Case Study

Why Lionbridge Chose Valence to Remediate their SaaS Security Risks

Industry

Translation, localization and AI training data

Company Profile

- Founded in 1996
- 6,000+ Employees
- 2,500+ Customers
- Primary Microsoft 365 environment with incidental use of additional architecture

LIONBRIDGE

Challenges

- Independently adopted SaaS solutions present across globally distributed business units
- Existing third-party integrations with high privilege access to core SaaS applications
- Limited governance of email forwarding rules
- Business requirement for greater visibility into inactive user accounts

Solution

Valence SaaS Security Platform

Key Results

- Detected and catalogued more than 1,000 SaaS-to-SaaS integrations
- Approximately 95% of inactive or obsolete integrations were deprecated via token revocation
- Classified high-risk and privileged-access integrations for immediate action
- Achieved 100% visibility and governance of unmanaged email forwarding rules
- Identified approximately 10% of user accounts as dormant, resulting in increased resource availability and cost savings through account deletion or archival

Valence Benefits

- Reduces time and effort requirements by replacing manual efforts with ongoing automated SaaS security remediation workflows
- Increases business-user opportunities for engagement and education on SaaS security best practices through identification and justification activities on a per-integration basis
- Places security boundaries around email forwarding rules.

Founded in 1996, Lionbridge Technologies, LLC is the leading provider of localization and translation services, supporting over 350 languages for 2,500+ customers worldwide. As a fast-growing company with offices in 23 countries and operations worldwide, Lionbridge serves companies who depend on breaking barriers and building bridges for their customers.

Automated SaaS Risk Discovery & Remediation

Lionbridge empowers its employees to independently adopt the most effective SaaS applications for their jobs, enabling the organization to respond to market needs efficiently. However, an independent adoption approach has led to decreased visibility into the cloud services, SaaS-to-SaaS integrations, user identities, privileges, and data sharing permissions in place leaving the security team at a disadvantage. Manual oversight over hundreds of integrations and settings also proved to be unsustainable long term for a team committed to a lean structure with multiple high-priority projects. Finding a solution that met Lionbridge's needs while preserving time and resources was high on the security team's wish list.

Lionbridge's SaaS Environment

Lionbridge presented several use cases to Valence because they connect with customers through diverse methods, sometimes leveraging proprietary platforms developed internally, third party SaaS platforms, and even utilizing customer-managed solutions. Flexibility in how Lionbridge connects with their customers facilitates efficient exchange of data, content, and ideas. While their primary productivity suite is Microsoft 365, Lionbridge also operates a sizeable footprint of alternative architecture such as Google Workspace and uses business apps for daily operations, such as a Customer Relationship Management platform. Plainly stated, their SaaS mesh is expansive and complex.

The Aha! Moment

Valence offered Lionbridge automated SaaS discovery and remediation, giving the security team unified visibility and control over risk across SaaS services while empowering business users by including them in remediation workflows.

When Lionbridge conducted a Proof of Concept trial with Valence they were surprised by the volume of SaaS applications present, including over 1,000 SaaS-to-SaaS integrations. All of their SaaS apps fell into two categories: those which were configured and deployed through official methods and which were known to the security team, and the rest which were independently adopted and integrated by business users.

> The ability to automatically mitigate SaaS security 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**

The Results

Setting policies was simple and efficient. Lionbridge was able to revoke 95% of obsolete or inactive tokens almost immediately. More than 20% were revoked by business users themselves with guidance natively available through Valence's remediation workflows. Business users provided justification for 5% of the tokens and 75% were revoked automatically by Lionbridge through Valence after the security team deemed them obsolete.

Lionbridge was able to revoke approximately

95%

of inactive tokens without any manual effort.

Today, Lionbridge oversees fully automated remediation workflows, replacing previously manual processes and time-consuming analysis with efficient oversight. Now configured, Valence can run without human interference. Nevertheless, Lionbridge retains the ability to log into the Valence platform to gather metrics for reporting purposes. By engaging with business users, the tool also increases education and awareness across the organization about good SaaS security hygiene.

As Lionbridge received regular updates, upgrades, and new features, they have expanded their remediation workflows to detect and eliminate external data oversharing, over-privileged and inactive user accounts, and unrestricted email forwarding rules. With Valence's reporting mechanisms, the security team can now demonstrate the efficacy of SaaS integration management while reducing their corporate attack surface.

About Valence Security

Valence Security offers collaborative remediation workflows that engage with business users to contextualize and reduce SaaS data sharing, supply chain, identity, and misconfiguration risks.