HongKe 虹科

MORPHISEC
Breach Prevention Made Easy

为什么终端检测和响应不足以阻止勒索软件？

警报过载

为了阻止勒索软件、供应链攻击、数据窃取和其他高级攻击，终端检测和响应（EDR）以及扩展检测和响应（XDR）解决方案必须配置为最高警报设置，从而产生大量虚假警报。这拖慢了你的系统、应用程序，团队处理 IT 支持票证和威胁分析的速度。

如果你能消除虚假的警报，会怎么样？

高EDR
警报模式

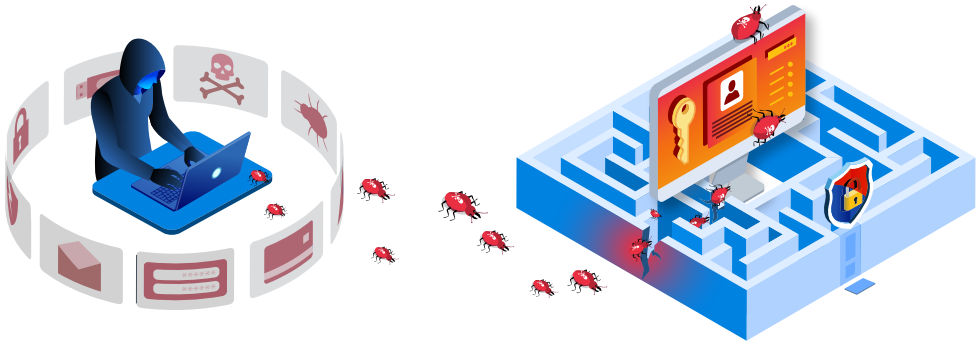
结果是？

- 系统退化
- **40%+** 假阳性
- **31%** 未调查的警报
- **83%** 的公司有警报疲劳症

低EDR
警报模式

结果是？

- ✕ 威胁正在绕过你的网络安全防御



被动，而不是主动

如果你使用标准的EDR/XDR警报设置，但是没有任何“哔哔哔”的报警声，这可能比太多的警报更糟糕。(这可能意味着你的EDR失效了。)EDR是为反应性检测和响应而设计的，而不是主动防御。但是，如果你可以使用标准的EDR设置而不漏掉高级攻击呢？领先的分析专家说，移动目标防御(MTD)以一流的预防措施增强了EDR的有效性，实现了真正的深度防御战略。

资源占用

EDR/XDR和管理检测和响应(MDR)需要经过检测、响应和分析培训的昂贵的员工。Ponemon研究显示，团队将25%的时间花在错误警报上。没有错误警报的团队通常设置过低，有可能面临勒索软件、品牌损害和诉讼的风险。考虑由管理服务提供商提供MDR和EDR服务，结合MTD来阻止绕过EDR的高级威胁。

挡不住最坏的人

EDR可以阻止具有已知特征和行为的攻击，但测试表明，大多数EDR对内存和无文件或运行时攻击无效。科学期刊出版商MDPI 使用Cobalt Strike MITRE ATT&CK战术测试了十几个顶级EDR解决方案—EDR显然需要增强来阻止高级攻击。许多甚至没有触发警报，除非处于极端激进的模式下，这会导致警报过载。顶级分析师说，MTD是一个改变游戏规则的工具，可以消除这个问题。

EDR	警报设置	CPL	HTA	EXE	DLL
Bitdefender	Standard	BLOCK / A	BLOCK / A	FAIL / NA	BLOCK / A
vmware	Standard	FAIL / A	FAIL / A	FAIL / NA	FAIL / NA
CROWDSTRIKE	Standard	FAIL / NA	FAIL / NA	BLOCK / A	FAIL / NA
CYLANCE	Standard	BLOCK / NA	BLOCK / NA	BLOCK / A	FAIL / NA
F-Secure	Standard	FAIL / A	FAIL / A	FAIL / NA	BLOCK / A
FORTINET	Standard	FAIL / NA	FAIL / NA	FAIL / NA	FAIL / NA
McAfee	Standard	BLOCK / A	FAIL / A	FAIL / NA	FAIL / NA
Microsoft Defender	Standard	FAIL / A	BLOCK / A	BLOCK / A	FAIL / NA
SentinelOne	Standard	FAIL / NA	FAIL / NA	FAIL / NA	BLOCK / A
SentinelOne*	Ultra Aggressive	BLOCK / A	BLOCK / A	BLOCK / A	BLOCK / A
SOPHOS	Standard	BLOCK / A	BLOCK / A	FAIL / NA	FAIL / A
Symantec	Standard	FAIL / A	BLOCK / A	FAIL / A	FAIL / A
TREND MICRO	Standard	FAIL / LA	FAIL / LA	FAIL / NA	FAIL / NA

A = Alert LA = Low Alert NA = No Alert

*STAR High Alert setting, high false positive alerts, PowerShell activity issues

MDPI Jan 2022 Report v3

狡猾的恶意软件

勒索软件的对手是大型企业。他们采用多态（转移）技术来隐藏和绕过EDR，特别是在标准警报设置中。大多数EDR和XDR使用静态防御，可以在低警报模式下阻止常见攻击。然而，为了检测狡猾的恶意软件，他们的代理需要处于高警报模式，这会增加CPU和内存资源的负担。服务器爬行或崩溃。性能下降，用户抱怨。

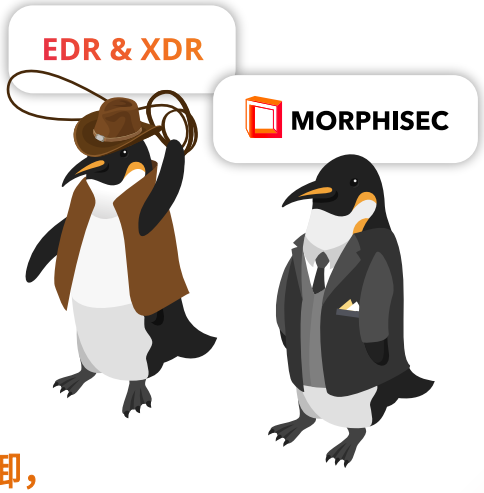
如果你的防卫也很“狡猾”呢？MTD使用轻量级代理和多态性预防，在不影响性能的情况下比坏人更聪明。

可怕的勒索软件

恶意软件经常会在网络中潜行，有时会持续数周，然后触发勒索软件。大多数EDR要么错过了高级攻击，要么抓得太晚。躲过了EDR的威胁可以在你的网络中横向移动，并在任何地方和任何时间攻击关键系统。分析师说，响应需要在几分钟内完成，而不是几天或几周。MTD在几秒内就能响应。

Light on Linux

大多数EDR和XDR解决方案都不是专门为Linux攻击而设计的。这些解决方案使用通用的Windows策略，不使用云工作负载保护平台(CWPP)或服务器工作负载功能。或者更糟的是，它们只是在服务器上运行的桌面解决方案。不要满足于此。MTD for Linux是专门为攻击Linux服务器而设计的。



免责声明：本产品没有得到Linux的认可，也不隶属于Linux，这里的任何内容都不应被视为暗示这种认可或隶属关系。

解决方案是什么？MTD多层防御，又称深度防御