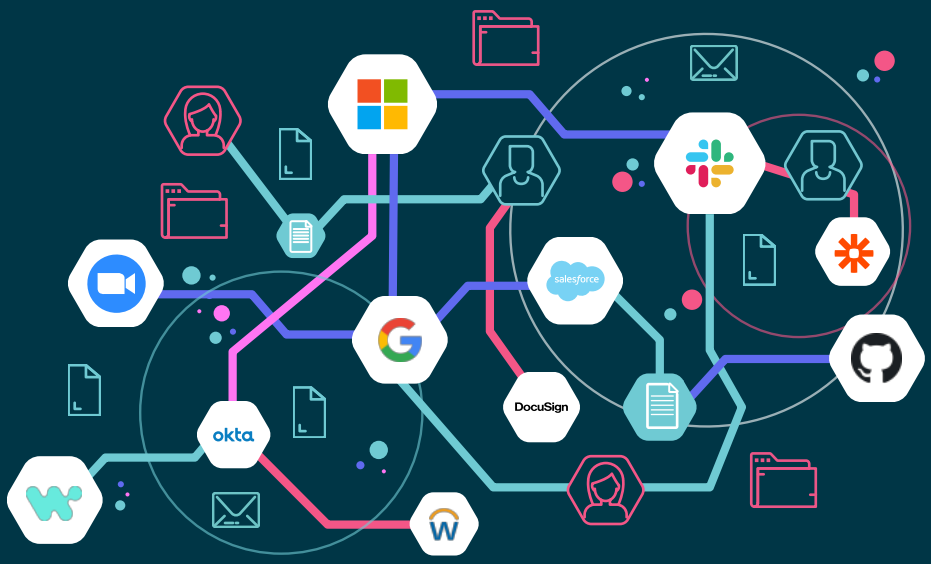


Collaboratively Remediate Your SaaS Security Risks

Eliminate your third-party integration, identity, and data sharing risk surface by automating workflows that engage with your business users across critical SaaS applications like Microsoft 365, Google Workspace, Salesforce and Slack.

The Risk of Democratizing IT

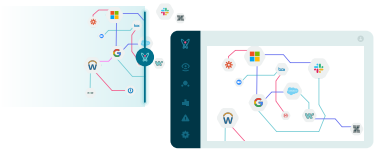
SaaS applications are designed to facilitate business productivity and efficiency, empowering end-users to adopt and interconnect them directly and at scale, according to the needs of the business. This democratization of IT has also resulted, unfortunately, in SaaS applications, integrations, users and data evolving into a sprawling SaaS mesh ungoverned and unmanaged by the organization's security team. The resulting security gaps have left organizations exposed to an accelerating number of SaaS supply chain attacks, data breaches, and account compromises.

Recent High-Profile SaaS Breaches

- Malicious OAuth apps taking over CEO accounts — January 28, 2022 — Microsoft
- 100s of companies impacted by breach — March 23, 2022 — okta
- Dozens of accounts breached — March 24, 2022 — HubSpot
- OAuth tokens abused to access customer tenants — April 22, 2022 — GitHub
- Gmail attack bypasses 2FA to read all email — August 4, 2022 — Google Workspace

The Valence Platform

Valence connects to your environment and tools to provide the visibility, context, and automation you need to scale security operations and reduce the security workload. It also prioritizes, executes and orchestrates risk remediation across your entire SaaS mesh, educating and engaging with your distributed business users to get the work done quickly, effectively, and continuously.



Discover and Gain Unified Control Across Your SaaS Mesh

Valence's unified cross-SaaS data and permissions model reduces the need for in-house security expertise for each SaaS application, allowing security teams to easily enforce consistent security guardrails.

Engage, Educate & Empower Your SaaS Business Users

Scale remediation workflows by engaging business users, educating them about their SaaS security risks, and empowering your security team as business enablement champions.

Automate SaaS Security Policy Enforcement

Valence's out-of the box SaaS security remediation workflows reduce the manual effort required to remediate SaaS risks associated with supply chain, identity, and data sharing.

Valence Example Use Cases

SaaS Mesh Discovery

Ensure continuous discovery and contextualization of your third-party SaaS applications

- Automated integrated SaaS discovery
- Vendor risk (TPRM) contextualization
- Third-party integrations threat intel

Data Protection

Secure your data from oversharing risky configurations that leave it exposed to external threats

- Files shared with external collaborators
- Publically open source code repositories
- Enabled email forwarding roles

Supply Chain Governance

Reduce the risks of supply chain attacks through removal of risky and suspicious integrations

- Inactive dormant API/OAuth tokens
- Over privileged third-party integrations
- Noncompliant no/low-code workflows

Identity Security

Detect identity and permission drift to ensure strong authentication and least privilege access

- Lack of MFA
- Failed offboarded users
- IdP unmanaged users

"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