CROWDSTRIKE

CrowdStrike Products

Data Sheet

Falcon Identity Threat Detection

Detect identity threats in real time

See live identity attack traffic

CrowdStrike Falcon® Identity Threat Detection, one of Falcon's identity threat detection and response (ITDR) modules, provides visibility for identity-based attacks and anomalies, comparing live traffic against behavior baselines and rules to detect attacks and lateral movement. With real-time alerts, Falcon Identity Threat Detection provides visibility into compromised credentials across hybrid identity stores. Since most breaches involve compromised credentials and lateral movement, the best path for securing every domain in your environment is by automating threat detection and creating dynamic risk profiling and alerting on identity traffic.

Adversary-focused detections

Understand adversary behavior and attack paths to protect sensitive data and crown jewel resources.

Real-time traffic alerting

Detect anomalous activity without requiring logs. Falcon Identity Threat Detection offers threat detection, a low false positive rate and the ability to detect threats that are difficult to detect via post-event, log-based security tools.

Hybrid identity store-ready

Falcon Identity Threat Detection works for identity stores on-premises or in the cloud, and for users/applications anywhere without any agents on endpoints or servers outside the domain controllers.

Key benefits

- Discover all identities across the enterprise, including stale accounts, with password hygiene
- Verify identity store (e.g., Active Directory, LDAP/S) security to discover weakness across multiple domains
- Investigate authentication events and questionable user behavior
- Group events around user, device, activity and more for improved incident response
- Gain unified visibility for authentication traffic to applications, resources and identity stores
- Reduce mean time to detect and respond, and improve SOC analysts' efficiency and response times by cutting down on the need to do complex, errorprone log analysis
- Improve alert fidelity and reduce noise by recognizing true positive events of interest

Key product capabilities

Discover all identities — even stale accounts — and detect identity threats in real time.

Extended protocol coverage

Falcon Identity Threat Detection provides granular visibility over incidents involving protocols like NTLM, Kerberos, SMB and LDAP/S, which are impossible or difficult to detect with traditional tools like next-generation firewalls, and user and entity behavior analytics (UEBA).

Speed to value

Most installations take less than an hour to see all identities on the network and start identifying anomalies immediately.

Behavior-based indicators and profiling

Falcon Identity Threat Detection profiles are based on both static information from identity stores and dynamic information in real time to catch insider threats, lateral movement and privilege or service account abuse. Eliminate risk guesswork and prioritize authentication tasks based on over 100 behavior analytics and risk scores for every account.

Visibility into identity store attacks

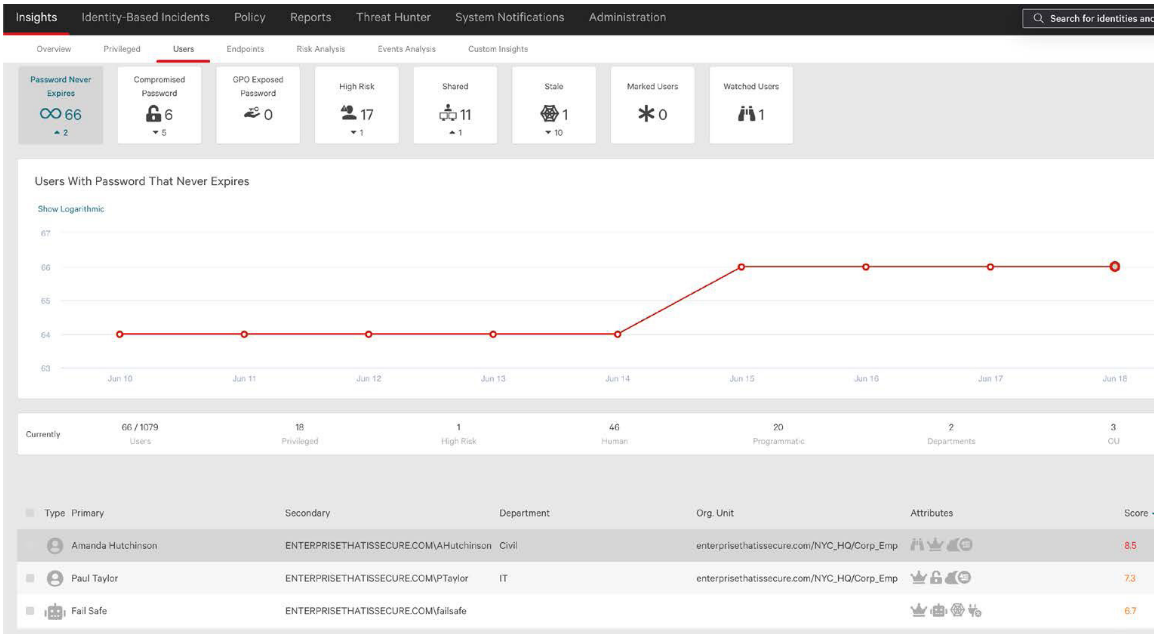
Detect identity store threats (and typical red-team exercise tests) like NTLM/LDAPS protocol threats, Golden Ticket attacks, Pass-the-Hash and other credential theft, as well as persistence techniques. Safely lure adversaries away from high-value resources and gain dedicated insights into their attack paths.

Tools for incident response

The Falcon Identity Threat Detection internal Threat Hunter feature offers visibility for all credential attacks and incident response, showing the chain of activity and subsequent increase in risk score. Threat Hunter is easy to use, requiring no command-line interface or sophisticated security knowledge to operate and administer. It integrates with many popular ticketing platforms.

Deep integration with other security tools

Falcon Identity Threat Detection can export in common event format (CEF) or Log Event Extended Format (LEEF) to any SIEM or to SOAR tools via API.



Password Never Expires 66 ▲ 2
Compromised Password 6 ▼ 5
GPO Exposed Password 0
High Risk 17 ▼ 1
Shared 11 ▲ 1
Stale 1 ▼ 10
Marked Users 0
Watched Users 1

Users With Password That Never Expires

Currently 66 / 1079 Users; 18 Privileged; 1 High Risk; 46 Human; 20 Programmatic; 2 Departments; 3 OU

Type Primary	Secondary	Department	Org. Unit	Attributes	Score
Amanda Hutchinson	ENTERPRISETHATISSECURE.COM\AHutchinson	Civil	enterprisethatissecure.com/NYC_HQ/Corp_Emp		8.5
Paul Taylor	ENTERPRISETHATISSECURE.COM\PTaylor	IT	enterprisethatissecure.com/NYC_HQ/Corp_Emp		7.3
Fail Safe	ENTERPRISETHATISSECURE.COM\failsafe				6.7

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

Free trial →