



The SSPM Justification Kit

This comprehensive kit can help you justify an SSPM decision internally. It contains detailed information and facts that can help you build a case and justify SSPM considerations and investments.

Table of Contents

The Role of SaaS Applications	3
The SaaS Security Challenge	4
Attack Vectors	5
Security Options	8
Fully Securing the SaaS Stack	12
SSPM and Compliance	15
Bottom Line	15
About Falcon Shield	16

The Role of SaaS Applications

Software as a service (SaaS) applications play a critical role in all businesses. They manage email, control supply chains, facilitate chat, provide support, oversee employees, store files, power websites with data-driven content, and more. They contain a wealth of data, maintain processes, and enable business operations.

What types of data do SaaS applications contain?

SaaS applications contain a wealth of corporate data.

Category of Data	Examples	Risk of Exposure
Personal data	Names, addresses, phone numbers, identification numbers, bank account info, and health records of employees, customers, partners	Significant penalties from regulatory agencies and governments, loss of trust
Company data	Financial reports, intellectual property, proprietary algorithms or secrets, source code, campaign strategies, sales forecasts, project plans	Loss of competitive edge, financial loss, damage to brand reputation
Communication data	Emails, meeting notes, recorded calls	Shared secrets, erosion of competitive edge, leaked company data, personally identifiable information (PII)

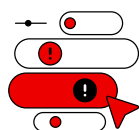
The SaaS Security Challenge

When it comes to SaaS security, there is a shared responsibility model in which SaaS vendors provide robust security controls. But at the end of the day, it is the organization's responsibility to ensure these controls are consistently implemented.

- 1 Volume and velocity of apps, users, and associated devices**
Each app has its own characteristics: UI, terminology, and security controls. It's a dynamic environment with a high pace of changes, including constantly enhanced security controls, users to add/modify/offboard, new apps being adopted, and more.
- 2 Lack of visibility**
SaaS applications are managed by business owners, and security teams often have no access and visibility into the app's security configurations.
- 3 Inability to manage applications**
Even if the security team has access and visibility into the apps, it requires the consent and help of the app owner to avoid interfering with operational workflows.
- 4 Inability to detect threats within SaaS environments**
SaaS threats are often sophisticated and are typically very subtle, making their accurate identification a significant challenges.
- 5 "Unknown unknowns"**
CISOs need to be on top of risks or vulnerabilities they are unaware of and don't even know to look for.

Attack Vectors

What types of attack vectors should security teams be aware of?

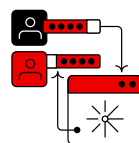


Misconfigurations

Misconfigured settings can allow unknown users to access applications, exfiltrate data, create new users, and interfere with business operations.

Identity protection

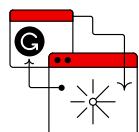
The identity-first security approach incorporates protection of the following attack vectors:



Human Identities

Consolidate visibility of user accounts, permissions, and activities across all SaaS applications, enabling effective risk management and ensuring appropriate access levels. This includes effective management of:

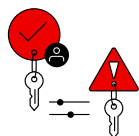
- Roles and permissions
- Privileged users and admins
- User activity level: dormant, active, hyperactive
- User classification: external/internal
- User-centric configurations (multifactor authentication, single sign-on, etc.)
- User status: joiners, movers, leavers (in many cases, leavers are not deprovisioned)
- Users with multiple login names
- Sign-in applications
- Group users
- Compromised identities
- Temporary role-based access
- Enforcing role-based access



Non-human identities

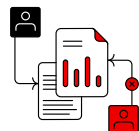
SaaS-to-SaaS connected applications: Manage the risk of interconnected apps through automated discovery of all SaaS applications that are present in the organization. Gain visibility into the requested scopes of connected apps, find out whether they are legitimate or malicious, and assess the level of risk they pose to your SaaS environment. This includes OAuth integrations, service accounts, API keys, and more.

