

Falcon Shield

Key features and capabilities of CrowdStrike's SaaS security solution

Security risks are growing for software as a service (SaaS) applications. CrowdStrike Falcon® Shield prevents adversaries from exploiting misconfigurations and accounts and delivers full visibility and control into misconfigurations, identities, and threats targeting your SaaS applications.

Falcon Shield provides:

- Misconfiguration Management
- Shadow SaaS Discovery
- Identity Security Posture
- Device-to-SaaS Security Posture
- Permissions Inventory
- Data Inventory
- SaaS Threat Detection
- AI Agent Discovery

Misconfiguration Management

Gain continuous, deep visibility and control of SaaS misconfigurations across your SaaS stack — and easily collaborate with app owners.

With Falcon Shield, every configuration in the SaaS stack is tracked in a centralized location. This enables business users and security professionals to see failed security checks itemized by severity levels, app security scores, affected users, impacted compliance, and remediation steps needed to improve the application's security posture.

The leading causes of SaaS misconfigurations are a lack of visibility across the SaaS stack and providing too many teams with access to SaaS settings.¹

¹ Cloud Security Alliance, [2022 SaaS Security Survey Report](#)

Key features and capabilities:

- **Automated checks of your key security settings:** Eliminate manual SaaS security checks covering thousands of configurations
- **Near real-time monitoring, alerts, and ticketing:** Receive configuration drift alerts immediately, and seamlessly create tickets with your ticketing system of choice
- **Alignment with compliance standards:** Check which settings need to be changed to help meet the requirements of leading compliance standards or in-house standards
- **Centralized data for the entire SaaS stack:** Review the company's SaaS security posture for the entire stack from a single dashboard
- **Fully configurable security checks:** Customize security checks and priority levels to meet the security needs and posture of your organization
- **Over 200 out-of-the-box integrations:** Connect your SaaS stack with pre-built SaaS checks that begin looking for high-risk misconfigurations within minutes of onboarding

Shadow SaaS Discovery

Gain visibility into shadow SaaS applications while detecting threats from malicious apps.

Falcon Shield delivers shadow SaaS discovery by leveraging Falcon's existing endpoint telemetry to provide comprehensive visibility into SaaS usage across the enterprise — without agents, integrations, or configuration. By correlating real user activity with posture integrations and identity context, organizations will gain crucial insight into sanctioned and unsanctioned SaaS environments. This unified approach enables security teams to identify risky shadow SaaS usage, prioritize the risk, and apply targeted governance aligned to business structure — maximizing ROI from existing Falcon investments while reducing operational complexity.

With Falcon Shield, you can also see how many third-party applications are interconnected to your SaaS stack, the name of each app, and each app's risk level based on granted scopes. Security teams can see which users authorized the app, app and vendor details, and the app installations, enabling them to make risk-based decisions on whether to disable the app.

Each third-party SaaS app check includes the following:

- **Vendor name and verification status:** Know exactly where the app came from and whether it may be malicious
- **Installation date:** Gain insight into how long the app has been connected
- **Who connected the app:** Check that the app is connected to current employees who are in the company identity provider (IdP) and not disabled in the company's HR platform
- **Description of the app:** See what the app does to check if the requested scopes of access are necessary
- **Scopes granted and risk severity:** Review access and permission granted and get insight into the risk of each access and permission
- **Usage dates:** See when each app was last used and a summary of when each app actualized its scopes

Key capabilities:

- **Visibility into connected apps:** Clarify your exposure and attack surface with an exceptional view into apps connected to the SaaS stack
- **Malicious app threat detection:** Discover unknown connected apps that may pose a danger to your data and operations

Falcon Shield

- **Risk quantification:** Measure your risk by reviewing apps that have requested high-risk scopes, including the ability to edit, write, and delete content as well as the ability to email and share materials
- **Third-party app discovery:** Create notifications and alerts when new applications are integrated into the SaaS stack
- **Third-party app risk reduction:** Detect over-privileged applications and trim unnecessary scopes or replace the applications with similar ones that require low-risk scopes
- **Dormant app discovery:** Find apps that are connected but unused, closing a backdoor into your SaaS applications
- **Shadow SaaS discovery:** Automatically discover and catalog all SaaS applications using Falcon endpoint DNS telemetry — no agents, integrations, or setup required
- **Instance-level discovery:** Map your organization's complete SaaS footprint by identifying distinct tenant instances across cloud services — this comprehensive discovery enables security teams to maintain an accurate inventory of cloud presence, track organizational SaaS adoption patterns, and strengthen security governance across the enterprise cloud ecosystem

Identity Security Posture

Govern all users, from employees and external users to non-human accounts.

