

FALCON ZERO TRUST

Prevent breaches with frictionless risk-based authentication

MULTI-DIRECTORY IDENTITY PROTECTION ACROSS ON-PREMISES AND CLOUDS

CrowdStrike Falcon Zero Trust enables frictionless Zero Trust security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics. A full 80% of breaches involve compromised credentials, and therefore segmenting identities, automating enforcement and using risk-based conditional access to verify authentication traffic can reduce risk and reduce IT complexity.

KEY PRODUCT CAPABILITIES

SEGMENT

Gain granular and continuous insights into every account and activity to highlight identity security gaps across identity stores, and empower your identity and access management (IAM) and security teams to better evaluate identities and the risks associated with them.

Continuous multi-directory visibility: Get deeper visibility into the scope and the impact of access privileges for identities across Microsoft Active Directory (AD) and Azure AD.

Auto-classification of all accounts: Automatically classify identities into hybrid (identities that are on-premises and cloud AD) and cloud-only (identities that reside only on Azure AD), and segment accounts into human, service, shared accounts and privileged accounts.

Customizable Active Directory security posture overview: Analyze user risk and behavior changes over time, like increase in account lockouts, high-risk endpoints and compromised passwords to get an overview of the attack surface of the organization.

KEY BENEFITS

Realize value from Day One — gain unified visibility and control of access to applications, resources and identity stores in hybrid environments

Reduce mean time to detect and respond, and improve SOC analysts' efficiency and response times by collating all connected anomalies and alerts into incidents

Improve alert fidelity and reduce noise by recognizing and auto-resolving genuine access incidents through identity verification

Enforce consistent risk-based policies to enable Zero Trust architecture with zero friction — actions include block, allow, audit, reset password and step-up using multifactor authentication (MFA)

Save log storage costs by storing only relevant authentication logs

Increase ROI from your MFA investment by extending it to legacy applications and tools

AUTOMATE

Enable real-time identity threat detection and protection without time-consuming log processing. Eliminate risky guesswork and prioritize authentication tasks based on 100+ behavior analytics and risk factors for every account.

Hybrid identity store protection:

Continuously assess the directory configuration, like Group Policy Objects (GPO), LDAP configurations and risky protocols. Analyze every account from on-premises to hybrid identity stores. Inspect live authentication traffic, including encrypted protocols (e.g., LDAP/S).

No-log, real-time threat detection:

Continuously assess identity events and automatically associate them with threats and malicious intent, in real time, without ingesting logs with Falcon Zero Trust's out-of-the-box machine-learning-powered detection rules. With advanced analytics and patented machine learning, uncover reconnaissance (e.g., LDAP, BloodHound, SharpHound, credential compromise attacks), lateral movement (e.g., RDP, pass-the-hash (PtH), Mimikatz tool, unusual endpoint usage, unusual service logins, etc.), and persistence (e.g., Golden Ticket attack, privilege escalation, etc.).

Intuitive threat hunting: Investigate faster with unified domain access into detailed activities of every account across hybrid identity stores without the need for complex, string-based queries. Choose from a list of predefined search criteria, including authentication events, use of unencrypted protocols, user roles, IP reputation, risk scores and many more. If required, create and save your own search criteria to proactively sift through raw events and email them as periodic reports.

Comprehensive API coverage: Extend the CrowdStrike Falcon® platform's risk score and high-fidelity information to other apps

(e.g., AD FS, SSO, IT systems and over 50+ integrations) with minimal effort using API-based connectors.

VERIFY

Secure employee or contractor access to applications, tools and resources with a zero-friction user experience. Ensure consistent login experience for genuine users, but automatically step up authentication when risk scores increase.

Zero-friction identity verification with flexible policies:

Define and enforce access policies with simple rules with Falcon Zero Trust's adaptive analysis, eliminating the need to write complex static conditions for every user. The policies are based on authentication patterns, behavior baselines, individual user risk score and device risk score (Zero Trust Assessment or ZTA score) to verify identities using MFA. This robust methodology secures access to identity stores and applications, with improved user experience — i.e., identity verification is triggered only when the risk increases or if there's a deviation from normal behavior.

Improved security posture with extended MFA:

Extend identity verification/MFA to any resource or application, including legacy/proprietary systems and tools that traditionally could not be integrated with MFA — for example, desktops that are not covered by cloud-based MFA solutions, and tools like PowerShell and protocols like RDP over NTLM — to reduce the attack surface.

Auto-resolve security incidents: With the platform's customizable enforcement policies, resolve standard incidents that the user approves using identity verification methods (2FA/MFA), so that your security analysts can focus on critical security incidents. Additionally, resolve these incidents with effortless API integrations into SOAR, SIEM and ticketing platforms.

FRICTIONLESS ZERO TRUST

Multi-directory identity layer

support: CrowdStrike Falcon Zero Trust supports Microsoft Active Directory and Azure Active Directory, and integrates with SSO and federation solutions, like Okta, AD FS and PingFederate.

Broad multifactor authentication

support: CrowdStrike Falcon Zero Trust supports multiple MFA solutions, including Okta, Azure MFA, PingID, RSA CAS, Duo and more.

Extended protocol coverage:

CrowdStrike Falcon Zero Trust provides granular visibility and control over encrypted protocols like NTLM and LDAPS, which are difficult to detect with traditional tools like SIEM and UEBA.

Extensive API coverage: CrowdStrike Falcon Zero Trust enables over 50+ integrations with API-based connectors, providing easy integration with identity as a service (IDaaS)/SSO, SIEM, SOAR, ticketing and asset management solutions.

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.

