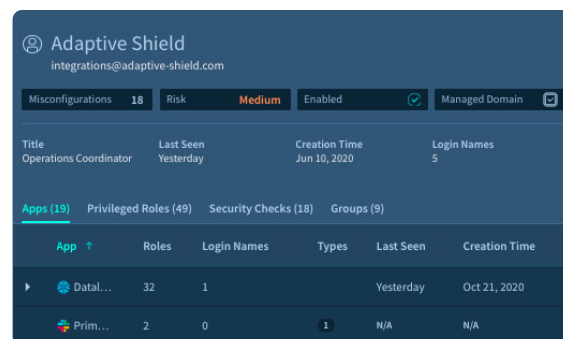


Falcon Shield: Securing Non-Human Identities

Gain visibility into service accounts, OAuth authorizations, and others

Threats come from all user types

CrowdStrike Falcon® Shield easily identifies non-human identities (NHIs) within the software as a service (SaaS) stack. Service accounts, OAuth authorizations, and API keys are all authorized non-human accounts with access to SaaS applications. These types of accounts fulfill critical roles within the SaaS ecosystem, adding functionality, carrying data, and ensuring applications perform as required.



NHIs are rarely required to use multifactor authentication (MFA) or single sign-on (SSO) when logging in. They work 24/7, invisibly performing tasks, and they are given broad permission sets. As a result, they are an inviting target to threat actors. By commandeering a non-human account with high privileges, threat actors can gain full access to everything within the application.

Falcon Shield provides full visibility into non-human accounts

User inventory

Monitor NHIs with the same tools security teams use to track human accounts.

Non-human configuration monitoring

Conduct security checks to ensure controls are in place to limit privileges granted to NHIs.

Permission trimming

Review granted scopes to ensure NHIs are not over-permissioned.

Threat detection

Identify anomalous behaviors by NHIs that could indicate malicious activity.

Non-human SaaS attack examples

Account hijacking

A non-human account with high permissions created a suspicious inbox rule, which would have compromised a user's email account.

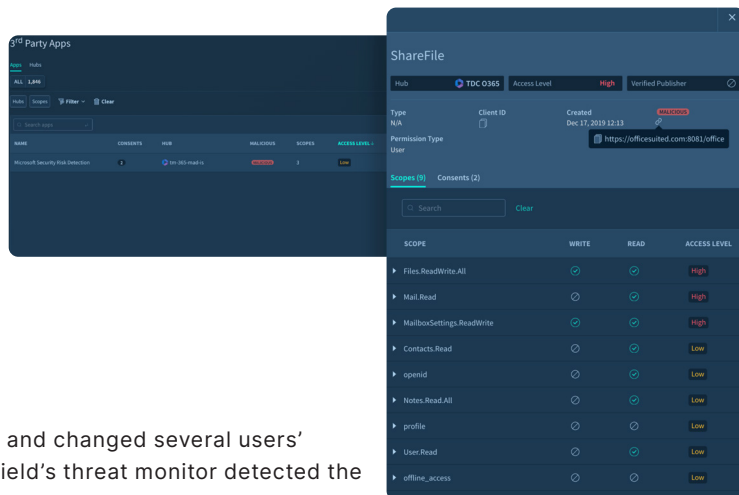
A Falcon Shield security check detected the change and triggered an alert, which prevented any damage from taking place.

Payday surprise

A non-human account accessed an HR system and changed several users' direct deposit bank account details. Falcon Shield's threat monitor detected the sensitive activity coming from a suspicious source and alerted security teams. As a result, the employees received their paychecks as expected.

Malicious apps

A connected app with significant scopes was flagged as malicious by Falcon Shield's threat monitor. The application had full access to users' email accounts but was stopped before a breach occurred.



[Learn more](#)

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/>

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

