

Falcon Shield

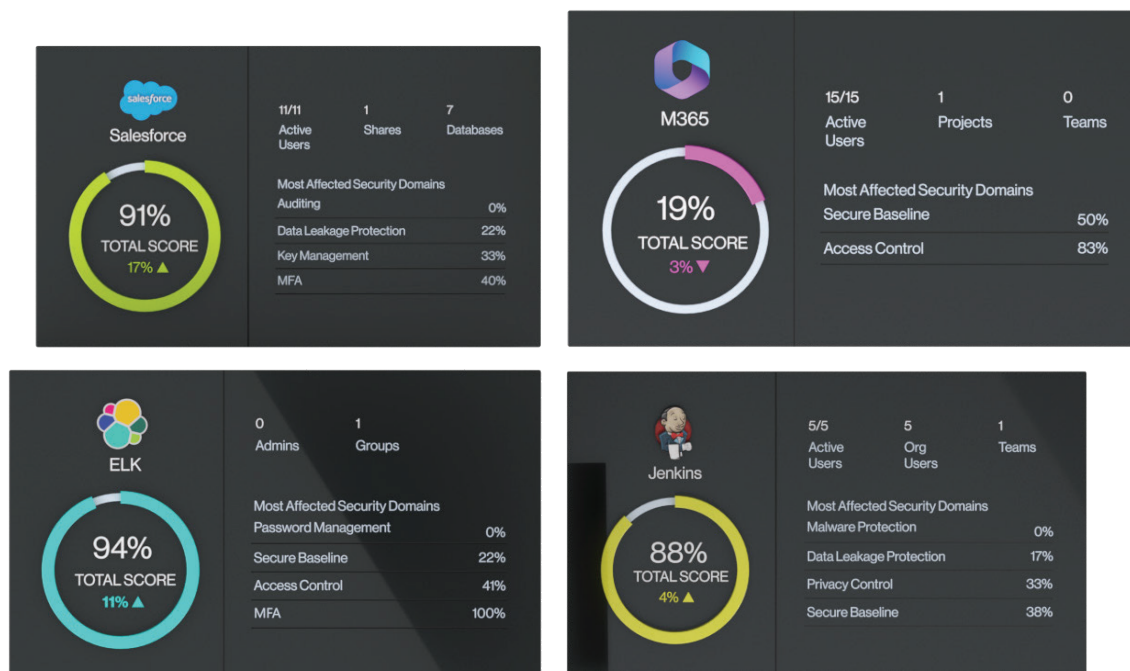
USE CASES & CORE CAPABILITIES

Secure Your Entire SaaS Stack

Gain deep, continuous visibility and control over your SaaS stack. CrowdStrike Falcon® Shield's SaaS security platform empowers you to prevent, detect and respond to SaaS threats. Easily collaborate with your app owners to fix any security drift.

