THREATDOWN™
Powered by Malwarebytes

ThreatDown Identity Threat Detection & Response

透過端點到身分的統一防禦，阻斷資安破口

Overview

隨著以身分為核心的攻擊激增，憑證濫用已成為導致企業資料外洩的首要原因，公司在無法擴編資安團隊的情況下，面臨巨大的壓力。涵蓋 Active Directory、Entra ID 和 Okta 的混合環境，造成傳統 IAM、MFA 和端點工具無法看見的盲點——提供攻擊者極易利用的「驗證後真空地帶」。

 # 1 身分攻擊是目前最主要的攻擊路徑

參考來源：IBM X-Force 2025; IBM Cost of a Data Breach 2025

ThreatDown ITDR 透過持續監控身分行為、將其與端點活動進行關聯分析，並自動化回應，以更少的人力更迅速阻止攻擊，從而滿足了這些市場需求。它使企業能夠在不增加額外開銷或團隊人數的情況下，提升資安成效、符合法規預期並維持業務連續性。

ThreatDown ITDR 核心優勢

- 看清從端點行為到身分淪陷的完整攻擊流程：

  ThreatDown 原生關聯了來自 EDR 的使用者相關數據，與內部部署 Active Directory、Entra ID 和 Okta 的身分活動。當攻擊者從受侵入的端點移動到竊取憑證、再到權限提升時，您可以在同一個地方看到完整的攻擊鏈。無需切換視窗，端點層與身分層之間不再有盲點。

- 主動強化攻擊路徑：

  ThreatDown ITDR 原生關聯端點遙測與跨 Active Directory、Entra ID 和 Okta 的身分事件，為安全團隊在單一介面提供完整的攻擊流程。當與 MDR（託管偵測與回應）結合使用時，專家資安分析師將全天候監控憑證使用、權限活動和工作階段（Session）行為。

面臨挑戰

- **身分型威脅激增**
  身分現已成為第一大網路攻擊表面，大多數的外洩事件都涉及憑證竊取。
- **太多的軟體與廠商過於發散**
  70% 的企業正積極整合資安工具，然而大多數 ITDR 解決方案卻只是增加了另一個資訊孤島。
- **無法及時回應造成災害蔓延**
  企業平均需要 241 天才能識別並遏阻一起資料外洩事件。

效益分析

- **主動的身分防禦**
  透過優先排序的洞察分析，持續識別並消除高風險曝露，從而降低組織風險。
- **更快的偵測與回應**
  透過同一個統一的雲端控制台來管理，藉此簡化工作流程、提高效率並降低資安營運成本，進而減少運作複雜性。
- **加速調查與補救措施**
  原生的「端點到身分」關聯分析能穿透雜訊，縮短平均回應時間（MTTR）；配合 24/7 MDR，專家分析師隨時在線，以更高準確度更快地遏阻威脅。

為精簡團隊簡化運作

只需點擊幾下即可完成部署，並可從與 ThreatDown EDR. MDR同一個控制平台進行管理，因此能減少工具蔓延（Tool Sprawl）和企業額外的營運開銷，在不增加複雜性的情況下為團隊提供更多保護。

揭露暗網威脅，讓潛伏無所遁形

持續監控暗網來源，尋找與您組織相關的外洩憑證。當偵測到受害帳戶時，ThreatDown 會直接在您的控制平台中呈現，讓您能夠快速採取行動，從強制重設密碼到為高風險使用者優先進行補救。

符合合規要求的身分洞察

統一的身分可見性與具體可行的報告，幫助組織輕鬆支持 GDPR、HIPAA 和審計規範，為監管機構、利益關係人和資安領導層提供清晰、合規有效的證明文件。

快速遏阻威脅

內建針對關鍵行動（如主機隔離、帳戶停用和攻擊路徑補救）的可採取措施，以減少警報雜訊，讓精簡的團隊能在幾秒鐘內（而非數小時）做出回應。

託管服務更早阻斷憑證驅動型攻擊

與 MDR 搭配使用時，專家資安分析師會 24/7 監控憑證使用、權限活動和工作階段行為。分析師協助在憑證竊取、權限提升、權杖（Token）濫用和橫向移動演變成實質外洩前，進行偵測與阻斷。無需額外聘雇身分安全專家團隊。

HOW IT WORKS

從偵測到遏阻只需數秒，而非數天

ThreatDown ITDR 持續監控您環境中的使用者行為。當偵測到威脅時，回應行動會在損害擴大前將其遏阻。