Every human identity, non-human identity (NHI), and AI agent is a potential entryway into the SaaS stack. Falcon Shield strengthens organizations' rich identity fabric, preventing unauthorized users from accessing corporate SaaS applications. With Falcon Shield, you can oversee all identity-based access to apps, provide security teams and app owners with full visibility into their users, and put sufficient protections in place to keep threat actors out.

Key features:

- **User risk level:** View user risk based on role, privilege level, and current configurations
- **User inventory:** See the list of active, deactivated, dormant, and unmanaged users
- **User SaaS profile:** View user roles, privileges, all of the apps users have access to, failed security checks, devices, groups, departments, titles, last login, and all usernames

Key capabilities:

- **Permission trimming:** Review access and permissions to confirm users have an appropriate level of access based on their roles and needs
- **User deprovisioning:** Create lists of users who are dormant, who are disabled in the Active Directory or LDAP, or who no longer require access, and deprovision their access
- **External user tracking:** Track external users to confirm they still require access and manage their privileges
- **Unmanaged user discovery:** Capture users with access who are not being managed by the company's IdP
- **Misconfiguration prioritization:** Identify users with the highest privileges and largest number of high-risk misconfigurations to set remediation priorities
- **Visibility of AI agents:** Discover AI agents across various SaaS platforms and check agents for misconfigurations, excessive permissions, anomalous behavior, and unmonitored integrations

Use cases:

- **Discover dormant accounts:** Dormant accounts, such as those involved in the initial application setup or ones that are no longer in use, expand the attack surface by providing an additional pathway for threat actors to enter the app. These accounts often have easy-to-remember passwords and may have expansive permission sets. Using Falcon Shield, organizations have the visibility needed to disable or delete these dormant accounts.
- **Aggregate users:** To achieve effective identity security, organizations must develop user profiles based on all of their online behaviors. When a user logs into several applications using different email addresses or usernames, Falcon Shield aggregates these accounts in a single user view. This provides organizations with a holistic view of each user's digital footprint and communication patterns.
- **Provision and deprovision users:** When adding users to an application, companies should follow the principle of least privilege and grant only the permissions necessary for the users to complete their job functions. Falcon Shield allows organizations to compare privileges between users with similar roles, titles, and departments to confirm that users are not over-permissioned. When employees leave the organization, their access must be fully removed from every application. While applications that are connected to the corporate IdP will automatically remove access through single sign-on (SSO), users with local access must be manually deprovisioned. Falcon Shield helps organizations discover users from across the SaaS stack that must be immediately deprovisioned.
- **Discover AI agents:** Falcon Shield provides unified discovery and classification of AI agents across SaaS platforms, delivering granular visibility into agent configurations, tool and API access, data sources, and ownership. Agent attributes are normalized into a consistent framework across vendors, enabling security teams to identify risky behavior, excessive privileges, and unmanaged agents. This foundation enables immediate cross-platform governance and compliance monitoring as AI agent usage rapidly expands across enterprise environments.

Device-to-SaaS Security Posture

Monitor risks from devices that are accessing your SaaS stack.

When employees access company data using a device with poor security hygiene, they put data at risk. Falcon Shield integrates with leading endpoint security tools and SaaS app user login data to create a device inventory that delineates every device that has accessed the SaaS stack and the user who used the device. Security professionals gain visibility into risks emanating from the devices and can adjust user access and permissions.

Key features:

- **Identification of privileged users with critical vulnerabilities:** Know which users are accessing SaaS applications with high-risk devices
- **Device posture score from endpoint platform:** See the CrowdStrike Falcon® Zero Trust Assessment (ZTA) score for all managed devices that access the SaaS stack
- **Device platform and operating system details:** See which devices are accessing SaaS data with out-of-date operating systems
- **Reporting:** Generate device management and device compliance policy reports
- **User data generation:** View usernames, SaaS roles, privileged roles, devices associated with users, and whether devices are in the organization's mobile device management (MDM) solution

Key capabilities:

- **Identify privileged users with critical vulnerabilities:** Discover users with high-risk permission sets using devices that could compromise the SaaS app
- **Create and run device security checks:** Automatically run security checks to identify devices that are not connected to the endpoint and vulnerability management system
- **Catalog device vulnerabilities:** Create cross-company reports of vulnerabilities to see the scope of the issue
- **Remediate device vulnerabilities:** Share on-screen step-by-step directions with device owners to upgrade the security hygiene of their devices
- **Discover out-of-date agents:** Prevent malware attacks by identifying users with out-of-date agents and limiting their access

Permissions Inventory

Easily manage user access through a single integrated dashboard.

