

Cynet Identity Security: Proactive Identity Protection Without Complexity

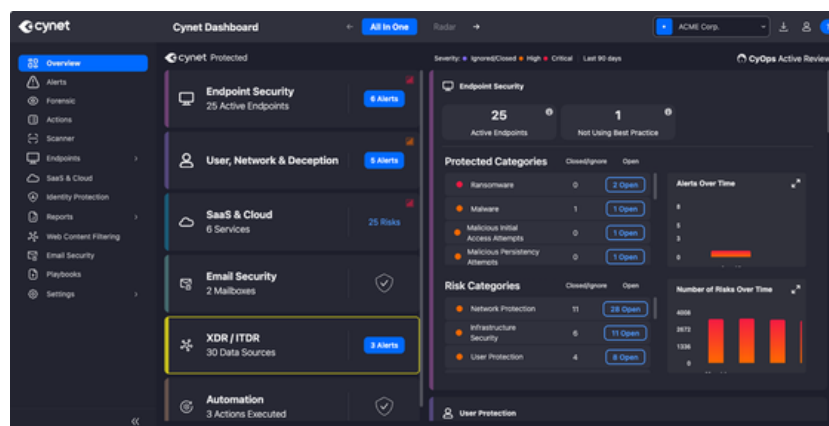
Secure every user. Protect every identity.

Identity is the #1 Breach Vector

Identity has become the most exploited attack surface in modern environments. Attackers no longer need malware when valid credentials, tokens, and over-privileged accounts provide a faster, quieter path to impact.

Why Identity Threat Detection (ITDR) is now mandatory:

- Over 80% of successful breaches originate from compromised credentials.
- 1/6 breaches in 2025 involved AI-driven attacks
- 40% of cloud NHIs have no identifiable owner, making them incredibly vulnerable



The Core Challenge:

Most organizations treat identity as a configuration problem, not a real-time threat vector. Posture tools share what might be risky. Cynet ITDR confirms what is being actively exploited and stops it.

Cynet Delivers Identity Security Through Two Tightly Integrated Layers:

ITDR - Cynet detects and stops identity-driven attacks as they happen- before they turn into ransomware, data exfiltration, or domain takeover.

Identity Posture & Exposure Awareness - Cynet continuously monitors identity configurations, permissions, and behaviors to reduce blast radius and prevent abuse.

Unlike bolt-on ITDR tools, Cynet ITDR is natively embedded inside our unified platform, enabling faster detection, richer context, and automated response across identity, endpoint, SaaS, and cloud.



Credential Theft & Account Takeover

- Detects compromised credentials via abnormal authentication patterns
- Identifies impossible travel, suspicious logins, and MFA bypass attempts
- Automatically isolates risky accounts and terminates malicious sessions



Token Abuse & Session Hijacking

- Identifies abuse of OAuth tokens and stale sessions.
- Detects anomalous access to SaaS apps and cloud resources
- Blocks attacker persistence without waiting for manual intervention



Privilege Escalation & Lateral Movement

- Monitors abnormal privilege changes and access expansion
- Detects identity-driven lateral movement across endpoints and cloud
- Correlates identity behavior with endpoint and network activity



Non-Human Identity Abuse

- Monitors service accounts, APIs, and machine identities
- Flags abnormal behavior tied to automation, scripts, and integrations
- Reduce blind spots created by over-privileged machine identities



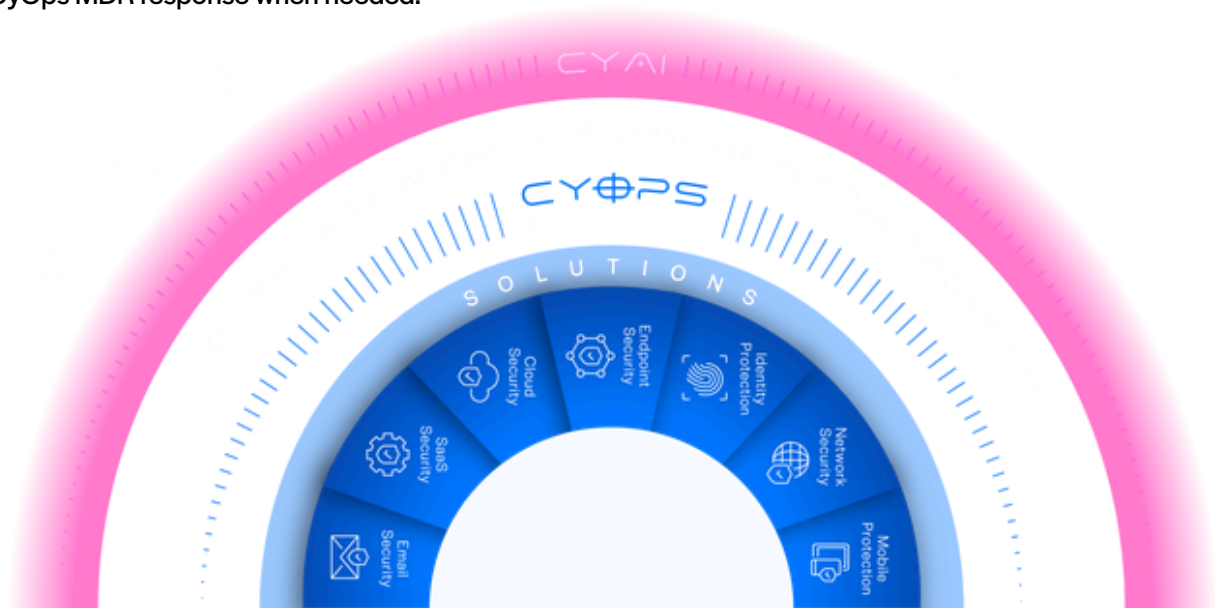
How Cynet ITDR Works

With Cynet, identity threats are contained in real time, quickly enough that threats are identified before attackers can move, persist, or escalate. So how does Cynet do this?

Identity Telemetry Ingestion: Cynet continuously ingests identity-related telemetry from identity providers, endpoints, user behavior, SaaS & cloud access activity, and network & lateral movement signals.

Correlation & Attack Path Mapping: CyAI correlates identity activity with endpoint, cloud, and SaaS signals to identify malicious identity behavior, visualize identity-driven attack paths, and distinguish real threats from benign misconfigurations.

Automated Identity Response: Cynet takes immediate action when risk is confirmed by disabling or isolating compromised identities, terminating suspicious sessions & tokens, blocking lateral movement & privileged abuse, and triggering CyOps MDR response when needed.



Cynet is Built Differently

Built Into Cynet's Platform, Not Bolted On

- Identity signals are analyzed alongside endpoint, network, SaaS, and cloud data
- No swivel-chair investigation, fragmented alerts or fine-tuning

Real-Time Response, Not Just Alerts

- Automatic containment of identity threats
- No dependency on manual analyst approvals

CyAI + CyOps MDR

- AI-driven detection backed by 24x7 human response with Cynet's CyOps team



Trusted Results (MITRE 2025)

- ✓ 100% Protection
- ✓ 100% Technique Coverage
- ✓ 100% Detection Visibility
- ✓ Zero False Positive Detections