DATA SHEET

THREATDOWN™
Powered by Malwarebytes

ThreatDown Identity Threat Detection & Response

Stop breaches with unified endpoint-to-identity defense

Overview

As identity-driven attacks surge and credential misuse becomes the leading cause of breaches, companies face mounting pressure to protect the business without expanding security teams. Hybrid environments across Active Directory, Entra ID, and Okta create blind spots that traditional IAM, MFA, and endpoint tools can't see—leaving a post authentication gap attackers readily exploit.

#1 Identity attacks are the top attack vector*

ThreatDown ITDR addresses these needs by continuously monitoring identity behavior, correlating it with endpoint activity, and automating response to stop attacks earlier and use less effort. It empowers organizations to improve security outcomes, support regulatory expectations, and maintain business continuity without adding overhead or headcount.

ThreatDown ITDR Advantages

- **See the full attack story from endpoint behavior to identity compromise**: ThreatDown natively correlates user telemetry from your EDR with identity activity across on-premises Active Directory, Entra ID, and Okta. When an attacker moves from a compromised endpoint to stolen credentials to privilege escalation, you see the complete chain in one place. No context switching. No blind spots between your endpoint and identity layers.
- **Proactive attack path hardening**: ThreatDown ITDR natively correlates endpoint telemetry with identity events across Active Directory, Entra ID, and Okta to give security teams the full attack story all in one place. When used alongside MDR, expert security analysts monitor credential use, privilege activity, and session behavior, 24x7.

* IBM X-Force 2025; IBM Cost of a Data Breach 2025

Challenges

- Identity-based threats are surging Identity is now the #1 cyberattack surface, with the majority of breaches involving stolen credentials
- Software and vendor sprawl for IT security 70% of organizations are actively working to consolidate security tools, yet most ITDR solutions add yet another silo
- Slow response amplifies damage Organizations take an average of 241 days to identify and contain a breach and contain a breach

Benefits

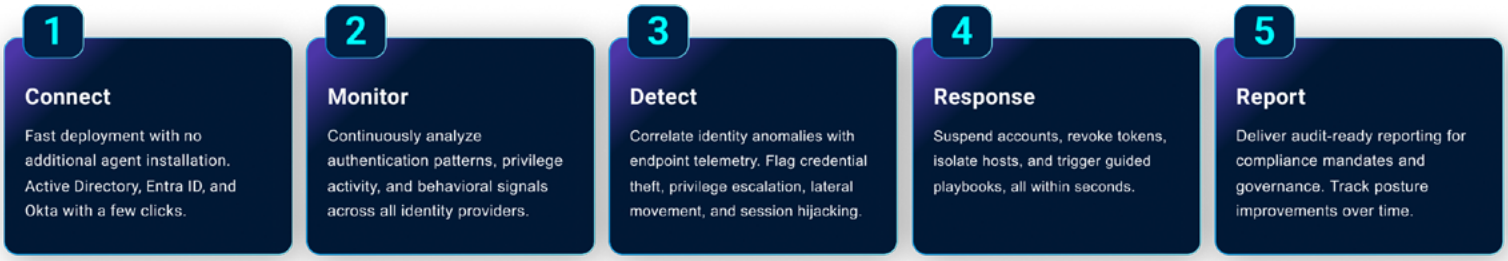
- Proactive identity defense Continuously identify and eliminate high-risk exposures with prioritized insights that reduce organizational risk
- Faster detection and response Reduce operational complexity by managing ITDR through the same unified, cloud-based console that powers the entire ThreatDown security stack to streamline workflows, improving efficiency, and lowering the cost of security operations
- Accelerated investigations and remediation Native endpoint-to-identity correlation cuts through noise and reduces mean time to respond — and with 24x7 MDR, expert analysts are always on hand to contain threats faster and with greater accuracy

- **Simplifies operations for lean team**: With deployment in just a few clicks and management from the same console as ThreatDown EDR and email security, ITDR reduces tool sprawl and operational overhead to give teams more protection without added complexity.
- **Dark web threats, brought to light**: Continuously monitor dark web sources for leaked credentials tied to your organization. When compromised accounts are detected, ThreatDown surfaces them directly in your console giving you the visibility to act fast, from forcing password resets to prioritizing remediation for your riskiest users.
- **Compliance ready identity insight**: Unified identity visibility and actionable reporting help organizations support GDPR, HIPAA, and audit mandates with ease, providing clear, defensible documentation for regulators, stakeholders, and security leadership.
- **Fast containment**: Built in guided playbooks for key actions such as host isolation, account suspension, and attack path remediation to reduce alert noise and enable lean teams to respond in seconds, not hours.
- **Managed services stop credential driven attacks earlier**: When used alongside MDR, expert security analysts monitor credential use, privilege activity, and session behavior, 24x7. The analysts help detect and block threats like credential theft, privilege escalation, token abuse, and lateral movement before they become breaches. Its the identity security team you didn't have to hire.

HOW IT WORKS

From Detection to Containment in Seconds, Not Days

ThreatDown ITDR continuously monitors user behavior across your environment. When a threat is detected, response actions contain it before damage spreads.



To learn more about how ThreatDown ITDR can help reduce cyber risk of your organization, please visit threatdown.com/itdr