Windows 终端安全防护

终端安全解决方案

基于检测的端点安全解决方案，如NGAV、EPP和EDR/XDR，足以阻止已知的、基于文件的网络攻击。但是，每天的新闻头条都在提供证据，证明它们无法阻止更复杂、无法检测到的威胁，比如零日攻击，以及勒索软件和供应链攻击中使用的多态、无文件、内存中的威胁。

30%的运行时内存安全缺口

最根本的问题是NGAV需要以前攻击的恶意文件签名来检测恶意文件并对其做出响应。EPP和EDR/XDR需要基于先前攻击的行为模式来检测和响应它们。

对于基于检测的解决方案来说，必须将新攻击与以前的攻击进行匹配，这是一个关键的安全漏洞。这意味着它们不能可靠地阻止隐藏在运行时内存中的未知攻击或无法检测到的攻击，这些工具无法有效扫描。为了量化这一差距，摩菲斯分析了Picus实验室2023年红色报告中的数据，该报告检查了50万个恶意软件样本，以及来自5000多家摩菲斯客户、900万个端点和1万多起日常事件的数据。基于检测的解决方案努力阻止十大MITRE攻击和攻击技术中的至少三种，这是一个关键的30%的安全漏洞。

核心能力

- 自动移动目标防御技术保护运行时内存免受未知和无法检测的攻击
- 增强的反勒索软件保护，从初始访问到加密/影响，全面预防攻击阶段
- 持续的应用程序库存可见性和基于风险的漏洞优先级

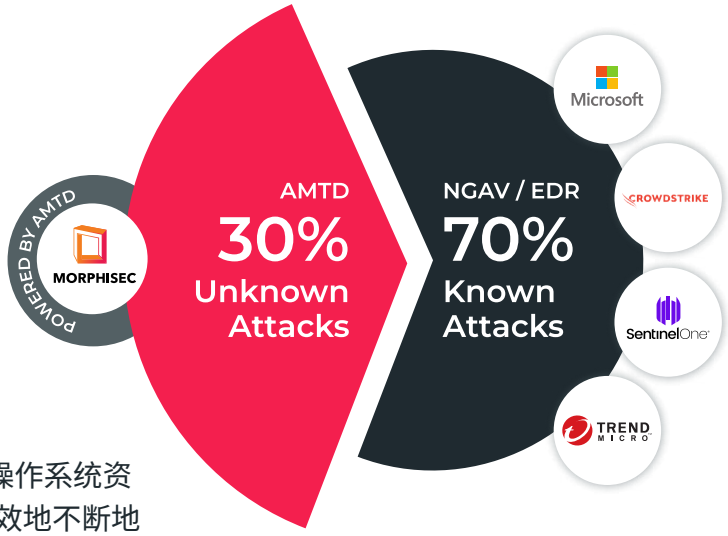
优势

- 阻止规避NGAV、EPP和EDR/XDR的高级攻击
- 降低成本，提高运营效率。超轻量级6MB代理无需额外人员即可大幅削减误报警报并提高安全性。
- 将旧式工作站保护回Windows 7。无需互联网连接或停机即可部署或维护。
- 无需重启即可快速轻松地部署易于使用、云管理的超轻量级代理。无需配置即可保护物理和虚拟(VDI)终端。
- 防止因安全违规和合规失败而导致的罚款、诉讼和品牌损害

结论

- TruGreen将误报率降低了95%，并将成本降低了三分之二
- Paccar：“ 摩菲斯填补了我们XDR解决方案的空白，以最少的占用空间和极少的误报实现真正的深度防御策略。”

自动移动目标防御：终端安全的下一步发展



与基于检测的解决方案不同，虹科摩菲斯的专利AMTD技术不需要签名或行为模式来检测和阻止威胁。

相反，虹科摩菲斯通过在运行时内存中创建威胁参与者无法穿透的动态攻击面来主动阻止攻击。

AMTD在运行时定期对应用程序内存、API和其他操作系统资源进行变形(随机化)，将诱饵留在它们的位置上。它有效地不断地将门移动到房子里，隐藏真正的门，并在它们的位置上留下假门。

任何试图打开假门的代码都会被捕获进行取证分析，并触发警报通知。即使威胁参与者可以找到真正的门——当他们返回时，它也不会在那里，阻止对手在同一端点上重复使用攻击，更不用说在其他端点上了。

> Gartner将AMTD称为“网络的未来”，并说：“自动移动目标防御是一种新兴的改变游戏规则的技术，旨在提高网络防御能力。”
>
> Gartner

必须将NGAV、EPP和EDR/XDR等概率技术设置为高灵敏度，以检测隐蔽的、躲避的网络攻击，从而生成压倒性的虚假警报和分析师分类。虹科摩菲斯可以确定性地阻止攻击，因此您可以降低现有解决方案的敏感度，提高运营效率。

> 在我们之前的安全平台上，我们过去每天会收到多达50个警报。现在，我们可能会得到一到两个。
>
> TRUGREEN

虹科摩菲斯不监控或收集个人数据，并保护物理和虚拟终端，包括VMware Horizon View和Citrix。
我们与Microsoft Defender(反病毒、计划1或计划2)无缝集成，或作为其他终端安全解决方案的配套产品。

虹科摩菲斯系统要求

支持的微软操作系统：Windows 7 SP1(32/64位)、Windows 7 Embedded Standard+Embedded Standard SP1+ Windows Embedded POS Ready 7、Windows 7、Windows 8+8.1、Windows 10、Windows 11、Windows IoT

磁盘空间：最小30MB

关于虹科摩菲斯

虹科摩菲斯针对最高级的威胁提供预防优先的安全，以阻止从终端到云的其他攻击。虹科摩菲斯的软件由自动移动目标防御(AMTD)技术提供支持，这是网络安全的下一步发展。AMTD可阻止勒索软件、供应链攻击、零日攻击和其他高级攻击。Gartner研究表明，AMTD是网络的未来。AMTD提供超轻量级深度防御安全层，以增强NGAV、EPP和EDR/XDR等解决方案。我们在不影响性能或不需要额外工作人员的情况下，针对无法检测的网络攻击缩小他们的运行时内存安全漏洞。超过5,000家组织信任虹科摩菲斯来保护900万台Windows和Linux服务器、工作负载和终端。虹科摩菲斯每天可以阻止联想、摩托罗拉、TruGreen、Covenant Health、公民医疗中心等数千次高级攻击。

HongKe 虹科

www.hocyber.com
hocyber@hkaco.com
T(+86)400-999-3848

M(+86)135 3349 1614
各分部：广州 | 成都 | 上海 | 苏州 | 西安 | 北京 | 台湾 | 香港| 日本 | 韩国 | 新加坡 | 美国硅谷

联系我们