Shadow IT: Implement automated discovery of all shadow apps that are not connected to any other applications and their level of risk.



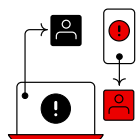
SaaS entitlement management

With complex and dispersed permission structures — along with different terminology and UIs within and between apps — it is almost impossible for security teams and app owners to facilitate security and compliance audits. These permission structures are highly complex in environments such as Salesforce, Workday, Microsoft 365, Zendesk, Google Workspace, and others. Managing these permission structures includes trimming permissions and detecting users with multiple login names, as well as managing SAML versions, sign-in apps, assigning group users, browser extensions and more.



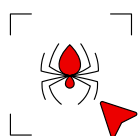
Data security

Organizations must detect resources that are at risk of exposure to prevent data leakage. Track every resource, providing at-a-glance visibility into their share settings. At-risk resources are classified as public (which means they are accessible to anyone) or external (which means they are shared with users from an outside domain).



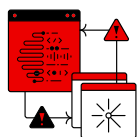
Identity's devices

Organizations need the ability to correlate risks stemming from user devices and the threat they pose to the SaaS ecosystem. This includes managing device vulnerabilities (CVE and CVSS), identifying unmanaged devices, and detecting out-of-date agents.



Identity threat detection and response (ITDR)

Organizations need to detect suspicious activities and indicators of compromise (IOCs) based on user access and behavior anomalies as well as changes in user permission settings. IOCs can include IP addresses, domain names, and URLs. By detecting unusual behavior, ITDR identifies threat actors as they navigate through applications.



GenAI security posture management

SaaS apps are increasingly adding GenAI functionality, enabling applications to write reports, proposals, campaigns, and other materials using data within the SaaS applications. Though these capabilities improve productivity, they also open the door to potential data leaks, as GenAI may share sensitive information with external parties.

What are some examples of industry breaches that have impacted SaaS applications?

Here are some examples of recent SaaS breaches:

Payday problem

A threat actor infiltrated an organization's HR information system tenant and changed direct deposit banking details for some employees to steal their salaries.

Malicious repository

Employees were manipulated to download malicious repositories that stole their login credentials and cryptocurrency.

Overprivileged employees

An employee was granted access to information for over 63,000 employees, including names, Social Security numbers, and compensation information.

Examples of Threats Detected by Falcon Shield

Payment Received

When a threat actor changed an invoice's account payment information to redirect the funds to their own account, CrowdStrike Falcon® Shield detected the change and ensured that the payment went to the correct account.

Two Places at Once

IP geographical data indicated a user accessed their customer relationship management (CRM) tool from Baltimore at the same time that they were logged in to their email account from Paris. Falcon Shield detected the anomaly and recognized that the Paris login was using an unusual OS. The company blocked the Paris login and reset the user's login credentials for all apps.

Wrong VPN Accesses App

A user who always logged in to their applications through the company's standard VPN was detected logging in through a private VPN, which is commonly used to hide identities. Though this alone wasn't enough to indicate a threat, the suspicious login took place at a time when it was unusual for the user to be logged in.

Security Options

SaaS applications are secure by design, but weak and misconfigured controls can quickly lead to breaches. SaaS applications follow the shared responsibility model, where the application vendor is responsible for application security, network controls, and the physical host while the buyer is responsible for information and data, user security, and access controls.

Can SaaS applications be secured with existing tools?

Most existing security products weren't designed to monitor applications with hundreds of settings, thousands of users, and terabytes of data stored in disparate applications located on different servers.

What security tools are effective in securing the SaaS stack?

SaaS security posture management (SSPM) solutions are the only security products designed to meet the demanding and diverse security needs of SaaS apps. SSPMs secure all key SaaS attack vectors, as they monitor configurations, manage users, monitor devices, discover third-party applications, catalog shared files, and engage in threat detection.



**What should
you look for in a
SSPM solution?**

Download The Ultimate
SaaS Security Checklist:
Future-Proof Your
SaaS Security

[Download Checklist](#)

Why Aren't CASBs Enough?