Software platforms contain two types of permissions: those that govern the use of the platform and those that limit access to information. This is driven by the need to shield sensitive data contained within the platform. However, the user entitlements of some key applications — including Salesforce, Workday, Microsoft 365, and Google Workspace — are often complex layers juxtaposing user profiles, permission sets, and custom permissions. These applications lack a single view of user permissions.

The Falcon Shield permissions inventory provides platform owners with advanced visibility of user permissions, enabling them to see precisely which users have access to what — all the way down to the field level.

Key features and capabilities:

- **View users by profile:** See all users by profile
- **View permissions by user:** See all permissions granted to a single user
- **Manage all tenants in a unified view:** Monitor users from all instances
- **Discover active users to offboard:** Find users who have retained access after leaving the company
- **Drill down on permissions:** See the level of risk stemming from each user's access across all applications

By application (partial list):

- **Salesforce:** Displays fine-grained permission allocation — down to the object and field level — from profiles and permission sets
- **Workday:** Shows user access (including custom elements) for different roles, security groups, and organizations
- **Microsoft 365:** Presents each role, its associated permissions, and the users assigned to it

Use cases:

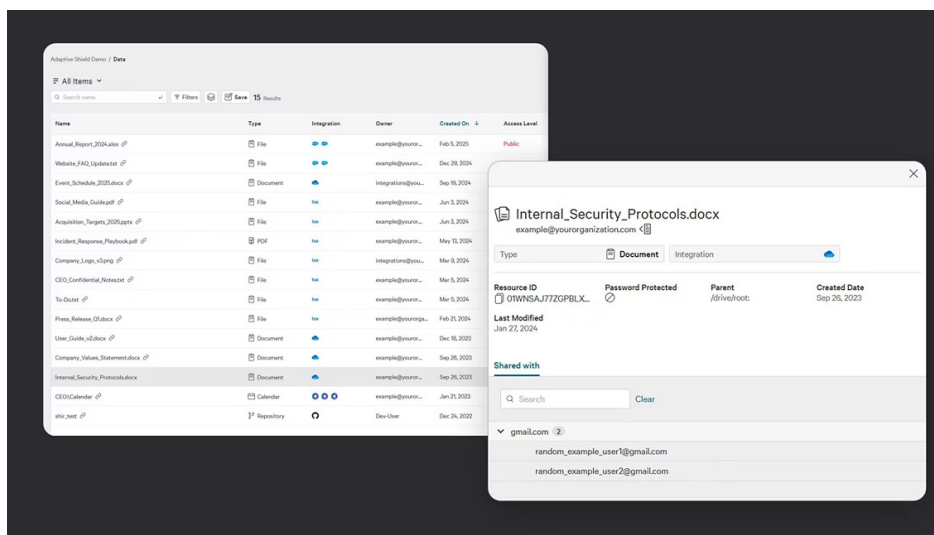
- **Certification campaign:** Review and validate user permissions as part of a user audit
- **Identity hardening:** Identify over-privileged accounts and users
- **Privilege creep prevention:** Continually assess privilege and prevent excessive permissions
- **Unified cross-platform visibility:** Develop SaaS-wide views of users and their permissions

Data Inventory

Secure documents, files, repositories, and other structured data, and prevent and detect data exposure from across the SaaS stack.

Enterprises create, store, and share a vast volume of documents, projects, source code, and files in their SaaS applications. Preventing data from leaking out of the SaaS stack and going to unauthorized users has become a priority.

Falcon Shield secures data in the SaaS stack in two ways. First, it monitors settings and alerts users when high-risk settings expose data to the public. Second, it reviews file share settings. Any publicly accessible or externally shared data is flagged and included in the Data Inventory, allowing users to secure this data.



Best practices for sharing data

SaaS applications are designed to encourage and simplify internal and external collaboration. Though collaboration is important, it must be balanced with security considerations and secured using each application's native access controls. Documents should be shared with specific individuals rather than through links that don't require any type of sign-in. When the application allows for it, expiration dates should be used to restrict access after a predetermined time period. Through the Falcon Shield Data Inventory, security teams have clear visibility into unprotected resources and the steps required to secure them.

Prevention through deep SaaS visibility

Falcon Shield's security checks automatically monitor all file-sharing configurations, including those in Microsoft 365, Salesforce, and Google Workspace. When configurations drift, Falcon Shield sends an alert warning users that their files, boards, repositories, and projects may be at risk.

