UEM? MTD? 兩者都需要!

啟動完整的端對端行動威脅防護

UEM

統一端點管理

允許合規設備存取公司電子郵件、應用程式和資料。

保護行動裝置與公司網路之間傳輸的資料。

用容器隔離公司業務與個人資料。

強制執行以風險為基礎的資安政策。

\+

MTD

行動威脅防禦

機器學習、隨時不間斷偵測終端裝置已知和未知攻擊。

初始環境風險評估。

即時偵測進階的設備、網路、應用程式和網路釣魚威脅。

即時修復和 MDM 後續資安防護。

情境式資料說明，詳細的威脅辨識分析，可將資料匯出至 SIEM 或威脅分析工具。

Ivanti 和 Zimperium 兩強攜手共同推出一套完整的企業行動資安解決方案，為 Everywhere Workplace 提供先進的威脅防護。這個解決方案能夠防範網路釣魚，還可保護和修復設備、網路和應用程式級別的攻擊。

Ivanti 和 Zimperium 一起協助企業管理和保護行動裝置不會受到各種不同的攻擊。Zimperium 持續不間斷偵測和分析威脅，並為 Ivanti 提供具可視性的分析資料，制定以風險為基礎的政策，保護行動裝置不致危害公司網路及其資產。

這個整合式解決方案為 IT 安全管理人員提供一套可同時導入政府供應裝備(GFE)和自攜裝置(BYOD)的方法，並在提高員工的行動工作效率和他們所選擇的設備之間取得了平衡，同時也保護行動裝置和企業免受進階威脅。

主要優勢

Zimperium 的 z9 行動威脅防護引擎專為行動裝置而建置，透過持續優化的機器學習技術，可在沒有連接網路的設備上運行。可提供全天候行動裝置保護，且不會影響使用者體驗或侵犯使用者隱私。行動威脅防禦(MTD)與 Ivanti UEM 端點整合，使管理人員可以確保所有使用者皆已導入行動威脅防護。

符合法規

NIST 800.53

NIST 特別版 800-53（第四次修訂版）提供組織可從根本上加強資訊系統和系統運行環境所需的安全控制之廣度和深度，也提供了更完整的資訊安全和風險管理方法，這有助於系統在面對網路攻擊和其他威脅時更有彈性。

Zimperium 的 z9 MTD 引擎不僅啟動行動威脅防護，還可偵測網路公共存取攻擊、應用程式和作業系統的惡意代碼、終端裝置的安全事件應變和掃描行動員工是否有資安漏洞。

NIST 800.124

NIST 特別版 800-124 第二次修訂版第 2 節 4.2.3 指出：「MTD 系統主要是在偵測行動應用程式或行動作業系統當中是否存在惡意應用程式、網路型攻擊、不當配置和已知漏洞。」Zimperium 的行動威脅防護提供了終端裝置、即時的、持續的監控設備、作業系統、網路、網路釣魚和應用程式。此外，Zimperium 的 z3A 進階應用程式分析對環境中的所有應用程式執行 20 點驗證，能夠偵測應用程式之間非預期的交互、含有缺陷代碼或誤導性代碼的應用程式、尚未得到解決的 CVE 或 PII 的存取。

MITRE ATT&CK® 架構

此架構是一套全球皆可存取的知識庫，觀察當今全球各地駭客攻擊戰術及技術。為了抵禦攻擊，MTD 進階應用程式分析可協助偵測和修復攻擊架構。

Zimperium 與 Ivanti 整合：

可輕鬆佈署和升級

Zimperium 的 z9 引擎已經嵌入到我們的 UEM Agent中，這也表示此解決方案已部署到設備上，只需啟用即可。只要將我們的 UEM 加到 zConsole 並啟用 UEM，即可開始保護設備，並完成相關配置，無需與使用者互動，也無需部署新的應用程式。

保護您的企業基礎架構

當 MTD 偵測到設備受到威脅時，它可以提供快速的補救方法來阻止攻擊。Ivanti 可根據攻擊和設定，執行各種保護措施，包括中斷網路連線、拒絕特定 IP／域名及制定明確的隔離措施。此外，Ivanti 伺服器可以制定以風險為基礎的合規性政策，依照威脅的嚴重程度進行補救。這些政策能夠暫時停用行動裝置與企業內部服務（電子郵件或其他應用程式、Wi-Fi 和 VPN）的連接，甚至還可從設備中刪除企業應用程式。這些措施能夠斷絕感染擴散並防止企業資料面臨外洩風險。

提供告警和報告

Ivanti 提供全面的行動威脅辨識資訊、可配置的終端使用者通知和按攻擊類型劃分的管理告警，以滿足企業各種不同的需求，並提供資料收集隱私權政策以符合地區性法規要求。

