

SAAS SECURITY POSTURE MANAGEMENT (SSPM).



Every SaaS app is its own security perimeter with its own settings — **SSPM continuously checks that perimeter against a baseline, instead of trusting that whoever configured it got it right once.**

- MISCONFIGURATION DRIFT
- OAuth APP RISK
- SHADOW SAAS DISCOVERY
- CONTINUOUS BASELINE CHECKS

01 THE MECHANISM



Configuration Baseline Scanning

SSPM connects to each SaaS app's admin API and continuously checks settings — sharing permissions, MFA enforcement, session policies — **against a security baseline for that specific app.**



OAuth & Third-Party App Risk

Every app a user grants access to inherits scopes into the core SaaS environment; SSPM inventories these connected apps and **flags excessive or unused permissions.**



Drift Detection & Alerting

A setting correct at rollout can be silently changed by an admin, an update, or an integration — SSPM flags the moment configuration drifts from baseline, **not months later during an audit.**

02 THE FLOW

The Monitored Tenant

BASELINED

1

An admin changes a sharing or authentication setting in a SaaS app, intentionally or by mistake.

2

SSPM detects the change within its next scan cycle and compares it against the required baseline for that app.

3

The security team is alerted with the specific setting, the change, and the fix, **often before the misconfiguration is ever exploited.**

The Unmonitored Tenant

DRIFTED

1

An admin changes a sharing or authentication setting in a SaaS app, intentionally or by mistake.

2

No one is watching that specific setting, so the change persists silently across hundreds of similar settings in dozens of connected apps.

3

The misconfiguration is discovered only after **a document is publicly shared** or an incident forces a manual review.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Per-App Configuration Baselines	Defines the correct security settings for each SaaS app individually, since a baseline for email differs from one for a CRM or file-sharing platform.
OAuth & Connected-App Governance	Inventories every third-party integration granted access to core SaaS platforms, and flags excessive or unused scopes.
User & Permission Hygiene	Surfaces dormant accounts, excessive admin roles, and external sharing that accumulate quietly over time.
Continuous Drift Detection	Rechecks every setting on an ongoing cycle instead of relying on a point-in-time audit or manual review.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Point-in-Time Security Review	No	Captures a snapshot that's already stale by the time the next configuration change happens.
CASB Without App-Specific Baselines	No	Controls data movement in and out of SaaS apps but doesn't validate whether the app's own settings are configured correctly.
Manual Admin Console Spot-Checks	No	Doesn't scale past a handful of apps and misses settings buried outside the primary admin screen.
IAM / SSO Coverage Alone	No	Confirms who can log in, not whether the application they land in is itself securely configured.
Continuous SSPM Scanning + OAuth Governance + Drift Alerting	Yes	Catches misconfiguration and risky integrations as they happen, across every connected app.

SAAS SECURITY POSTURE MANAGEMENT. DISCOVER · CONFIGURE · MONITOR

05 PROGRAM OPERATIONS

Every SaaS app is a separate security perimeter with its own settings. There is no single control plane that secures a CRM, a chat tool, and an HR platform the same way.

Shadow SaaS expands the perimeter faster than IT can track it. Employees connect new apps and OAuth integrations continuously, often without any security review.

A correct configuration today is not a correct configuration next quarter. Vendor updates and admin changes silently shift settings out of compliance.

OAuth scope creep is invisible without dedicated monitoring. A connected app that requested read access at install can be granted broader access later without a fresh review.

06 CONTROL MAPPING

CSA SAAS GOVERNANCE

Best practices for assessing and continuously governing security posture across third-party SaaS applications.

NIST SP 800-53 (CM FAMILY)

Configuration management controls requiring baseline configurations and monitoring for unauthorized change.

SOC 2 (COMMON CRITERIA)

Requires evidence of ongoing monitoring and change management for systems handling customer data, including SaaS platforms.

CIS CRITICAL SECURITY CONTROLS

Inventory and configuration management controls that extend directly to SaaS and cloud application settings.

07 WHAT THIS DOES NOT SOLVE

Vulnerabilities in the Vendor's Own Code

SSPM governs how an app is configured, **not the security of the vendor's underlying platform or infrastructure.**

Data Classification & Content Risk

Flags an overly permissive sharing setting but **doesn't know whether the shared file itself contains sensitive data.**

Insider Misuse of Legitimate Access

A user with correctly configured, authorized access **can still misuse it within policy.**

Non-SaaS Attack Surface

Endpoints, on-premises systems, and infrastructure outside SaaS applications **fall entirely outside SSPM's scope.**

08 MYTHS VS. REALITY

MYTH	REALITY
"If SSO is enforced, the SaaS app is secure."	SSO controls authentication into the app; hundreds of other settings — sharing, API access, session length — remain independently configurable and unmonitored.
MYTH	REALITY
"CASB and SSPM cover the same ground."	CASB focuses on data movement and access control at the network edge; SSPM validates the configuration inside the application itself.
MYTH	REALITY
"IT approved the app, so it's covered."	Approval at onboarding says nothing about whether the app's settings remain correctly configured six months later.
MYTH	REALITY
"Only large, well-known apps need posture management."	Smaller or niche SaaS tools often ship weaker default security settings and get far less scrutiny.
MYTH	REALITY
"OAuth permissions are a one-time approval."	Connected apps can be re-authorized with expanded scopes without triggering a new security review.

09 SPEAK THE PROGRAM — KEY TERMS

SECURITY POSTURE BASELINE

The defined set of **correct, secure configuration settings** for a specific SaaS application.

CONFIGURATION DRIFT

Any deviation of a live setting from its established security baseline, **whether intentional or accidental.**

OAuth SCOPE

The specific set of **permissions a connected third-party app is granted** within a core SaaS platform.

SHADOW SAAS

Applications connected to organizational data or identity **without formal security review or IT approval.**

SHARED SIGNALS FRAMEWORK (SSF)

An emerging cross-vendor standard for SaaS platforms to **share real-time security event signals** with each other and monitoring tools.

TENANT

An organization's isolated instance of a SaaS application, **containing its own users, data, and configuration settings.**