 **External Links File Permissions**
Security Domain: Data Leakage Protection

Status **Passed** ⓘ

Impact **High** (Edited) ✎

Integration  **Internal Portals** ⌵

Description
Externally shared links can only give "view" permissions.
[➤ More info](#)

[Overview](#) [Compliance](#) [Journal](#)

▼ Remediation Plan

In the SharePoint admin center → Policies → Sharing → File and folder links → "Choose expiration and permissions options for Anyone links" → navigate to "These links can give these permissions" → Files → choose "view" from the list.

Detection in the data inventory

The Falcon Shield Data Inventory lists files that are either public with a link or shared with external users. These detections enable users to secure their documents and protect against data leakage.

Each item listed in the Data Inventory includes:

- File name
- File type
- Application source
- Link to file
- Owner
- Created date
- Last accessed date
- Last modified date
- Expiration date
- Password protection

This unique visibility into resources allows organizations to secure files before the data is discovered by adversaries.

Use cases:

- **External content sharing:** Discover documents shared with external users beyond the corporate security perimeter
- **Content that has never been accessed:** Find publicly shared content that has never been accessed and revoke access
- **Stale content:** Find documents without an expiration date that haven't been accessed in a significant amount of time
- **Publicly accessible calendars:** Discover user calendars that are shared publicly, which can lead to leaked meeting invites and social engineering attacks

SaaS Threat Detection

Monitor user behavior to stop threats.

Falcon Shield's SaaS threat detection utilizes data and behavior from across the entire SaaS stack to detect suspicious activities. Through its broad coverage of integrations (200+ out-of-the-box app integrations), the different data sources provide context into each alert while significantly limiting false positives.

Though each application has threats specific to its domain, the following threats are frequently seen throughout the SaaS stack. If you detect any of these threats, follow the step-by-step mitigation guidance for the application or your incident response policy.

Threat detection capabilities

The following is a partial list of the SaaS threats Falcon Shield can detect:

- **Browser downgrade from an untrustworthy autonomous system number (ASN):** Detection of a user accessing an application from an untrustworthy ASN while using an older version of a browser than normal
- **Operating system downgrade from an untrustworthy ASN:** Detection of a user accessing an application from an untrustworthy ASN while using an older version of an operating system than normal
- **Simultaneous suspicious activity:** Detection of one user accessing two applications from different locations at the same time
- **Successful password spraying attack:** Detection of a cluster of login attempts from a single IP address, leading to one successful login
- **Unusual operating system from an untrustworthy ASN:** Detection of a user accessing an application from an untrustworthy ASN using an unusual operating system, such as a Windows user logging in on a macOS device

Threats are often built on multiple indicators of compromise (IOCs). The following are examples (partial list) of the IOCs Falcon Shield detects and monitors as it scans for threats, and users can also create their own threat detection by combining IOCs:

- **Abnormal download activity:** Detects users performing multiple download activities in a single session beyond their baseline activity
- **Anomalous tokens:** Detects abnormal characteristics in a token, such as a lifetime token or a token played from an unfamiliar location
- **Credential stuffing:** Detects a successful login from an IP address that exceeded the threshold of password attempts
- **Failed login spike:** Detects failed logins on an ASN from multiple user accounts
- **Honeytoken activity:** Detects when a honeytoken account participates in suspicious activity
- **Leaked credentials:** Detects user logins with passwords that have been breached and appear in some third-party marketplace sites
- **Unusual private VPN sign-in:** Detects when users access an application using an unusual private VPN account

Key features and capabilities:

- **MITRE ATT&CK® mapping:** Enhance incident response capabilities and improve threat detection and mitigation by aligning observed or potential attack techniques with the MITRE ATT&CK framework
- **Alerts and notifications:** Get alerts in multiple channels — such as email, Slack, or Microsoft Teams — indicating potential security incidents or suspicious activities that require immediate investigation or response
- **SIEM and SOAR integrations:** Seamlessly integrate with your existing security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools, such as CrowdStrike Falcon® Next-Gen SIEM and CrowdStrike Falcon® Fusion SOAR, improving threat correlation and incident response efficiency
- **Native integration with Falcon Next-Gen SIEM:** Falcon Next-Gen SIEM natively ingests and pre-enriches Falcon Shield SaaS logs as first-party data to deliver unified threat visibility across SaaS, endpoint, identity, and cloud environments, enabling powerful cross-domain detection, threat hunting, and incident response across the entire attack surface
- **Remediation guidance:** Get actionable recommendations and step-by-step guidance to address and mitigate vulnerabilities, weaknesses, or compromises in the event of a security incident

[Learn more about Falcon Shield](#)

[Watch a demo](#)

[View all 200+ supported integrations](#)

[Free trial](#)

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: www.crowdstrike.com

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

