UEM？MTD？何不二者兼得？

实现全面的端到端移动威胁防御

Ivanti正在和Zimperium携手合作，打造全面的企业移动安全解决方案，为无处不在的工作空间提供周密的威胁防御。除了防范网络钓鱼之外，该解决方案也会在设备、网络和应用程序层面上提供保护和攻击补救。

在Ivanti和Zimperium的共同力量下，企业将能够管理和保护移动设备，防止绝大多数的攻击。Zimperium会持续对威胁进行检测和分析，所提供的可视性让Ivanti能够制定基于风险的策略，确保移动设备不会造成企业网络和资产被渗透。

这款集成式的解决方案为IT安全管理员找到了同时安全启用政府提供的设备（GFE）和自带设备（BYOD）的办法，完美平衡了赋权于移动员工和安全之间的平衡，员工可以选择最得心应手、效率最高的设备，而移动设备和企业也将得到保护，免受精心策划的威胁攻击。

主要优势

Zimperium的z9移动威胁保护引擎完全为移动设备设计，它使用的机器学习技术经过优化，适于在没有互联网连接的情况下在设备上运行。非侵入性的设备安全防护方式可提供全天候的保护，而不会影响用户体验或侵犯用户隐私。移动威胁防御（MTD）与Ivanti UEM客户端集成，便于管理员实现100%的用户采纳率。

监管合规

NIST 800.53

《特别文书SP800-53第4版》提出了更全面的信息安全和风险管理方法，为企业规定了从根本上巩固信息系统与其运行环境的安全所必要的安全控制的广度和深度，使系统在面对网络攻击和其他威胁时具有更强的防御能力。Zimperium的z9 MTD引擎为移动威胁防御提供动力，可检测网络的公共访问攻击、针对应用程序和操作系统的恶意代码、设备内事件响应和移动工作环境的漏洞扫描。

NIST 800.124

NIST的《特别文书SP800-124第2版》第4.2.3节指出：“移动威胁防御的目的是侦测移动应用程序或移动操作系统自身内的恶意应用程序、基于网络的攻击、不当配置和已知漏洞。”Zimperium的移动威胁防护系统为设备、操作系统、网络、网络钓鱼和应用程序提供设备内的实时持续监控。此外，Zimperium的z3A高级应用分析对环境中的所有应用程序进行20点验证，并能检测到应用程序之间的异常交互、包含有缺陷或误导性代码的应用、未解决的常见漏洞和暴露或个人身份信息访问。

MITRE ATT&CK® 框架

这是一个开放全球访问、基于实际问题研究建立的攻击者策略和技术知识库。MTD高级应用分析协助检测和补救攻击框架，从而应对攻击。

Zimperium 如何与Ivanti整合：

轻松部署和升级

Zimperium的z9引擎已经嵌入我们的UEM代理。也就是说，这款解决方案已经部署到设备上，只需激活即可。 要完成配置，请添加我们的UEM到zConsole中，然后通过UEM启用激活，以开始保护设备。无需用户操作，也不需要部署新的应用。

保护您的企业基础架构

当MTD检测到设备被入侵时，它可以采取快速补救措施来挫败攻击。根据攻击和设置的具体情况，Ivanti可以执行多种多样的保护操作，包括终止网络连接、拒绝特定的IP/域名和启用指定的隔离操作。此外，Ivanti服务器还可以根据威胁的严重程度，启动基于风险的合规策略来进行补救。此类策略可以暂时禁用有关移动设备与企业服务（电子邮件或其他应用程序、Wi-Fi和VPN）的连接，甚至可以从设备上删除企业应用程序。 这样的操作将阻止攻击扩散，防止企业数据遭遇风险。

