CrowdStrike Falcon Identity Threat Detection and Response (ITDR)

Stop identity-based attacks in real time

In the work-from-anywhere world, protecting workforce identities has never been more important. That's why industry analysts are recommending that organizations adopt identity threat detection and response (ITDR) solutions to protect against compromised user accounts, leaked passwords, data breaches and fraudulent activity. Frictionless security requires all users, whether inside or outside an organization's network, to be authenticated, authorized and continuously validated. This strengthens your identity security posture and ensures the right person has the right access to the right resources at the right time.

Whether you're already adopting single sign-on (SSO) and multifactor authentication (MFA), or still working on how to transfer more applications to the cloud, CrowdStrike Falcon® ITDR modules can offer the information and assistance you need to identify, reduce and respond to potential identity-based threats.

Two CrowdStrike Falcon platform modules are offered to support ITDR and identity security posture management (ISPM) security frameworks, depending on what your organization needs for identity protection to fit your Active Directory (AD) security use cases: CrowdStrike Falcon® Identity Threat Detection for either identification/detection-only and CrowdStrike Falcon® Identity Threat Protection for active prevention of identity attacks.

Key highlights

Falcon identity protection consists of two Falcon platform modules:

- **Falcon Identity Threat Detection:** Serves as the first level of detection for AD security, providing identity risk analysis and detecting threats to the authentication system and credentials as they happen
- **Falcon Identity Threat Protection:** Enables frictionless security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics that combine with nearly any MFA/SSO provider to challenge threats in real time

Falcon Identity Threat Detection: AD Security Alerts

Falcon Identity Threat Detection represents the first level of detection for AD security. Falcon Identity Threat Detection provides visibility for identity-based attacks and anomalies, comparing live traffic against behavior baselines and rules to detect attacks and lateral movement. It provides real-time AD security alerts on rogue users and sideways credential movement within the network or cloud.

Falcon Identity Threat Detection enables you to:

- See all organizational service accounts, privileged users and user credentials
- Add the context of "who" to network attack discovery and investigation, with behavioral analysis for each credential
- Track every authentication transaction, and alert when the risk is elevated (e.g., accessing new systems or being granted additional privileges), or if the traffic is abnormal (varies from normal patterns of the user behavior)
- Expand understanding for both architecture and security teams by combining context of authentication-level events with recommended best practices for network security

Seeing user authentication activity everywhere, from local legacy apps to your cloud environment stack, is the first step toward effectively managing AD security for identity and access.

Falcon Identity Threat Protection: Frictionless Conditional Access

Powered by CrowdStrike® Security Cloud — the world's largest, unified, threat-centric data fabric — Falcon Identity Threat Prevention enables frictionless security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics.

With a nebulous enterprise perimeter, internal applications that were previously considered secure for authenticated users are now open to access from compromised systems and compromised users.

Falcon Identity Threat Protection:

- Provides unified visibility and control of access to applications, resources and identity stores in hybrid environments
- Improves alert fidelity and reduces noise by recognizing and auto-resolving genuine access incidents through identity verification
- Enforces consistent risk-based policies across cloud and legacy systems with zero friction — actions include block, allow, audit and step-up using MFA
- Optimizes log storage costs by storing only relevant authentication logs

More mature security operations may be looking for controls for a hybrid environment in real time, in a way that prevents user fatigue and simultaneously secures service and privileged accounts. Falcon Identity Threat Protection provides that level of control without sacrificing end-user MFA fatigue by providing risk-based adaptive authentication.

Feature Comparison: Falcon Identity Threat Detection vs. Falcon Identity Threat Protection

Feature	Falcon Identity Threat Detection	Falcon Identity Threat Protection
Microsoft AD accounts analysis	Yes	Yes
Azure AD accounts analysis	Yes	Yes
Insights and analytics	Yes	Yes
Security assessment	Yes	Yes
Detection of AD security incidents	Yes	Yes
Deep packet inspection of live traffic	Yes	Yes
Real-time threat detection for authentication and authorization access requests	Yes	Yes
Real-time cloud activity visibility, baselining and monitoring for federated access via AD FS and Okta or PingFederate	Yes	Yes
Near real-time cloud activity visibility, baselining and monitoring using events analysis from Okta, Azure AD and Ping	Yes	Yes
Policy creation for monitoring or enforcement	No	Yes
Real-time cloud activity enforcement (e.g., block, MFA)	No	Yes
Real-time enforcement and secured access to Microsoft AD (e.g., block, MFA)	No	Yes
Custom threat detection — create real-time alerts from policy rules	No	Yes
Reports (including custom)	Partly — includes report for incidents, activity and Threat Hunter (custom)	Yes
Threat hunting	Yes	Yes
API support	Yes — to SIEM or SOAR tools	All, plus SSO and MFA tools
Email integration to report events	Yes	Yes
Technical support	Yes	Yes

Because 80% of breaches involve compromised credentials, Falcon ITDR modules improve your security posture by segmenting identities and automating analysis and enforcement of AD security.

Improved security posture with extended MFA: Extend identity verification/MFA tools to any resource or application, including legacy/proprietary systems and legacy systems traditionally not integrated with MFA — such as desktops, tools like PowerShell and protocols like RDP over NTLM — to reduce the attack surface.

Enhanced identity store security posture: Designate accounts as honeytokens to safely lure adversaries away from your critical resources, with dedicated insights into their attack paths. Get instant visibility into SMB to DC authentication events and reduce credential stuffing vulnerabilities with visibility into accounts that share passwords.

Both Falcon identity protection modules provide Active Directory attack detections:

- Account enumeration reconnaissance (BloodHound, Kerberoasting)
- Bronze Bit (CVE-2020-17049)
- Brute force attacks (LDAP simple bind, NTLM, Kerberos)
- Credential scanning (on-premises)
- Cloud-based (Azure AD) brute-force/credentials scanning
- DCSync — Active Directory replication
- DCShadow
- Forged PAC for privilege escalation (Bulletin MS-14-068)
- Golden Ticket
- Hidden object detected
- NTLM Relay Attack (including MS Exchange)
- Overpass-the-Hash (Multiple methods - Mimikatz, CrackMapExec)
- Pass-the-Hash (Impacket, CrackMapExec, Metasploit)
- Pass-the-Ticket
- Possible exploitation attempt (CredSSP) CVE-2018-0886
- Remote execution attempts
- Skeleton Key and Mimikatz Skeleton Key
- Suspected NTLM authentication tampering (CVE-2019-1040)
- ZeroLogin (CVE-2020-1472)

Both Falcon ITDR modules provide visibility to "rogue credential" or behavior anomalies:

- Access from a forbidden country
- Adding a user to a privileged group
- Anomalous DCE/RPC
- Bronze Bit (CVE-2020-17049)
- Custom threat detection using policy rules
- Excessive access (servers)
- Excessive access (services)
- Excessive access (workstations)
- Hidden object detected
- Identity verification denied
- Identity verification timeout
- Service account misuse
- Suspicious VPN connections — unusual user geolocation
- Unusual access to a server
- Unusual access to a service
- Unusual protocol implementation
- Usage of IP with a bad reputation
- Use of stale endpoint

Whether you need to identify potentially malicious identity traffic or you're ready to challenge it and create risk-based conditional access, CrowdStrike has the right product for you.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

See it in action →