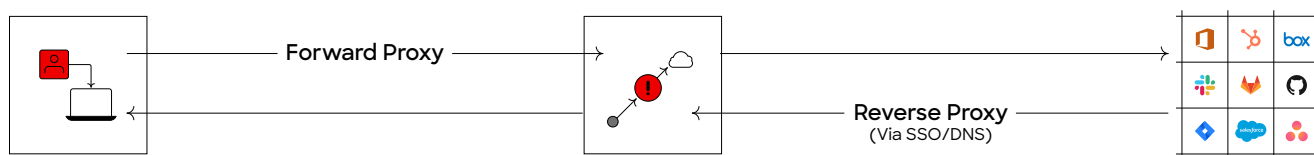
Cloud access security brokers (CASBs) are unable to secure SaaS applications for a number of reasons:

- 1 Configuration monitoring requires extensive customization**
CASBs can't cover the different configurations and security settings in each SaaS application.
- 2 Security policy application**
CASBs normalize policies across an organization's cloud network. However, this approach is inadequate when dealing with diverse SaaS applications that require SaaS-specific rules.
- 3 Lack of adaptability**
CASBs lack flexibility in addressing evolving SaaS characteristics and threats.
- 4 Security blindness**
CASBs focus on pathways and look at the app "from the outside," causing them to miss user behavior nuances.
- 5 Integration complexity**
CASBs require a proxy, slow down access, and add considerable cost and effort for each application that they integrate with.

CASB

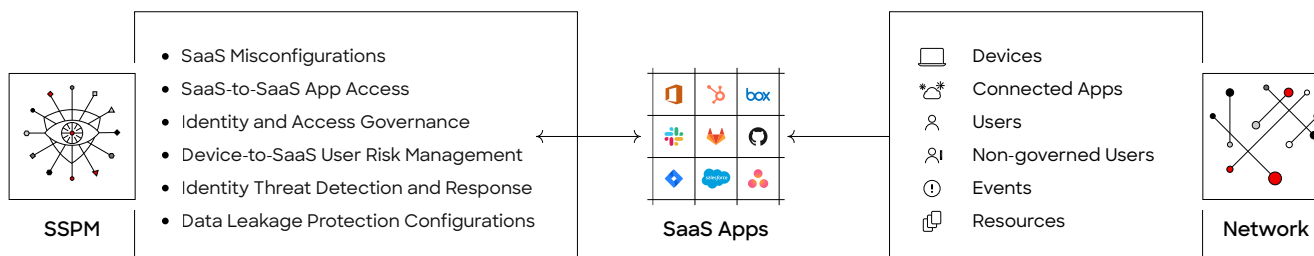
In-line data between SaaS to organization, including users, data access, and authentication

*API only for DLP and event



SSPM

Access all configurations and data at the source from within the SaaS application

