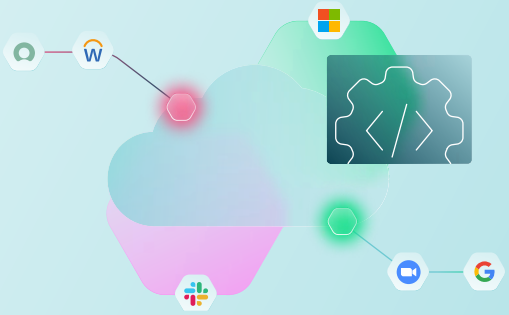
valence

Find and Fix SaaS Risks

Valence combines SaaS discovery, SSPM, ITDR, and remediation capabilities to enable security teams to reduce risks associated with SaaS configurations, identities, data, SaaS-to-SaaS, and GenAI



More SaaS » More Risk

The distributed adoption and management of SaaS has led to increased shadow IT challenges and misconfiguration risks, making SaaS applications a prime target for attackers. Many security teams struggle to identify and track the growing number of SaaS applications adopted by various business users—especially with the rise of GenAI tools, which are typically delivered as SaaS.

Adding to the complexity, platform admins are often embedded within business functions—Salesforce admins in sales, Workday admins in HR, GitHub admins in engineering—dramatically increasing the likelihood of misconfigurations due to misunderstandings of the shared responsibility model.

Recent attack campaigns targeting Snowflake, Microsoft 365, GitHub, Okta, and others underscore this trend. Attackers are increasingly focused on SaaS platforms because they often house sensitive data and powerful permissions.

To mitigate these risks, security teams must build strong partnerships with business users and SaaS admins to maintain control over applications, data, identities, and SaaS-to-SaaS integrations—while ensuring continuous monitoring to detect and respond to potential breaches.

Why SaaS Security Is A Top Priority

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

Identity Sprawl

100% of organizations have failed to completely roll out MFA

Configuration Management

SaaS complexity is a top challenge for 43% of organizations

Data Exposure

94% of external file shares are inactive, with no recent usage by the external users

SaaS-to-SaaS Integrations

For every 1 human identity, there are 8.6 non-humans identities

The Valence Platform

Security teams are empowered with complete visibility into their SaaS ecosystems—including sanctioned and unsanctioned applications—alongside prioritized SaaS risk management, threat detection, and advanced remediation capabilities.

SaaS Security Posture Management (SSPM)

Centrally manage risks across your SaaS applications to identify and prioritize misconfigurations, enforce security policies, and comply with industry standards

SaaS Identity Threat Detection and Response (ITDR)

Monitor activities of both human and non-human identities to detect suspicious behavior and proactively hunt threats, empowering you to respond to SaaS incidents effectively

SaaS Discovery

Leverage a comprehensive inventory of all SaaS applications, identify security gaps, and reduce risks related of shadow IT, unmanaged identities, and sensitive data exposure

SaaS Risk Remediation

Scale risk reduction with flexible options from manual to automated remediation, including collaboration features that engage users and admins to gain necessary business context

Discover and Secure Your SaaS Ecosystem

valence

SaaS Configuration Management

Continuously analyze SaaS security configurations to detect misconfigurations and drift from best practices

- Harden default configurations with insights to improve SaaS security posture
- Comply with industry frameworks such as CIS, ISO, HIPAA, and NIST
- Detect configuration drift from defined baselines and best practices

SaaS Identity Security

Discover all your SaaS identities and ensure they leverage strong authentication with least privilege

- Discover users leveraging shadow SaaS applications such as GenAI tools
- Ensure strong authentication is enforced with single sign-on (SSO) and multi-factor authentication (MFA)
- Continuously apply least privilege and verify timely offboarding of accounts

SaaS Data Protection

Secure your data with zero-trust access controls to prevent data exposure or leakage

- Identify all data shared with external access and open/public links
- Reduce overshared files, code repositories, sales data, financial information, and more
- Manage external data sharing and remove collaborator access that is no longer needed

SaaS-to-SaaS Governance

Manage access of third-party integrations, non-human identities, and service accounts

- Monitor privileges and activities to identify inactive, overprivileged, or risky integrations
- Gain centralized visibility and control over API keys and OAuth tokens
- Review and revoke unauthorized SaaS-to-SaaS integrations

"We had the visibility that we wanted in our existing tools, but it was hard to understand, hard to analyze, very time consuming, and very manual. What **took us weeks to analyze and uncover in the past,** with Valence we were able to **highlight and understand in minutes, if not seconds.**

Mandy Andress | CISO

elastic

"The ability to **automatically mitigate SaaS security risks** is a game changer for our security team. Instead of manual and labor intensive workflows, Valence **automatically collects the business context** and **encourages users to remediate risks on their own.**"

Doug Graham | Chief Trust Officer

LIONBRIDGE

"**Valence allowed us to see which platforms were exposing data** that we didn't necessarily know about, and enabled us to **quickly eliminate those file exposures.**"

Matt Walker | Managing Director, IT Security and Compliance (CISO)

goosehead INSURANCE

"The reason **we swapped from our previous tool** was that there appeared to be a lack of **innovation** and little to no **automation**. With Valence, the partnership was a big piece."

Michael Lyborg | CISO

SWIMLANE

Secure 150+ Apps That Power Your Business

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

And More!

Learn How We Strengthen Your SaaS Security
www.valencesecurity.com

Find Out More