DELL Technologies

Dell SafeGuard and Response

CrowdStrike Falcon® Identity Threat Protection

Key Benefits

- **Gain visibility of workforce identities across multi-directory environments**
  Falcon Identity Threat Protection enables unified visibility and control of user access to applications, resources and identity stores, with actionable insights into user behavior and risks, eliminating security blindspots across hybrid environments.
- **Get hyper-accurate threat detection and reduce response times dramatically**
  Falcon Identity Threat Protection reduces false positives, brings down the mean time to detect and resolve incidents by eliminating the need for complex, error-prone log analysis, and improves SOC analysts' efficiencies by cutting down alert fatigue.
- **Enable real-time prevention of identity-based attacks with conditional access policies**
  Falcon Identity Threat Protection enforces consistent risk-based policies to automatically block, allow, audit or step up authentication for every identity, and at the same time ensuring a frictionless login experience for genuine users.

Multi-directory identity protection across on-premises and clouds

CrowdStrike Falcon® Identity Threat Protection, a part of the CrowdStrike Falcon® Platform, enables frictionless security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics. Breaches involve compromised credentials, and therefore segmenting identities, automating enforcement and using risk-based conditional access to verify authentication traffic can help 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, such as increase in account lockouts, high-risk endpoints and compromised passwords to get an overview of the attack surface of the organization.

Automate

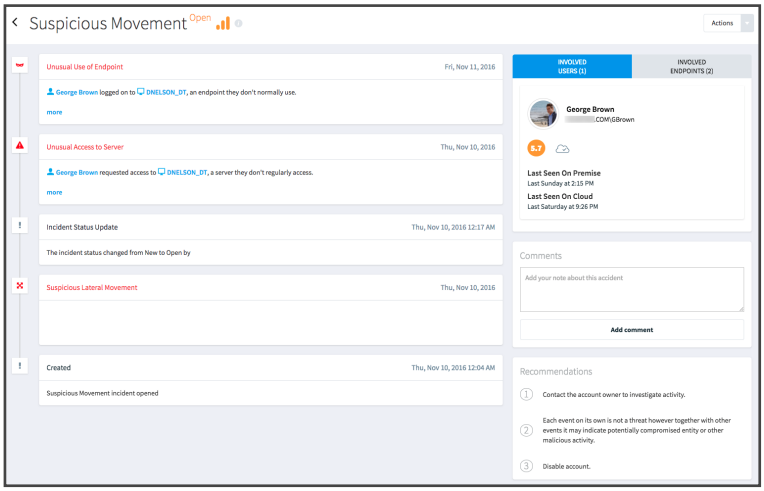
Enable real-time identity threat detection and protection without time-consuming log processing. Eliminate risky guesswork and prioritize authentication tasks based on 100+ behavior analytics and risk factors for every account.

Learn more at www.Dell.com/endpoint-security

CROWDSTRIKE

DELL Technologies

- **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 Identity Threat Protection'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 pre-defined 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 Identity Threat Protection adaptive analysis, eliminating the need to write complex static conditions for every user. Policies are based on authentication patterns, behavior baselines, individual user risk score and device risk score (via API integration) 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 your security analysts can focus on critical security incidents. Additionally, resolve these incidents with effortless API integrations into SOAR, SIEM and ticketing platforms.

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com, for more information about the Dell solutions to help improve your security posture

Learn more at www.Dell.com/endpoint-security

CROWDSTRIKE