Stay on Top of Security Misconfigurations

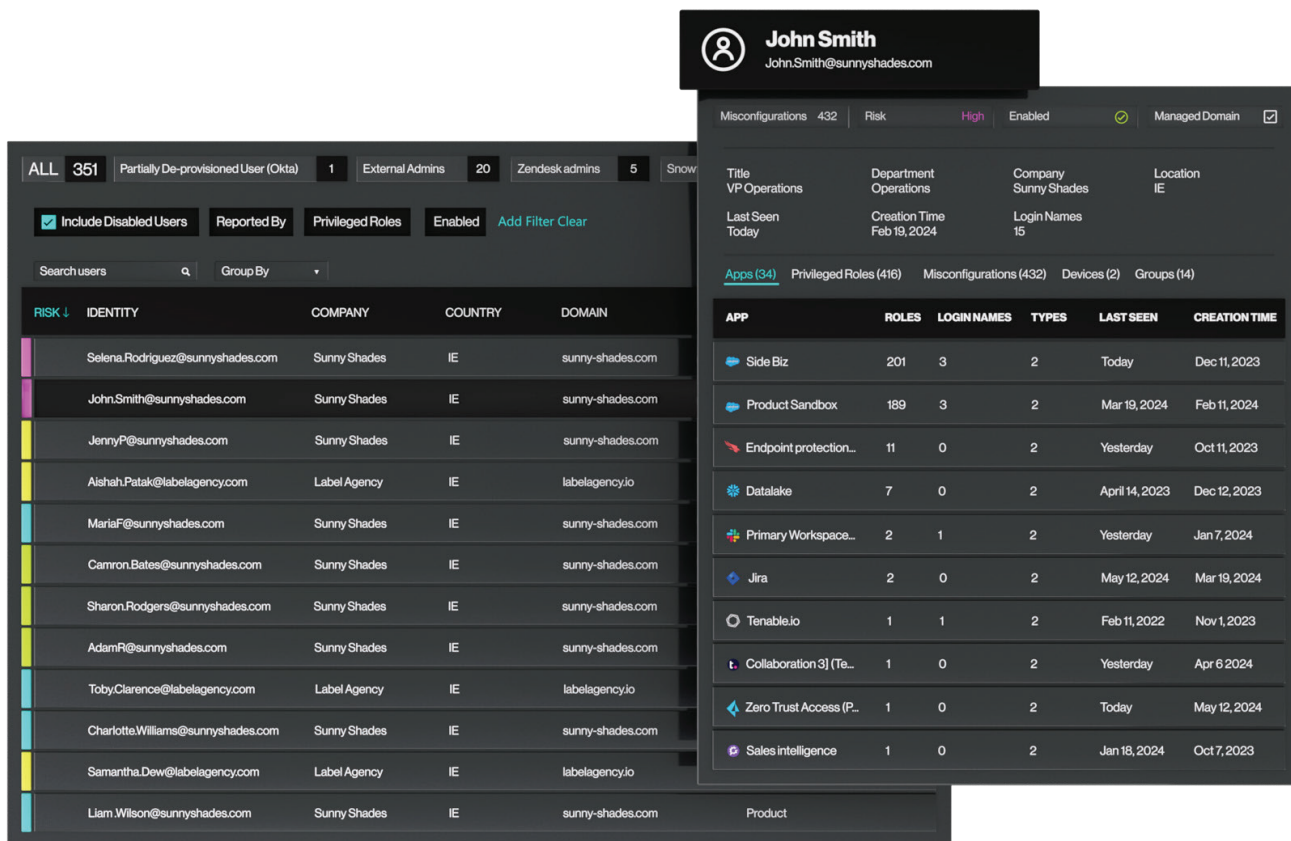
Integrate with all SaaS apps to monitor and manage security misconfigurations through in-depth security checks and auto/step-by-step remediation.



With Falcon Shield, you can achieve:

- App breadth and security depth
- Risk management prioritization by severity or security domain
- Guided remediation
- Compliance mapping

Strengthen governance of internal and external SaaS users, monitor permissions and secure non-human identities.



Identify privileged users to prioritize misconfiguration management, device management and third-party app access.

Implement the principle of least privilege (PoLP), and ensure each SaaS user has the right level of access needed while still enabling business operations.

Detect users that have been disabled in Active Directory but retained access to SaaS apps, dormant users and privileged accounts from external domains.

Identify which users are external, internal, non-human and any other categorization of choice.

Discover Connected and Shadow Apps

Detect and control all sanctioned and unsanctioned SaaS apps and other integrations connected to your core SaaS stack that can pose a risk to your business.



App Discovery

Discover and control third-party app access, connected to your core SaaS stack.

Malicious App Discovery

Identify malicious applications and gather forensics through the activity monitoring panel. These applications put data at risk of ransomware, theft and destruction.

Measure Risk Level of Connected Apps

Once connected applications are detected, understand which ones request high-risk scopes.

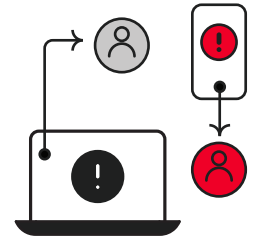
Dormant App Discovery

Find high-risk applications that have access to the SaaS stack but haven't been accessed over long periods of time.

Additional Use Cases

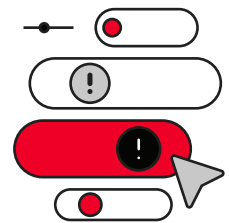
Manage Device Risk

Manage SaaS risks deriving from user devices and prioritize high-privilege users with devices that have poor hygiene, are unmanaged or are non-compliant to deliver a holistic Zero Trust approach.



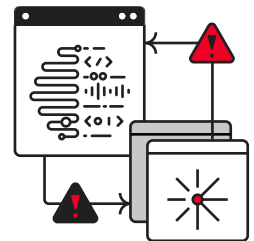
Gain Visibility into Data Exposure

Discover public and externally shared documents, files, code repositories and calendars to prevent data leaks and limit phishing attacks.