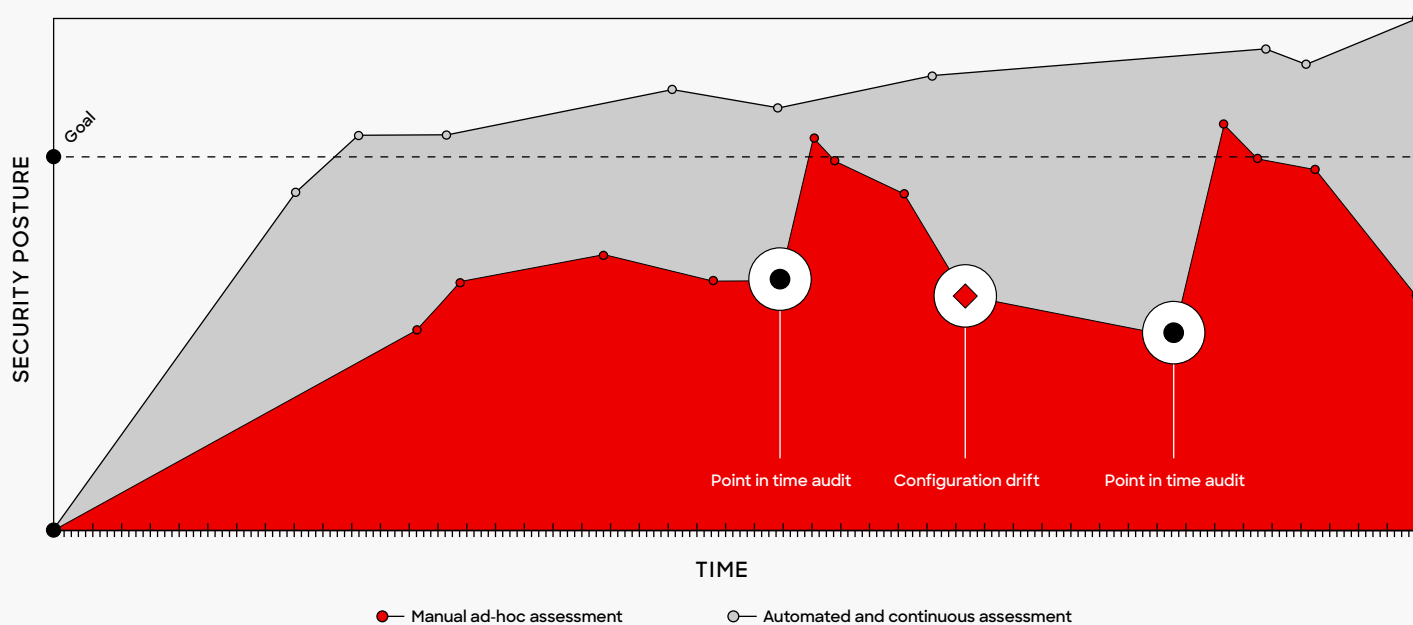


Why aren't manual audits enough?

Manual audits leave companies vulnerable to misconfigurations and other issues. They provide a snapshot view of an application's security settings, but they are unable to ensure that those settings remain unchanged between audits.

To be effective, the auditor must be familiar with the application and its settings. Considering that applications use different terminology and the ramifications of their settings vary, a true manual check demands an experienced security professional taking their time going through every setting and user permission within an application.

As a result, these checks are time-consuming and expensive. They also rely on human beings looking at hundreds of toggle switches and checkboxes, leaving plenty of room for human error.



Fully Securing the SaaS Stack

What tools are needed to secure the SaaS stack?

Organizations need SSPM for prevention purposes and ITDR for threat detection and response.

How does SSPM provide SaaS security?

SSPM is the prevention catalyst in SaaS security. It integrates directly with each application to provide visibility into application configurations, user risks, device risks, connected applications, and shared files. When an SSPM identifies a risk, it triggers an alert process designed to secure the application immediately.

Where does threat detection fit in SaaS security?

Current ITDR solutions primarily address endpoint and on-premises Active Directory protection, but they don't cover the intricate SaaS environment. Addressing SaaS-related threats demands deep expertise that can only be achieved by cross-referencing and analyzing suspicious events in context from multiple sources.

SaaS ITDR solutions use SaaS logs to monitor events and detect threats emanating from external threat actors and authorized users. They look for IOCs based on login data, user/non-human behavior, and device data and alert security teams when IOCs indicate a threat.

Falcon Shield integrates with over 150 applications out of the box, enabling customers to connect their entire stack and receive accurate IOC alerts, drastically reducing false positives.

How are other organizations securing their SaaS applications?

The Annual SaaS Security Survey Report: 2025 CISO Plans and Priorities found that 70% of organizations had a dedicated SaaS security team or role.

This Cloud Security Alliance (CSA) survey was commissioned by Adaptive Shield (acquired by CrowdStrike in 2024) and surveyed over 450 IT and security professionals from large organizations from various industries and locations to better understand the industry's priorities and plans around SaaS security.

