valence threatLabs

Shadow SaaS-to-SaaS Integration Report

Understanding SaaS Supply Chain Risks
Perception vs Reality

valencesecurity.com

Table of Contents

About This Report

This report covers key trends and challenges organizations face when trying to gain visibility and control over the growing and fast-changing world of SaaS-to-SaaS third-party integrations – **known as the SaaS mesh**. This mesh grows via API tokens, OAuth third-party apps, SaaS marketplaces, and no/low-code automated workflows that place sanctioned business-critical SaaS applications at risk of supply chain attacks.

Statistics in this report include both results from a survey of top CISOs, collected anonymously by Valence Threat Labs researchers in conjunction with YL Ventures Venture Advisory Board, and cross tenant metadata extracted from the Valence SaaS Mesh Security Platform that has been aggregated and anonymized to ensure customer privacy.

okta

Several supply chain breaches occurred in just the first few months of 2022 including the GitHub, Okta (LAPSUS$), and Mailchimp breaches.

While security teams are still reeling from the quick succession of attacks, these are only the latest incidents that have been accelerating the awareness that SaaS security, and SaaS supply chain security in particular, is a growing concern among CISOs.

Executive Summary

917
SaaS integrations are used in an average organization–
4-5X more than CISOs estimate

Impact:
Lack of Visibility Into Integrations

48%
of SaaS integrations sit unused – typically due to not being properly offboarded after a failed PoC

Impact:
Growing Integration Attack Surface

53%
of CISOs don't have a process to ensure proper correlation between TPRM and their integrations

Impact:
Over Privileged SaaS-to-SaaS Integrations

85%
of CISOs are unhappy with their current SaaS mesh visibility and risk reduction solutions

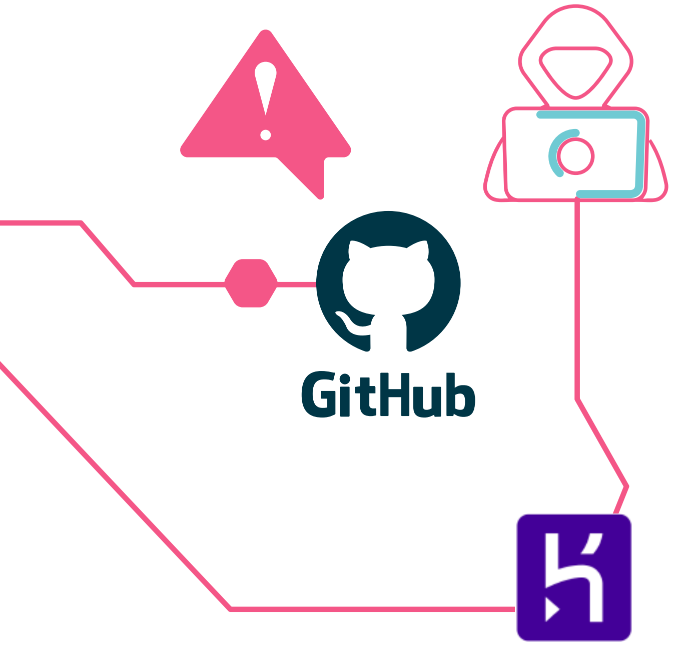
Impact:
Inadequate SaaS Mesh Security Solutions

SaaS Mesh Risks

The democratization of IT has empowered business users across organizations to manage best of breed SaaS applications directly, without IT security review or governance. This has greatly reduced deployment time and enhanced business agility, productivity, and collaboration. However, the indiscriminate connection of SaaS applications also increases the risk of unvetted supply chain access to business-critical applications like Salesforce, Microsoft 365, and Google Workspace.

These high-risk connections are typically driven by end users that are encouraged to consent to OAuth apps by SaaS vendors without understanding the security implications of their actions and how to revoke the access they granted. In addition, business owners often generate over-privileged API tokens that significantly increase the blast radius of any supply chain vendor breach. Lastly, citizen developers automate workflows by creating complex data flows that are hidden from security teams who lack visibility into no/low-code platforms.

> "Some core SaaS applications are administered by business units, therefore [we have] limited ability to apply controls for establishing/approving new connections."
>
> -CISO Survey Respondent



During the GitHub attack campaign in April 2022, attackers were able to steal and abuse OAuth tokens issued to well known vendors like Travis CI and Heroku. According to GitHub, the attackers were able to leverage the trust and high access granted to highly-reputed vendors to steal data from dozens of GitHub customers and private repositories.