警报和报告

Ivanti提供全面的移动威胁取证功能，可根据攻击类型配置终端用户通知和管理员警报，以满足任何企业的需求。此外，也提供隐私数据收集策略功能，以满足地方法规要求。

功能	UEM	MTD	MTD 高级
支持iOS和Android设备。	✓	✓	✓
为操作系统/设备、网络、应用程序和网络钓鱼提供初始漏洞风险安全态势。	✓	✓	✓
检测设备是否启用了适当的物理安全防御（密码、设备层面加密）。	✓ 基本	✓	✓
检测设备是否经过用户越狱/root（使用已知哈希值和文件位置）。		✓	✓
完成设备入侵或攻击所使用的工具和技术方面的取证。		✓	✓
检测操作系统/内核和USB的暴露、身份/配置变化和系统篡改。		✓	✓
检测权限提升攻击。		✓	✓
检测网络攻击（中间人、流氓Wi-Fi和蜂窝网络攻击）。		✓	✓
检测SSL剥离、伪造SSL和SSL流量拦截企图。		✓	✓
检测攻击者的侦察性扫描。		✓	✓
检测网络钓鱼、短信钓鱼、URL钓鱼、短URL等。		✓	✓
企业应用程序交付和删除。	✓		
保护企业文件共享。	✓		
保护业务线应用程序。	✓		

功能	UEM	MTD	MTD 高级
检测恶意应用程序、已知和未知恶意软件以及利用下载执行的动态威胁。		✓	✓
撤销不合规移动设备的访问权限。	✓		
提供详细的移动威胁取证。		✓	✓
执行基于风险的策略，包括锁定或选择性地擦除受入侵的设备。	✓	✓	✓
在检测到攻击时执行即时补救。		✓	✓
扫描内部开发的应用程序的隐私和安全问题/风险。			✓
接收已安装在设备上的应用程序发送的隐私和安全信息。			✓
威胁检测	**UEM**	**MTD**	**MTD 高级**
与主机相关的严重和高等级威胁			
Android设备，可能被篡改		✓	✓
异常进程		✓	✓
开发者选项		✓	✓
设备加密	✓	✓	✓
设备PIN码	✓	✓	✓

威胁防御	UEM	MTD	MTD 高级
与主机相关的严重和高等级威胁			
设备越狱/ROOT MDM的越狱/root检测过于简单，易于绕过。此外，MDM不提供取证功能，无法获取攻击中使用的工具和技术信息。	✓	✓	✓
权限提升		✓	✓
文件系统更改		✓	✓
侧面加载的应用程序		✓	✓
SE Linux禁用		✓	✓
系统篡改 这是高等级的设备入侵，可能使用也可能不使用额外的设备越狱或root步骤。		✓	✓
可疑的iOS应用程序		✓	✓
可疑的Android应用程序		✓	✓
不受信任的配置文件		✓	✓
USB调试模式开启		✓	✓
有漏洞的Android版本		✓	✓
有漏洞的iOS版本		✓	✓

网络钓鱼检测和预防			
始终开启的钓鱼网址检测和拦截。		✓	✓
设备内网络钓鱼检测。		✓	✓
增强的远程服务器网络钓鱼网址检测。		✓	✓
始终开启的针对设备上所有应用程序、所有互联网流量的钓鱼网址检测和拦截，包括本地补救操作。		✓	✓
与网络相关的严重和高等级威胁			
MiTM		✓	✓
MiTM - ARP		✓	✓
MiTM – ICMP重定向		✓	✓
MiTM – SSL剥离		✓	✓
MiTM – 伪造SSL剥离		✓	✓
SSL/TLS 降级		✓	✓

关于Ivanti

Ivanti让无处不在的工作空间成为可能。通过“无处不在的工作空间”，员工可以在任何地方、使用多种设备来访问IT网络、应用程序和数据，同时保证工作效率。Ivanti自动化平台集成了业内领先的统一端点管理、零信任安全和企业服务管理解决方案，通过一站式平台实现为企业实现自我修复和自我安全，并为终端用户提供自我服务。已经有4万多位客户，包括78家《财富》百强企业，选择了 Ivanti 为他们检测、管理、保护和维护从云端到边缘的IT资产，同时为员工提供卓越的终端用户体验，无论他们在哪里、使用何种方式工作。更多信息请访问 ivanti.com。

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com