The Annual SaaS Security Survey Report

2025 CISO Plans and Priorities

Download Report



39%

increased their SaaS security budget

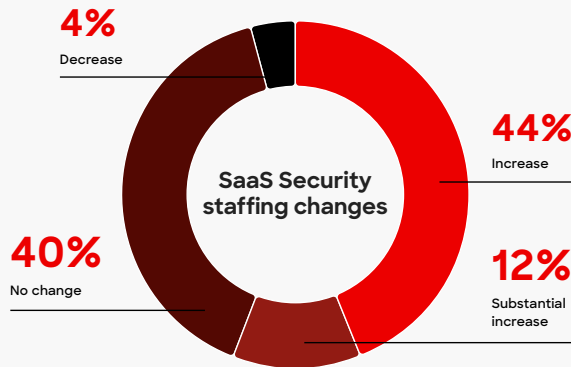


56%

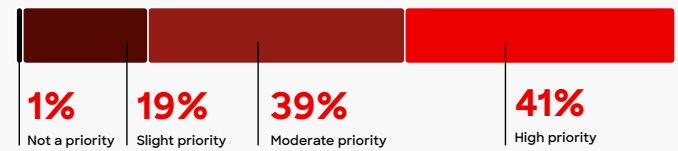
increased their SaaS security staff

70% of organizations have established dedicated SaaS security teams

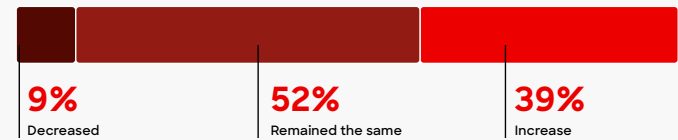
SaaS security is more important than ever to organizations. According to [The Annual SaaS Security Survey Report](#), 39% of organizations increased their SaaS security budget and 56% increased their SaaS security staff. Despite economic uncertainty and layoffs, dedicated SaaS security teams are addressing this area for the first time.



Priority level of SaaS security in organizations



SaaS Security budget changes



What does a successful SaaS security implementation plan look like?

SaaS security is a strategy. It requires prioritization and collaboration between app owners and security teams. Once key stakeholders have committed to the process, the SaaS security task force should map applications to help prioritize which apps to secure first.

The team should develop a responsibilities table, also known as a RACI chart, and devise short- and long-term plans to improve SaaS security posture. The plans should include goals and key performance indicators (KPIs) to measure progress.

Begin by securing high-risk, low-touch items first for quick wins. Once configurations are secure, move on to review users, third-party applications, and devices that access the application. Measure progress periodically and continually add more applications to your SSPM.



Kick-Starting a Robust SaaS Security Program

[Download Guide](#)

SSPM and Compliance

Does SSPM enable organizations to meet best practices, regulatory requirements, and compliance standards?

SSPMs align SaaS application security settings with standards, allowing organizations to see whether their apps meet regulatory compliance requirements. Every security check is mapped to relevant compliance standards — such as SOC2, HIPAA, and ISO 27001 — providing a clear path toward compliance.

Bottom Line

Is SSPM a must-have for today's enterprises?

Yes. According to Gartner, SSPM is a must have. In [2021](#), Gartner included SSPM as one of four must-have technologies. Gartner's 2024 [Technology Adoption Roadmap](#) for Security and Risk Management also included SSPM as a High Enterprise Value Platform with a Low Deployment Risk.

It's easy to see why. Today's enterprise landscape relies heavily on SaaS applications and demands a robust and comprehensive security solution. SSPMs are the only solutions on the market that can ensure continuous operations and protect critical data. Relying on any other solution compromises operational integrity and data security.

