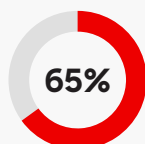


SaaS Threat Services

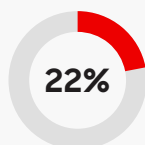
Secure your SaaS estate through proactive assessments and attack emulations

Increase confidence in your SaaS security

As global organizations adopt software as a service (SaaS) platforms at unprecedented speed to remain nimble and efficient, eCrime and nation-state adversaries are expanding their focus just as rapidly to steal and destroy victims' data. SaaS solutions proliferate and grow more complex each day, and while SaaS vendors keep improving security controls, the growing complexity exposes enterprises to misconfigurations and human errors — with potentially catastrophic consequences.



65% of organizations struggle with tracking and monitoring risks from third-party integrated apps and rectifying SaaS misconfigurations¹



Cross-domain attacks are reshaping the threat landscape, with **22% of relevant intrusions** involving threat actors accessing SharePoint²

Recognizing the urgent need for organizations to control their SaaS exposures, CrowdStrike developed SaaS Threat Services — a specialized offering to combat evolving SaaS risks. Leveraging CrowdStrike Falcon® Shield, CrowdStrike's industry-leading experts rapidly assess, diagnose, and recommend remediations across your SaaS estate. They uncover misconfigurations, risks, and threats that could lead to breaches or data tampering.

As a leader in SaaS security, CrowdStrike equips organizations with the intelligence and expertise needed to defend against evolving threats — ensuring your SaaS ecosystem remains protected in an increasingly complex threat landscape.

Key benefits

Gain full visibility into your SaaS security risks with a comprehensive assessment across communication, email, data sharing, identity management, security tools, code repositories, and more.

Prevent data leaks before they happen by rapidly identifying exposed documents and objects across 150+ SaaS applications.

Minimize excessive access, uncover shadow IT risks, harden genAI posture with dedicated security checks, and govern access to genAI applications.

Proactively close security gaps with prioritized SaaS security configuration recommendations to prevent breaches.

Uncover hidden attack pathways by identifying interconnections between SaaS apps that adversaries could exploit for data theft or destruction.

¹ Cloud Security Alliance, "The Annual SaaS Security Survey Report 2025 Plans and Priorities"

² CrowdStrike 2025 Global Threat Report, p. 41

SaaS Threat Services components

Undetected breaches in SaaS applications allow theft, tampering, and destruction of sensitive data at record speeds, disrupting business operations and triggering costly reporting requirements. CrowdStrike's advanced security services for SaaS empower organizations to reduce their SaaS risks across more than 150 apps.

SaaS Security Assessment

- **Diagnose exposed data and vulnerable identities:** Rapidly identify excessively exposed documents, files, and objects, as well as users, accounts, and applications prone to compromise.
- **Illuminate security-relevant configuration issues:** Receive recommendations to remediate vulnerable configurations such as lack of multifactor authentication (MFA) enforcement for administrators, bypassing single sign-on (SSO), poor protections against password brute force attacks, dormant identities, excessive permissions, suspicious or unauthorized third-party applications and integrations, and other misconfigured security controls.
- **Cover your entire SaaS stack:** Protect 150+ SaaS apps including those for analytics, productivity, IT, CI/CD software development, identity and access management, marketing, project management, security engineering, and more.

Compromise Assessment for SaaS

- **Identify unauthorized activity:** Identify suspicious and unauthorized user activity across the SaaS stack.
- **Find data residency violations:** Identify data being accessed from unapproved geographic locations.
- **Reveal supply chain attacks:** Zero in on third-party apps, API keys, and integrations for evidence of misuse by nation-state and eCrime adversaries.
- **Detect cross-domain compromise:** Discover malicious activity that adversaries weave between identity, device, digital workplace, and software development SaaS apps to evade detection from piecemeal solutions.

Red Team/Blue Team Exercise

- **Expose the SaaS attack chain:** CrowdStrike's SaaS Red Team experts rigorously test your prevention and detection capabilities, simulating real-world attack scenarios that range from basic to highly stealthy techniques. This approach ensures your team remains in the "growth zone," strengthening their ability to detect, respond to, and mitigate SaaS-based threats.
- **Strengthen and validate defenses:** CrowdStrike's SaaS Blue Team experts guide your defenders through simulated breach scenarios, providing continuous incident-driven insights.
- **Compound capability enhancements:** Regular exercises build SaaS detection and response capabilities, making for superior teams ready to defend SaaS estates.

SaaS Incident Response

- **Gain real-time visibility:** Speed to visibility is paramount when responding to an incident, and SaaS is no exception. Falcon Shield allows CrowdStrike Incident Response (IR) real-time visibility into an organization's SaaS estate to identify exploitable configurations, implement tailored detections, and respond to adversary activity.
- **Contain the threat:** Through real-time visibility and the intelligence-led detection rules of Falcon Shield, CrowdStrike IR takes a proactive stance to quickly identify and contain adversaries targeting your SaaS estate.
- **Investigate cross-domain attacks:** Securing both SaaS identity platforms and countless SaaS apps, Falcon Shield allows CrowdStrike IR to rapidly identify, respond, and triage cross-domain adversary activity.

Learn More →

About CrowdStrike Services

CrowdStrike Services delivers Incident Response, Technical Assessments, Training and Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations and recover from a breach with speed and precision. Harnessing the power of the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary-focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: We stop breaches.

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

Email: services@crowdstrike.com

Follow us: [Blog](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)