The following survey questions and actual usage data provide insights into risks from SaaS-to-SaaS third-party integrations and current efforts to mitigate them.

Survey Methodology

The survey queried decision-makers with job titles relevant to cybersecurity such as CISOs, CIOs, and Directors/VPs of IT security distributed across organizations ranging in size from under 1000 employees to more than 20,000 employees. Respondents were recruited via email invitations containing an embedded link to the online survey. The email invitations were sent to a select group of YL Venture's qualified database.

Valence Security was responsible for all survey design, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

Survey Terminology

Core SaaS application

Any business critical SaaS application (i.e. Microsoft 365 or Salesforce) that is typically deployed and managed by the IT team.

SaaS-to-SaaS connection

Any connection between two SaaS applications created via API, no/low-code workflow, etc. (i.e Salesforce connected to Hubspot via API)

Third-party integration

Any connection to a core SaaS application created by a third-party vendor (i.e. Calendly or Grammarly). These integrations may be configured (using OAuth) by an employee or business department without IT oversight or security review.

No/low-code platform

Platforms like Workato, Zapier, Mulesoft, and Microsoft Power Platform that connect to core SaaS applications and allow citizen developers to easily build logic and applications without dependence on software development teams.

Lack of Visibility Into the SaaS Mesh

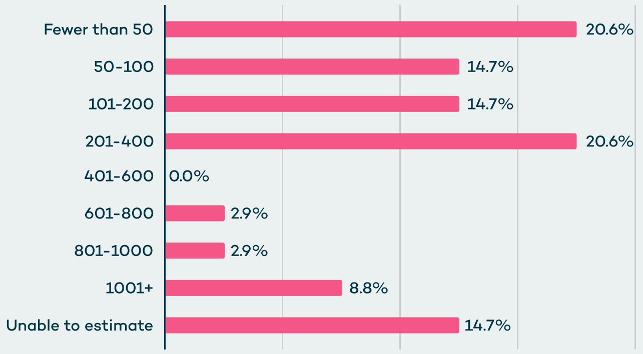
Existing security solutions such as managed devices, endpoint security, IdP, CASB, and ZTNA focus on human-to-SaaS security, leaving non-human SaaS-to-SaaS access ungoverned and unsecured. Lack of appropriate tooling means that already-overburdened security teams need to spend time and resources that they don't have to manually discover and manage the risk of SaaS-to-SaaS third-party integrations on a continuous basis. This is why the majority of CISOs are not satisfied with the current processes they have in place and underestimate the number of these integrations in their organizations.

What the Survey Says...

Question

If you had to estimate, how many SaaS-to-SaaS connections and third-party integrations are connected to your core SaaS applications?

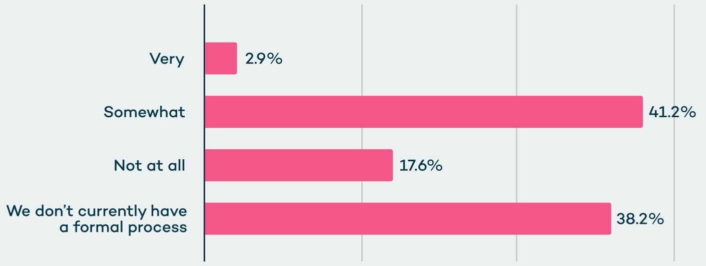
50% of CISOs responded that they have 200 or fewer SaaS-to-SaaS integrations or that they didn't know how many they have.



Question

How effective is your current process for discovering and managing your SaaS-to-SaaS connections and third–party integrations?

56% of CISOs either don't have a process in place, or are not satisfied with the process they have.



See What the Data Shows →

...What The Data Shows

The average organization has

917

SaaS-to-SaaS third-party integrations.

These integrations are

4-5x

the average CISO's estimation.