About Falcon Shield

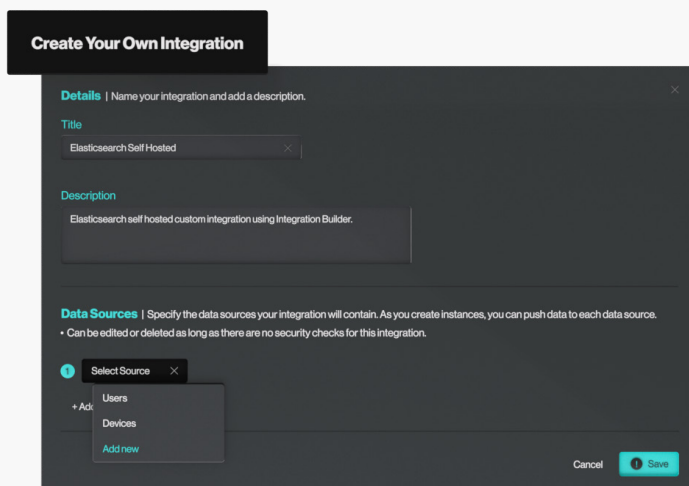
Falcon Shield's SSPM and ITDR solution enables security teams to stay on top of their organizations' apps and identities as well as any unusual behavior in the SaaS ecosystem.

With 150+ supported applications out-of-the-box and the ability to monitor custom applications, Falcon Shield offers full coverage of the SaaS ecosystem.



Integration builder: Secure every app in the stack

Secure custom apps, niche apps, and any SaaS application that isn't integrated out-of-the-box with the integration builder. Manage configurations, monitor users, and gain visibility into devices that access your SaaS stack.



Why should I buy an SSPM solution instead of building one from scratch?

SaaS security expertise

SaaS security is highly specialized, as each SaaS application's security configurations are unique. Terminology and the implications of a misconfiguration will vary between applications. As a result, an effective in-house application requires a deep understanding of SaaS security, the applications being monitored, and compliance issues.

Rapid changes in the market

New security threats and app updates are always on the horizon. Maintaining an in-house application so that it stays ahead of the latest changes and threats requires a dedicated team committed to staying on top of every application and evolving threat.

Time to market

Falcon Shield can begin monitoring and securing SaaS applications within minutes. An in-house solution may take months to build, leaving SaaS applications exposed while it is built.

What industry recognition has Adaptive Shield (now Falcon Shield) received?

Prior to the CrowdStrike acquisition, the industry recognized Adaptive Shield (now Falcon Shield) for its leading SaaS security innovations and easy-to-use platform. These awards include:



Best Cloud Security
Management Solution
Finalist



Gartner® 2022
Cool Vendor



2024 Global Infosec
Awards Winner



2024 Fastest Growing
Cybersecurity Company



Globe Awards



Top Ten Baby Black
Unicorns



2023 Best Practices
Award from Frost &
Sullivan



Top Infosec Innovator
Awards



2024 Cybersecurity
Excellence Awards



Proud Community Member



Proud Community Member



Star Level One Certified

Why should you use Falcon Shield to secure your SaaS stack?

Falcon Shield is the only SaaS security platform to integrate with an industry-leading 150+ SaaS applications out-of-the-box, and its integration builder allows users to add and monitor any additional SaaS app or home-grown app.

Falcon Shield is at the forefront of innovation, covering new use cases in SaaS security and committed to cover any evolving threat. The solution was designed to meet the ever-expanding needs of SaaS security, providing the communication infrastructure to support the democratization of SaaS security.

Learn more at <https://www.crowdstrike.com/platform/falcon-shield>

Who are Falcon Shield's customers, and how do we help them?

Falcon Shield provides SaaS security to hundreds of enterprise customers, including Fortune 100 companies, consumer brands, retailers, sports leagues, financial institutions, security companies, technology companies, and more.

Customer success and account management teams ensure that Adaptive Shield users get the most out of the solution. From onboarding applications, product training, and KPI monitoring to sending guidance following major breaches, Falcon Shield acts as a full partner in ensuring that your SaaS stack is positioned to handle any threat.





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>

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

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