功能	UEM	MTD	MTD Premium
支援 iOS 和 Android 裝置。	✓	✓	✓
為作業系統／設備、網路、應用程式和網路釣魚提供初始漏洞風險歷程資料。	✓	✓	✓
偵測設備是否啟用了適當的實體安全性（密碼、設備級加密）。	✓ Basic	✓	✓
偵測設備是否被使用者越獄／提權（使用已知的雜湊值和檔案位置）。		✓	✓
為設備入侵或攻擊的工具和技術提供辨識完整資料。		✓	✓
偵測作業系統／核心和 USB 攻擊、設定檔／配置異動、系統篡改。		✓	✓
偵測權限提升攻擊。		✓	✓
偵測網路攻擊（中間人攻擊、惡意 Wi-Fi 和行動網路）。		✓	✓
偵測 SSL Stripping 攻擊、偽造的 SSL 憑證、試圖攔截 SSL 流量。		✓	✓
偵測進行偵察掃描的攻擊者。		✓	✓
偵測網路釣魚、簡訊釣魚、URL 網路釣魚、短網址等。		✓	✓
企業應用程式派送和移除。	✓		
安全保護公司文件共享。	✓		
安全保護企業應用程式。	✓		

功能	UEM	MTD	MTD Premium
偵測是否有透過下載和執行的惡意應用程式、已知及未知的惡意軟體、動態威脅。		✓	✓
禁止不合規行動裝置的存取。	✓		
提供詳細的行動威脅辨識資訊。		✓	✓
執行以風險為基礎的政策，包括鎖定或選擇性抹除已被攻擊的設備。	✓	✓	✓
一旦偵測到攻擊，立即提供補救措施。		✓	✓
掃描內部開發的應用程式是否存在隱私和安全疑慮／風險。			✓
從設備上安裝的應用程式接收隱私和安全資料。			✓
威脅偵測	**UEM**	**MTD**	**MTD Premium**
與主機相關的嚴重威脅和高度威脅			
Android 裝置 – 可能遭到竄改		✓	✓
異常流程		✓	✓
開發者選項		✓	✓
設備加密	✓	✓	✓
設備密碼	✓	✓	✓

威脅偵測	UEM	MTD	MTD Premium
與主機相關的嚴重威脅和高度威脅			
設備被越獄／提權。MDM 越獄／提權偵測非常簡單且可容易避開。此外，MDM 無法提供已被攻擊的設備可供分析的工具，技術及完整辨識資料。	✓	✓	✓
權限提升		✓	✓
檔案系統更改		✓	✓
側載應用程式		✓	✓
SE Linux 停用		✓	✓
系統篡改。這是一種設備上的進階感染，可能會或可能不會使用越獄或提權設備的另一種步驟。		✓	✓
可疑的 iOS 應用程式		✓	✓
可疑的 Android 應用程式		✓	✓
不受信任的個人資料		✓	✓
USB 除錯模式開啟		✓	✓
易受攻擊的 Android 版本		✓	✓
易受攻擊的 iOS 版本		✓	✓

網路釣魚偵測和預防			
不間斷偵測和阻斷網路釣魚 URL。		✓	✓
偵測終端裝置的網路釣魚。		✓	✓
遠端伺服器上強化的網路釣魚 URL 檢查。		✓	✓
不間斷網路釣魚偵測和阻斷來自所有應用程式和設備上的所有網路流量(包括本機修復操作)的網路釣魚 URL。		✓	✓
與網路相關的嚴重威脅和高度威脅			
MiTM		✓	✓
MiTM - ARP		✓	✓
MiTM – ICMP 重新導向		✓	✓
MiTM – SSL strip 攻擊		✓	✓
MiTM – 偽造的 SSL strip 攻擊		✓	✓
SSL/TLS 降級		✓	✓

Ivanti 簡介

Ivanti 使 Everywhere Workplace 成為可能。在 Everywhere Workplace, 員工可以使用各式各樣的設備存取 IT 網路、應用程式和資料, 無論在任何地方工作, 都能保持工作效率。Ivanti 自動化平台連接 Ivanti領先業界的統一端點管理、零信任安全和企業服務管理解決方案, 為企業提供單一管理平台, 實現自我修復和自我保護設備, 以及自助服務終端使用者。我們擁有超過 40,000 家客戶, 其中包括財經雜誌《財星》(Fortune)百大企業中的 78 家。他們選擇 Ivanti 來探索、管理、保護和服務他們從雲端到邊緣的 IT 資產, 並為員工提供卓越的終端使用者體驗, 無論他們在哪裡和如何工作。

如欲了解更多資訊, 請瀏 ivanti.com

ivanti.com
+886 975-125148
ContactChina@ivanti.com