valence

Find and Fix SaaS Security Risks

Minimize your SaaS attack surface with advanced visibility and remediation to address configuration, identity, integration and data risks.

More SaaS -> More Risk

SaaS applications have become deeply embedded in every business function within organizations. They facilitate business productivity and efficiency through collaboration, automation and innovation. Business admins and users feel empowered to manage them at scale, without involving IT. Therefore, SaaS vendors aim to make SaaS adoption as easy and seamless as possible, but as a result they create complex platforms that are difficult to securely configure. This leads to an increase in misconfigurations that introduce new SaaS security risks that legacy solutions such as CASB do not cover since they focus on user-to-SaaS access rather than SaaS configurations.

High profile breaches have shown that attackers are targeting SaaS applications and are leveraging misconfigurations and human errors to gain high privilege access to sensitive applications and data. First lines of defense like MFA and SSO are proving insufficient. You only have to look so far as the recent breaches and compromises (MGM, Caesars and Okta) to see the impact on security vendors such as BeyondTrust, Cloudflare, and 1Password. Attackers have identified that MFA fatigue, social engineering and targeting the SaaS providers themselves, can bypass many of the existing mechanisms that security teams have put in place. These add to high profile breaches where attackers leveraged legitimate third-party OAuth tokens to gain unauthorized access to SaaS applications such as GitHub, and many more attack examples.

Why SaaS Security Is A Top Priority

Enterprise environments are experiencing increased SaaS risks due to complex configurations and decentralized business unit adoption.

- 1 in 8 SaaS accounts are dormant
- 21 third parties have tenant-wide access
- 90% external shares are inactive
- 100% of orgs have MFA exceptions

Securing SaaS Applications with Valence

SaaS Configuration Management

Continuously analyze SaaS security configurations to detect risky misconfigurations and drifts

- Gain insights into how to harden default security configurations.
- Maintain compliance with industry frameworks such as CIS, ISO 27001 and NIST.
- Detect configuration drift from defined baselines and best practices.

SaaS Identity Security

Reduce your identities and account risks from insecure access and over privileged access

- Ensure strong authentication is enforced with SSO and MFA.
- Monitor account lifecycle process to properly, offboard dormant accounts.
- Apply least privilege access by reducing overprivileged admin access.

SaaS Data Protection

Apply zero trust principles to secure your data from oversharing with external collaborators

- Protect a wide range of SaaS data - such as files, code repositories, and financial data.
- Remove external collaborators access that is no longer necessary for the business.
- Identify overly shared data with public access and open links.

SaaS Integration Governance

Manage access of SaaS-to-SaaS, third-party integrations, non-humans and service accounts

- Gain visibility into third-party vendors with API keys, OAuth tokens and third-party apps.
- Monitor privileges and activities to identify risky and overprivileged integrations.
- Collaborate with users for context to revoke inactive integrations.

The Valence Platform

Valence's SaaS Security Platform is implemented in minutes thanks to its agentless deployment and delivers value from day one. The platform can integrate into dozens of SaaS applications and provides in-depth visibility into SaaS risks with its SaaS security posture management (SSPM) functionalities. Valence provides security teams with flexible options to monitor and remediate risks with and without automated workflows. The workflows can optionally send custom security notices to business users via email or Slack, to collect additional context that enables the remediation efforts.

SaaS Risk Management

Gain holistic visibility into your SaaS security posture with actionable insight

Business User Collaboration

Collaborate with your business users to contextualize and remediate SaaS risks

SaaS Risk Remediation

Define security policies that can leverage automated workflows to remediate SaaS risks

> "The ability to automatically mitigate SaaS risks is a game changer for our security team. Instead of executing manual and labor-intensive workflows, Valence's self governance workflows automatically collect the required business context, educate business users about SaaS risks and encourage them to remediate risks on their own."
>
> Doug Graham
> Chief Trust Officer
>
> LIONBRIDGE

Secure the Apps That Run Your Business

Valence integrates with these business-critical SaaS applications and more, enabling security teams to quickly discover and remediate risks.

Microsoft 365 · Google Workspace · salesforce · GitHub · workday. · slack · ATLASSIAN · okta · servicenow · zoom · snowflake · NETSUITE · monday.com · DocuSign · workato · zendesk · PingIdentity.

Reduce SaaS Attack Surface

Minimize your SaaS attack surface by removing idle resources and enabling native SaaS security configurations

Increase Business Productivity

Instead of blocking SaaS usage, educate and enable users to leverage SaaS features with security guardrails

Minimize Security Overhead

Automated workflows and user engagement to minimize manual effort by security teams and SaaS admins

Gain Immediate Time-to-Value

Connect Valence's platform to SaaS applications in minutes to discover security risks and actionable insights

Request A SaaS Security Risk Assessment

Get a detailed assessment of your SaaS security posture with detailed recommendations for remediating risks for one of your core SaaS platforms like Microsoft 365, Google Workspace, or Salesforce.