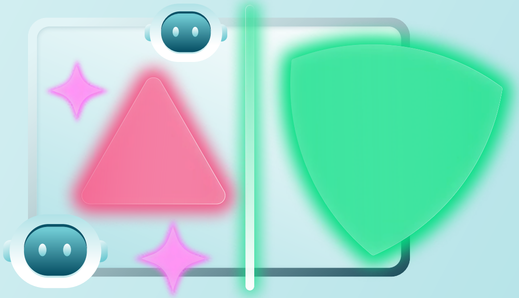
valence

Secure SaaS and AI in the Agentic Era

Valence protects organizations from SaaS and AI sprawl with unified discovery, SSPM, AI governance, AI agent security, ITDR, and flexible remediation options.



More SaaS and AI » More Risk

The distributed adoption and management of SaaS has led to increased shadow IT challenges, misconfiguration risks, and unmanaged AI usage, making SaaS and AI applications a prime target for attackers. Many security teams struggle to identify and track the growing number of SaaS apps, AI tools, and autonomous AI agents adopted by business users, especially as AI functionality is rapidly introduced through SaaS-delivered services.

Adding to the complexity, business teams now manage these applications, with Salesforce admins in sales, Workday admins in HR, and GitHub admins in engineering. This dramatically increases the likelihood of misconfigurations and AI-related oversights due to misunderstandings of the shared responsibility model.

Recent attack campaigns targeting Salesforce, Snowflake, Microsoft 365, GitHub, Okta, and others underscore this trend. Attackers increasingly focus on SaaS and AI platforms because they house sensitive data, powerful permissions, and high-value non-human identities, including AI agents.

To mitigate these risks, security teams must build strong partnerships with business users and SaaS admins to maintain control over applications, data, identities, AI agents, and SaaS-to-SaaS connections, while continuously monitoring to detect and respond to misconfigurations, abuse, and potential breaches.

Why SaaS and AI Security are a Top Priority

SaaS Sprawl

55% of employees adopt SaaS without security's involvement

Configuration Management

SaaS complexity is a top challenge for 43% of organizations

AI Risks

56% are concerned about overprivileged AI tools

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

The most comprehensive platform to cover your entire SaaS security program and govern your AI adoption

SaaS and AI Discovery

Reduce shadow IT, SaaS, and AI risks with a comprehensive inventory of all your SaaS/AI applications and associated identities

Posture Management (SSPM)

Improve your SaaS security posture with a unified view of prioritized misconfigurations and compliance gaps

AI Security Posture Management (AI-SPM)

Secure AI adoption within your SaaS applications across shadow AI tools, AI agents, AI integrations, and built-in AI features

Risk Remediation

Reduce SaaS risks and scale policy enforcement with flexible options ranging from one-click remediation to automated workflows

Threat Detection (ITDR)

Monitor activities of both human and non-human identities to detect suspicious behavior and proactively hunt threats

Discover and Secure Your SaaS and AI Ecosystem

valence

Discover Shadow SaaS and AI

Uncover unsanctioned SaaS apps and AI tools across your environment with full visibility into every integration and identity

Comply with Industry Standards

Map SaaS and AI controls to frameworks like CIS, ISO, SOC 2, NIST, and NYDFS to streamline and maintain compliance

Strengthen Identity Security

Ensure strong authentication, least privilege access, and clean offboarding for employees and contractors

Reduce Data Exposure

Identify overshared files, public links, and personal-account access to eliminate unnecessary external data exposure

Manage SaaS and AI Configuration Risks

Continuously detect misconfigurations and drifts to maintain secure settings across all business-critical SaaS and AI applications

Secure AI Agents

Discover AI agents, their connections, and permissions to enforce least privilege access and reduce data exposure

Govern Non-Human Identities

Manage API keys, service accounts, and OAuth tokens to prevent excessive privileges and reduce integration-related risk

Detect and Respond to Threats

Monitor activity across human and non-human identities and quickly surface suspicious behavior for investigation and response

"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 175+ Apps That Power Your Business

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

And More!

Learn How We Strengthen Your SaaS and AI Security

www.valencesecurity.com

Find Out More