Missing Business Context of SaaS-to-SaaS Integrations

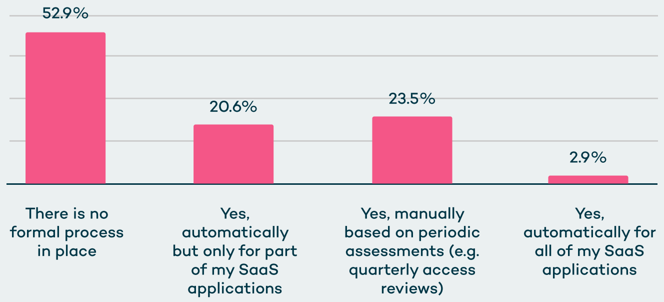
Business units can test and replace many different third-party vendors on an ongoing basis. Most decentralized SaaS admins rarely offboard integrations after a PoC or if they are terminated/abandoned over time. Unlike with human users, most organizations do not have a continuous process in place that allows them to assess the business justification of non-human identities and properly offboard unnecessary third-party vendors. These inactive, over-privileged integrations can facilitate the lateral movement of threats and increase both your SaaS attack surface and blast radius in the event of a third-party vendor breach, and should be revoked.

What the Survey Says...

Question

Do you currently have a continuous process to ensure correlation between the assumed level of access and the actual level of access of a third-party vendor?

53% of CISOs don't have a process in place for determining if an integration is over-privileged and may therefore need to be offboarded or right-sized.



See What the Data Shows →

...What The Data Shows

The average organization has

443

inactive SaaS-to-SaaS integrations, many of which are over-privileged.

Inactive integrations make up

48%

of the total number of overall integrations. Most of these inactive integrations are managed by admins outside of IT.

Continuous Onboarding of New Third-party Integrations

As SaaS-to-SaaS third-party integrations are rapidly adopted by employees and business units, it becomes a challenge for security and compliance teams to ensure proper coverage of their third-party risk management (TPRM) programs since they lack visibility and context into which vendors have access to their applications and the scope and exposure of such access.

This is problematic since SaaS admins typically provision integrations with excessive privileges due to the difficulty of manually configuring API scope access with least-privilege. Without a security review process in place, over-privileged integrations facilitate the lateral movement of threats, placing your data at elevated risk of cross-SaaS compromise once an attacker gains access to your supply chain.

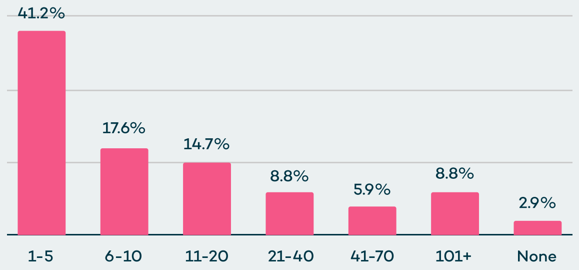
> "[With] our workforce changes (on and off boardings), contractors, and cloud environment changes it is difficult to keep up with SaaS connections."
>
> -CISO Survey Respondent

What the Survey Says...

Question

On average, how many new SaaS-to-SaaS connections and third-party integrations are connected on a monthly basis to your core SaaS applications?

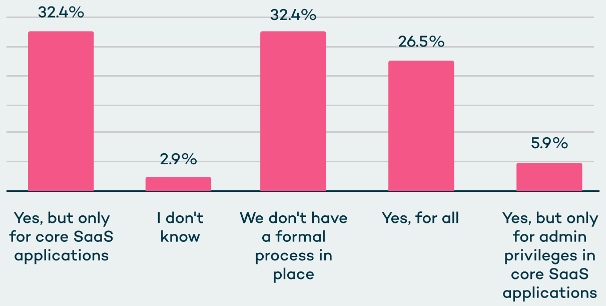
76% of CISOs believe they have under 20 new integrations added every month.



Question

Do you currently have a process to review and vet new vendors that receive access tokens to your SaaS applications?

65% of CISOs have a process in place, but only 27% have a process that applies to all vendors, including those adopted by employees and business units.



See What the Data Shows →

...What The Data Shows

On average, users onboard

76

third-party integrations every 30 days.

Newly onboarded integrations are

3-4x

the amount estimated by the average CISO.

Ungoverned Citizen Developers Automating With No/low-code

No/low-code workflow misconfigurations by citizen developers are relatively common, and can lead to exposed sensitive data and PII. Most organizations do not have the appropriate equivalent of AppSec and DevSecOps for such automation workflows in platforms like Workato, Zapier, Microsoft Power Platform, etc.

For CISOs who either believe their organizations don't use these workflows, don't know, or don't have processes in place to monitor them, they are leaving a significant part of their SaaS attack surface unmanaged and exposed.

