

Falcon Shield: SaaS Security for Tech Companies

Implement agile security

Code sits at the heart of every tech company. Using software as a service (SaaS) tools like GitHub, Jira, ServiceNow, and ShiftLeft, they develop, test, and optimize their code. However, the very SaaS tools that enable high levels of collaboration and communication can undermine these efforts. Recent repository breaches have demonstrated just how sensitive fragile share settings can be. Code that has taken months and millions of dollars to develop can be stolen in a moment.

The CrowdStrike Falcon® Shield SaaS security posture management (SSPM) solution improves the security posture of the entire SaaS stack, from workflow tools to storage repositories. It alerts security teams when high-risk configurations are changed, monitors users and devices accessing SaaS applications, and reviews permission settings for every connected third-party app. Most importantly, it identifies threats from across the SaaS stack, enabling SOC teams to get ahead of breaches.

Benefits of SSPM

- Secure high-risk misconfigurations
- Detect threats from across the SaaS stack
- Identify high-privilege users using low-hygiene devices
- Correlate SaaS settings to support SOX compliance efforts
- Prevent high-risk connected app access
- Detect and prevent data leakage

Use case spotlight

Protect software

development: Prevent threat actors from detecting secrets, keys, or other tokens while scanning repositories

Secure data lake

insights: Prevent unwanted access by restricting the ability for guests to edit and manage content in data lakes

Limit access to plans:

Close data leaks before they happen by limiting publicly accessible dashboards and publicly accessible projects in project management applications

Support SOX compliance

Tech companies often adhere to SOX compliance to satisfy their regulatory requirements. Using Falcon Shield, security teams can see how each application's security settings compare to the different standards. The user interface is designed to mirror compliance requirements, making it easy for users to compare their security posture with their chosen standard.

 SOC 2 TYPE 2 The SOC 2 is a report based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) existing Trust Services Criteria (TS... Read more		29	171/430
		Apps	Failed Checks
Status	Apps	Search	Clear
		Export	Collapse All
▼ Logical and Physical Access Controls 156/380 Failed			
▶ CC6.1. ...logical access security software, infrastructure, and architectures over protected information assets... 91/207 Failed			
▶ CC6.2. ...the entity registers and authorizes new internal and external users whose access is administered by the entity... 17/40 Failed			
▶ CC6.3. ... authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles... 14/29 Failed			
▶ CC6.4. ... restricts physical access to facilities and protected information assets... 10/20 Failed			
▶ CC6.6. ... logical access security measures to protect against threats from sources outside ... 9/30 Failed			
▶ CC6.7. ... restricts the transmission, movement, and removal of information to authorized internal and external users and processes... 9/16 Failed			
▶ CC6.8. ... implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software ... 18/67 Failed			
▼ System Operations 21/68 Failed			
▶ CC7.1. ...the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities... 18/45 Failed			
▶ CC7.2. ...monitors system components and the operation of those components for anomalies that are indicative of malicious acts... 3/16 Failed			

See your SaaS security posture in minutes

1. Connect SaaS applications via API
2. See initial application security posture scores within minutes
3. Identify high-risk configurations
4. Remediate risk
5. Improve application security posture

[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/>

