防御

Threat Defense 使用终端应用程序在破解事件发生之前识别恶意软件、有漏洞的配置和有风险的连接，以保护移动工作人员和设备。

实时报告和策略控制

统一的策略引擎，让管理员能够快速配置安全策略并立即强制实施，从而可以即时地对政策进行调整和定制。可以在 Threat Defense 门户中查看详细的报告，也可以通过易于使用的集成导出到第三方工具。

条件式访问策略

当风险阈值超过预定义的值时，阻止对业务应用程序的访问。条件式访问策略可以在 Threat Defense 网络中或者通过与 Jamf 或身份提供商的集成在本地强制实施。

统一的操作和管理

Threat Defense 直接与管理基础设施集成，让该服务能够迅速部署到托管的设备。这一集成还在报告中添加人类可读的名称，为 ThreatOps 操作简化事件监测和威胁发现。

Jamf Threat Defense 可与您现有的 IT 服务和技术无缝搭配运行。

与 Microsoft、Google、Cisco 等公司产品的深度集成可帮助您扩展自己现有技术栈的价值。

jamf

www.jamf.com

如需了解 Threat Defense 如何保护用户、移动设备和组织数据的详细信息，请访问 jamf.com