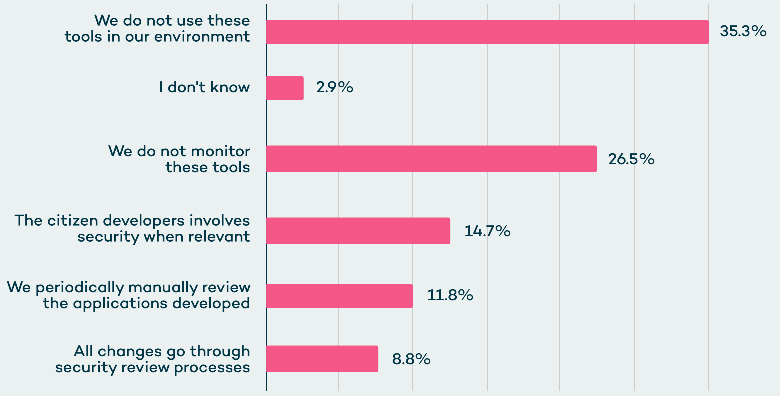
> "Misconfigurations regarding access to Microsoft's low-code platform led to the **exposure of 38 million records** of sensitive data, such as COVID-19 contact tracing, employee IDs and email addresses, belonging to 47 government agencies and companies."
>
> -TechRepublic, Aug. 24, 2021

What the Survey Says...

Question

How do you monitor applications developed by citizen developers on no/low-code platforms like Workato, Zapier, and Microsoft Power Platform?

35% of CISOs said that they do not use these tools in their environment.