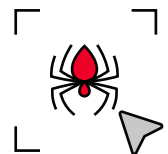
Get a Handle on GenAI

Take control of GenAI tools in your SaaS stack to prevent data leakage and unauthorized access.



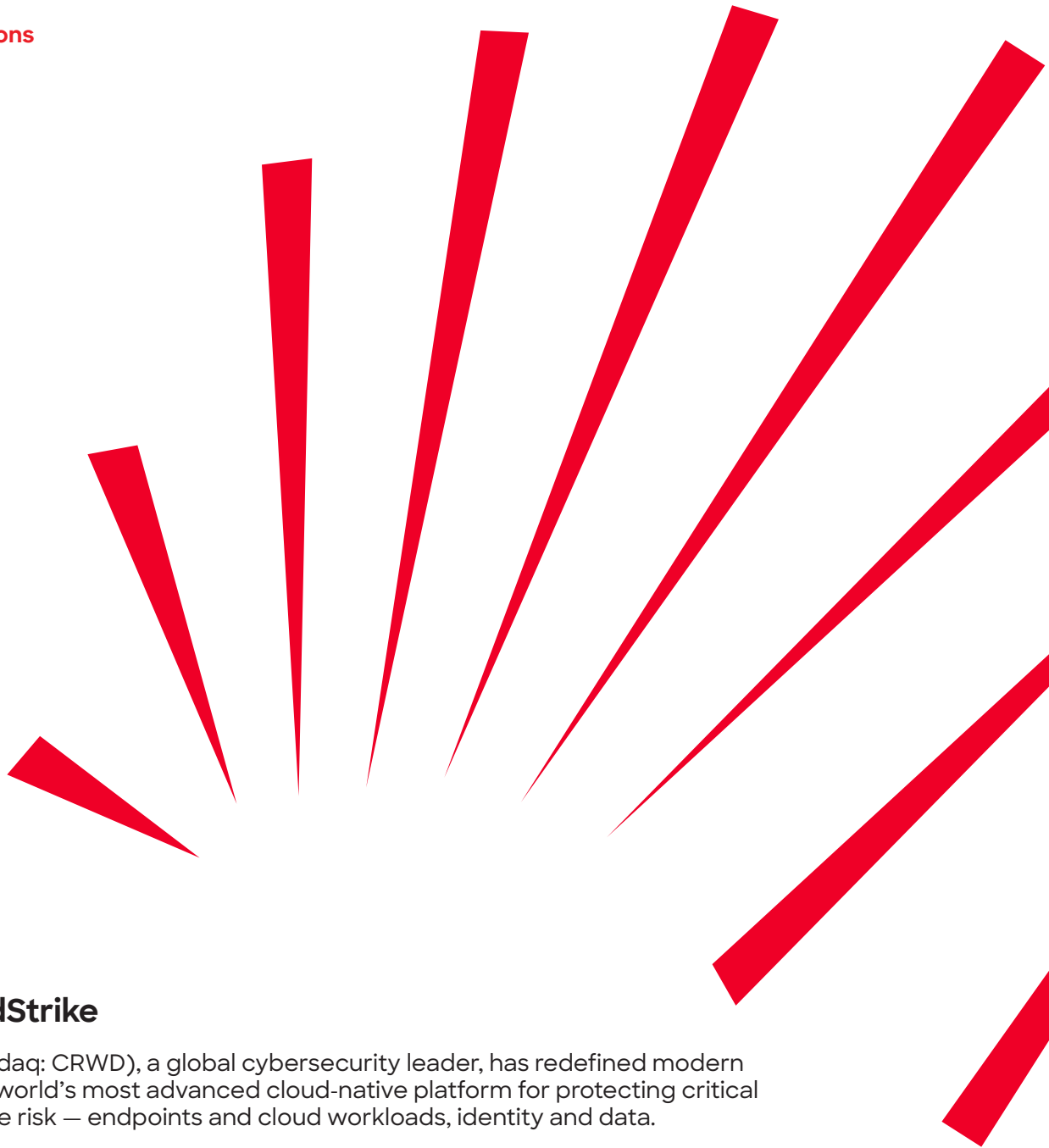
Detect and Respond to Threats

Detect and respond to identity-centric threats originating from the SaaS ecosystem such as unusual activities, malicious applications or any indication of compromise.



Falcon Shield is the only SSPM with out-of-the-box support for over 150 SaaS applications





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/>

[Watch a Demo](#)

[Contact Us](#)

