技術規格

# CRITICALSTART®
# 擴充式威脅偵測和應變 (MxDR) 託管服務指南

## 防範入侵可以很簡單。

Critical Start 是目前市場上唯一一家敢於首先接受複雜事物，來簡化網路安全問題的 MDR （提供威脅偵測和應變服務） 供應商。當別人專注於發現弱點時，我們專注於發現優勢。當其他人還在排序處理或者抑制警報時，我們解決所有的警報。

Critical Start 為您提供一支技術精湛的安全專家團隊，他們將深入了解您的環境，並根據您組織的需求進行調整和擴展，與您合作偵測、調查和應變針對您組織的特定威脅。

Critical Start 提供無價的安全感，包括以下好處：

- ✓ 我們提供現場和遠端事件的應變和數位蒐證能力，適合需要資深事件應變人員的情況
- ✓ 不論是我們團隊的每一個動作或檢查的資料點、我們所偵測到的內容，還是您的安全工具與 MDR 服務所提供的偵測範圍，全都 100% 清楚可見
- ✓ 無論嚴重程度如何，我們對所有警報提供「偵測所需時間 (TTD)」和「解決事件中位時間 (MTTR)」的服務等級協議，保證在一個小時或更短時間內解決，並且沒有任何細節限制

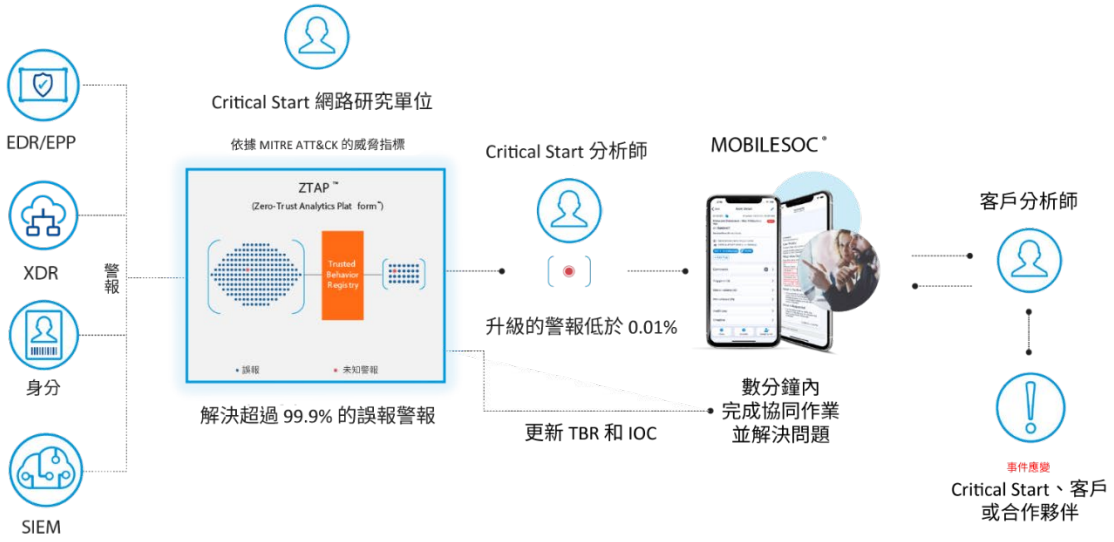
Smarter technology for all

Lenovo

MDR 服務是業界唯一的 Trusted Behavior Registry™ (TBR)，並且是建立在我們的 Zero-Trust Analytics Platform™ (ZTAP™) 上，可以解決所有的警報。它與多種安全工具整合，包括端點、SIEM、XDR 和身分驗證，能將警報量減少超過 99%，僅不到 0.01% 的警報需升級，並且不會重複發送相同的警報。

# 主要優勢

- ✓最佳化安全投資：生產監控第一天的誤報率即降低 90%，僅低於 0.01% 的警報需要升級處理
- ✓減少風險暴露：能解決超過 99% 的警報，從而降低風險暴露
- ✓減少複雜性：超過 40% 的客戶依賴我們將多種安全工具的概念深入解析整合在一起，以減少複雜性



# 實現方式

## 偵測正確的威脅。透過 MxDR 服務，完成以下步驟：

- ✓ 管理、維護並整理安全工具製造商隨時啟用的偵測功能和 IOC (威脅指標)。
- ✓ 管理原始和第三方威脅情報，並結合即時威脅分析，為現有和新出現的威脅建立高度可靠且可行的資訊視圖。
- ✓ 根據不斷變化的安全環境，持續開發和豐富新的威脅偵測與威脅指標 (IOC)。
- ✓ 將威脅偵測內容對應至 MITRE ATT&CK® 框架，以確保您受到最新的攻擊者技術、戰術和程序 (TTP) 的保護。

## 以正確的行動應變。

- ✓ Critical Start 提供專業的安全營運中心 (SOC) 分析師，透過全天候、全年無休的監控、快速調查和持續的威脅搜尋，能迅速偵測並回應所有升級的警報。
- ✓ MOBILESOC® 應用程式使您能夠與 SOC 進行溝通，並隨時隨地執行應變行動。

## 提供靈活度和適應能力。

- ✓ 從一開始，我們的專屬專案經理和執行團隊即會深入研究您的環境、獨特需求和業務目標。
- ✓ 我們的客戶成功團隊將成為您的支持者，在整個過程中與您同行，根據您的需求變化，提供建議和支援。

## Critical Start 只提供**最佳解決方案**。

Critical Start 的 MDR 服務與領先的安全技術整合在一起，以偵測每一個警報、解決每一個警報並回應入侵行為。

Microsoft Defender for Endpoint
Microsoft 365 Defender
Microsoft Sentinel
CORTEX
splunk>
TREND MICRO
vmware Carbon Black
BlackBerry CYLANCE
SentinelOne
DEVO
CROWDSTRIKE