In this work-from-anywhere world, frictionless security requires all users, whether inside or outside an organization's network, to be authenticated, authorized and continuously validated for security configuration and posture before being granted access or keeping access to applications and data.

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® identity protection can offer the information and assistance you need to pass audits and succeed in security tests.

Two CrowdStrike Falcon® platform modules are offered for identity protection to fit your Active Directory (AD) security use cases for either identification/detection-only or active prevention of identity attacks: CrowdStrike Falcon® Identity Threat Detection and CrowdStrike Falcon® Identity Threat Protection.

**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:
FRICIONLESS 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

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

Because 80% of breaches involve compromised credentials, Falcon identity protection 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)

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.