DATA SHEET

THREATDOWN™

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. The threat extends beyond human users. Attackers don't just steal user credentials—they hijack service accounts, API tokens, and OAuth credentials to log in as legitimate users and machines. 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 challenges by continuously monitoring both user accounts and non-human identities after authentication, detecting threats like credential abuse, token hijacking, privilege escalation, and lateral movement. It empowers organizations to improve security outcomes, support regulatory expectations, and maintain business continuity without adding overhead or headcount.

ThreatDown ITDR Capabilities

- **Full attack story, endpoint to identity**: Correlates EDR telemetry with identity activity across Active Directory, Entra ID, and Okta — see the complete chain from compromised endpoint to compromised credentials to privilege escalation, with no blind spots or context switching.
- **Unified visibility, human and non-human**: One console covers AD, Entra ID, and Okta as well as services accounts, API tokens, and OAuth credentials. Machine identities are auto-discovered and baselined, so abuse is flagged even when the credential is technically valid.

* 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

Benefits

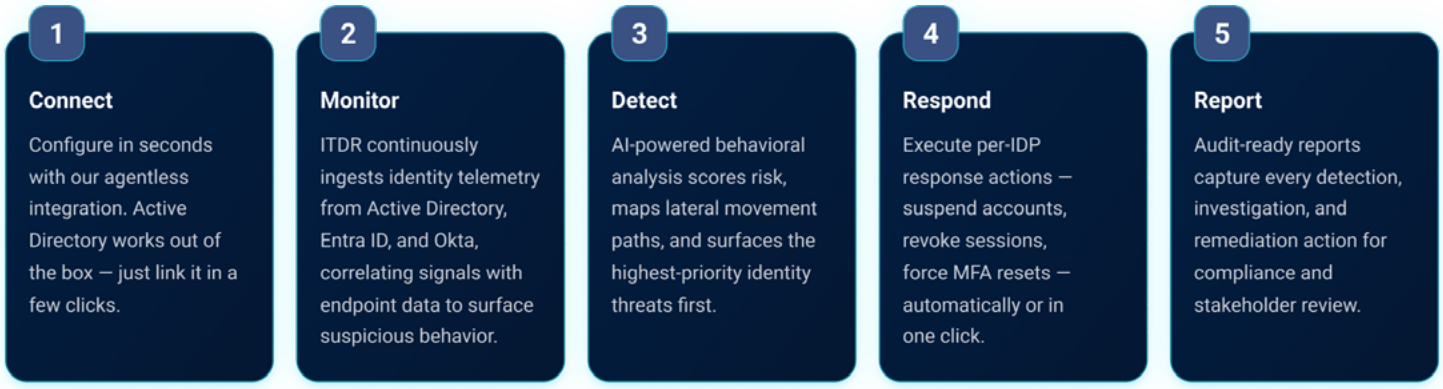
- Proactive identity defense across human and non-human identities Continuously identify and eliminate high-risk exposures across user accounts, service accounts, API tokens, and OAuth credentials with prioritized insights that reduce organizational risk
- Faster detection and response Reduce operational complexity by managing ITDR through the same unified, cloud-based console that powers 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

- **Fast, low-overhead deployment**: Deploys in a few clicks and runs in the same console as ThreatDown EDR and email security — less tool sprawl, less complexity.
- **Dark web monitoring**: Continuously scans for leaked credentials tied to your organization and surfaces them in-console for fast action, from password resets to prioritized remediation.
- **Compliance-ready reporting**: 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, guided containment**: Suspend accounts, revoke sessions/tokens, or disable service accounts automatically or in one click, with guided playbooks for isolation and remediation — respond in seconds, not hours.
- **MDR-backed protection**: Paired with MDR, analysts monitor credential use, privilege activity, and session behavior 24x7 — catching credential theft, escalation, and lateral movement before they become breaches.

HOW IT WORKS

From Detection to Containment in Seconds, Not Days

ThreatDown ITDR continuously monitors human and non-human identities 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