CROWDSTRIKE

CROWDSTRIKE FALCON IDENTITY PROTECTION MODULES

Active Directory (AD) security for your Zero Trust architecture

Zero Trust is a security framework that 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 solutions can offer the information and assistance you need to pass audits and succeed in security tests.

Two Falcon products 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: Falcon Identity Threat Detection and Falcon Zero Trust.

KEY HIGHLIGHTS

Two Falcon identity protection solutions are available:

Falcon Identity Threat Detection (ITD): 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 Zero Trust (ZT): Enables frictionless Zero Trust 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 (ITD): AD SECURITY ALERTS

CrowdStrike Falcon Identity Threat Detection (ITD) represents the first level of detection for AD security. Falcon ITD 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 Active Directory security alerts on rogue users and sideways credential movement within the network or cloud.

Falcon ITD 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 ZERO TRUST (ZT): FRICTIONLESS CONDITIONAL ACCESS

CrowdStrike Falcon Zero Trust (ZT) enables frictionless Zero Trust 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 ZT:

- 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 to enable Zero Trust architecture with zero friction — actions include block, allow, audit and step-up using MFA
- Saves overhead of 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 Zero Trust 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 ZERO TRUST

Feature	Falcon ITD	Falcon ZT
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 identity protection products advance your Zero Trust architecture 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.

Improved security posture and significantly reduced attack surface by extending MFA: Extend identity verification/MFA tools to any resource or application, including legacy systems like desktops, tools Ike PowerShell, and protocols like RDP over NTLM.

CROWDSTRIKE FALCON IDENTITY PROTECTION MODULES

Both solutions 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 solutions 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 Zero Trust conditional access, CrowdStrike has the right product for you.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Schedule a Demo

Learn more **www.crowdstrike.com**