See What the Data Shows →

...What The Data Shows

Over

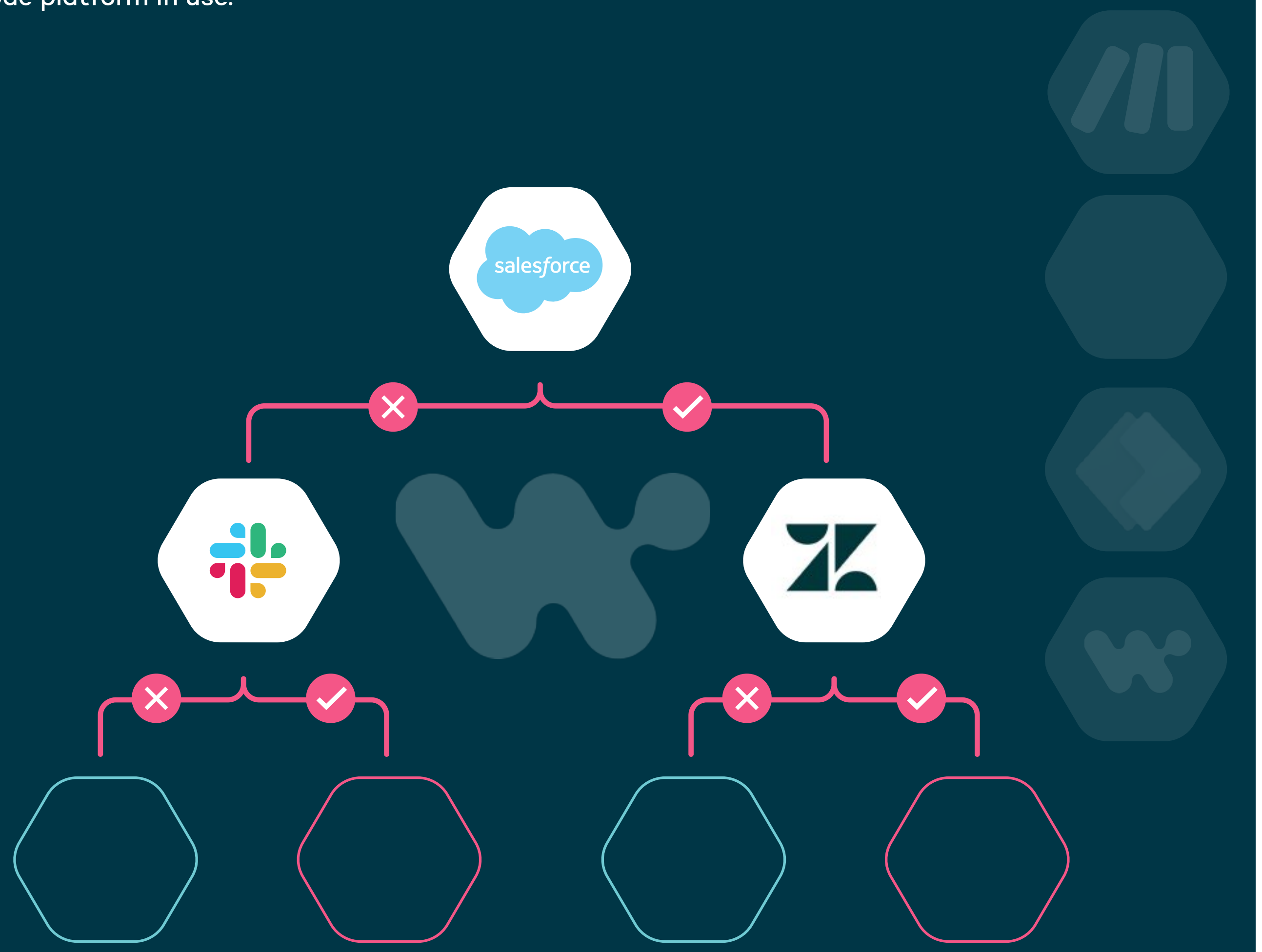
96%

of companies have at least one no/low-code platform in use.

On average they had

4-5

no/low-code platforms.



On the State of SaaS-to-SaaS Integration Security

Existing security solutions such as managed devices, endpoint security, IdP, CASB, and ZTNA focus on securing human-to-app connections. But in the new world of the SaaS mesh, they are inadequate, leaving non-human app-to-app access ungoverned and unsecured. Again, this increases the risk of supply chain attacks and the lateral movement of threats.

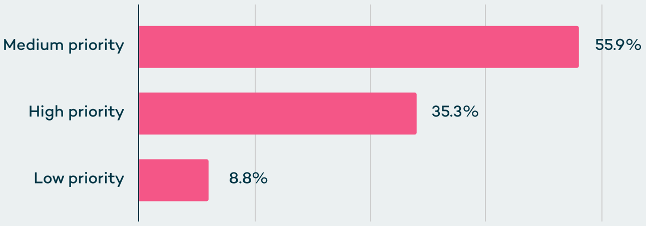
> "[What we need most is a] toolset to identify and classify risk of integrations. Bonus points for controlling them."
>
> -CISO Survey Respondent

What the Survey Says...

Question

How big of a priority is SaaS security in your organization in 2022/2023?

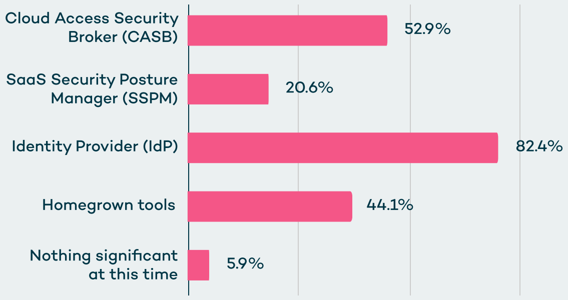
Only 9% of respondents in the survey said that SaaS security is a low priority, With 91% indicating that it is a medium or major priority.



Question

What solutions do you have in place to secure your core SaaS applications? (Choose all that apply)

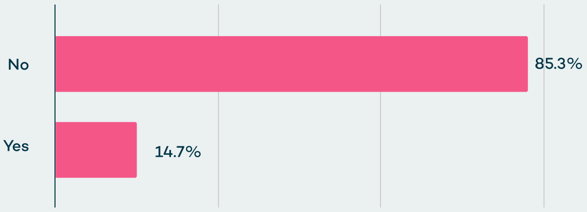
Of those who have a traditional security solution, most had either a CASB (53%) or an IdP (82%) – Neither of which secure non-human identities.



Question

Do you feel that your existing solutions provide the appropriate visibility and protection from the risks of SaaS-to-SaaS connections and third-party integrations?

The fact that 85% of CISOs were unhappy with their current solutions suggests the need for more solutions specifically designed to protect the SaaS mesh.



About Valence Threat Labs

Valence Security is the first security platform that enables organizations to enforce zero trust controls on the rapidly expanding mesh of third-party integrations connected to their sanctioned business critical SaaS apps. The platform ensures continuous compliance by automating the enforcement of least privilege access and revocation of unnecessary access across all of an organization’s API tokens, OAuth third-party apps, third-party integrations, and no/low-code automated workflows.

Valence Threat Labs is a vendor-agnostic research team dedicated to creating original research, responding to threats, and educating the cloud security community on best practices for securing third-party SaaS-to-SaaS integrations.

Report Contributors

The Valence Security team thanks our contributors for making this report possible.

YL VENTURES

Panorays