Crowdstrike Products

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. Since 80% of breaches involve compromised credentials, segmenting identities, automating enforcement, and using risk based conditional access to verify authentication traffic can reduce risk and reduce IT complexity. 100+ enterprises have already secured 4M+ workforce identities in hybrid deployments.

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 IAM/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 and Azure AD

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

KEY BENEFITS

Realize value from day one

Gain unified visibility and control of access to applications, resources and identity stores in hybrid environments

Reduce MTTD/R and improve SOC analysts' efficiency and response times by cutting down on the need to do complex, error-prone log analysis

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

Enforce consistent risk-based policies to enable Zero Trust security (actions: block, allow, audit, or step up using MFA) with zero friction

Save log storage costs by storing only relevant authentication logs

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

Customizable security posture overview – Analyze user risk and behavior changes over time, like increase in account lockouts, high risk endpoints, compromised passwords, and so on, to get an overview of the attack surface of the organization

AUTOMATE

Enable real-time identity threat detection and protection without looking back into logs. 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 across on-premises and hybrid identity stores. Inspect live authentication traffic, including encrypted protocols (e.g. LDAP/S)

No logs, 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 ML-powered detection rules. With advanced analytics and patented machine learning technology ,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 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, like 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 platform's risk score and high-fidelity information with minimal effort to other apps (for example, ADFS, SSO, IT systems and over 50+ integrations) using API-based connectors.

VERIFY

Secure user access to applications, tools and resources with zero friction user experience. Ensure consistent login experience for genuine users, but automatically step up authentication when the risk increases.

Zero friction identity verification with flexible policies – Define and enforce policies with simple rules, with Falcon Zero Trust's adaptive analysis, eliminating the need to write complex static conditions for every user. The rules are based on authentication patterns, behavior baselines and individual risk scores to verify identities using MFA and secure 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 on tools like PowerShell and protocols like RDP over NTLM - and reduce the attack surface

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

FRICTIONLESS ZERO TRUST

Multi-Directory Identity Layer Support – CrowdStrike Falcon Zero Trust supports Microsoft Active Directory, Azure Active Directory, and also integrates with SSO and federation solutions, like ADFS, PingFederate, and Okta.

Broad Multi-Factor Authentication Support – CrowdStrike Falcon Zero Trust supports multiple MFA solutions, including but not limited to Azure MFA, PingID, RSA CAS, Duo, Okta and many others.

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 IDaaS/SSO, SIEM, SOAR, ticketing and asset management solutions.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. backed by 24/7 managed hunting. There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

Learn more at **www.crowdstrike.com**