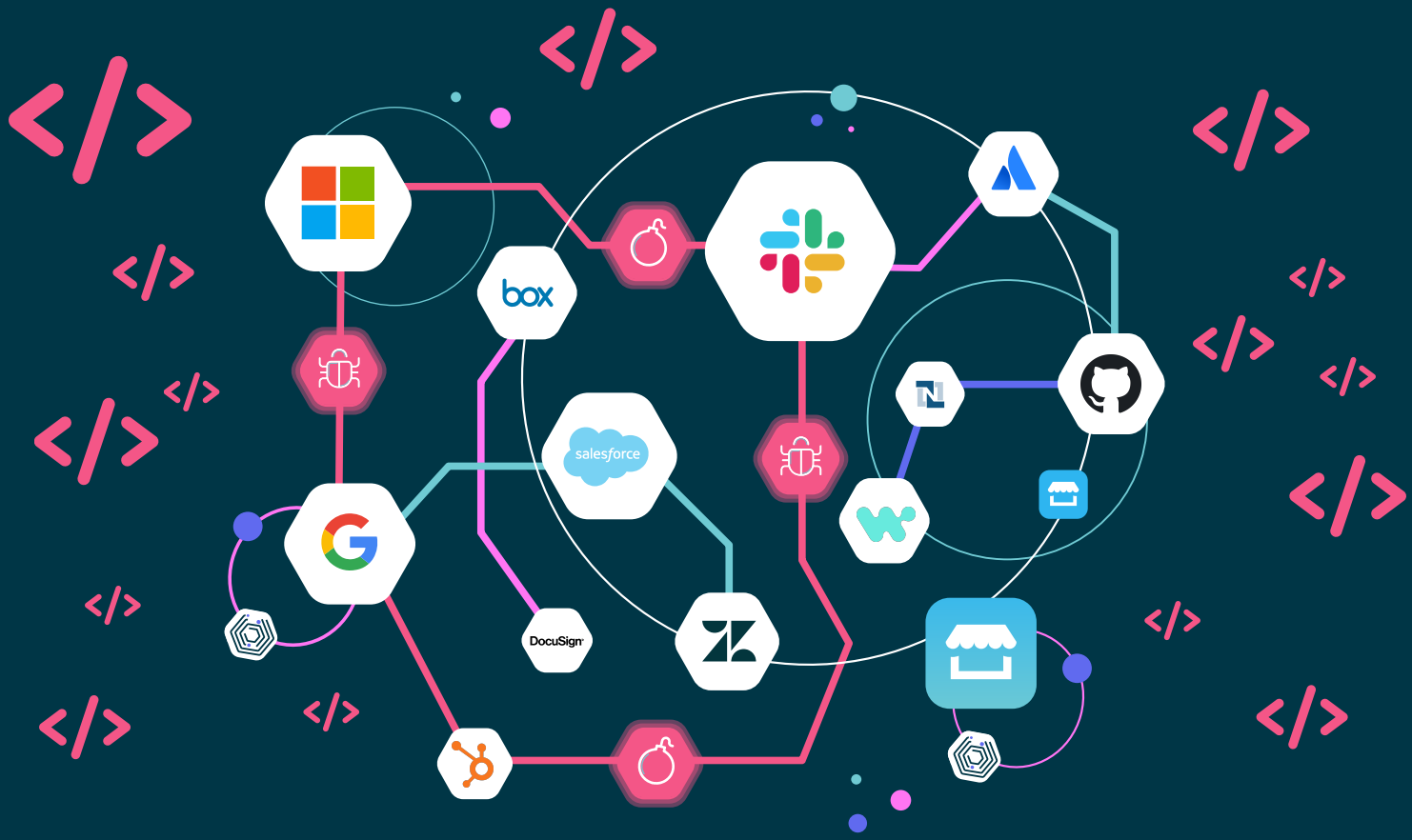


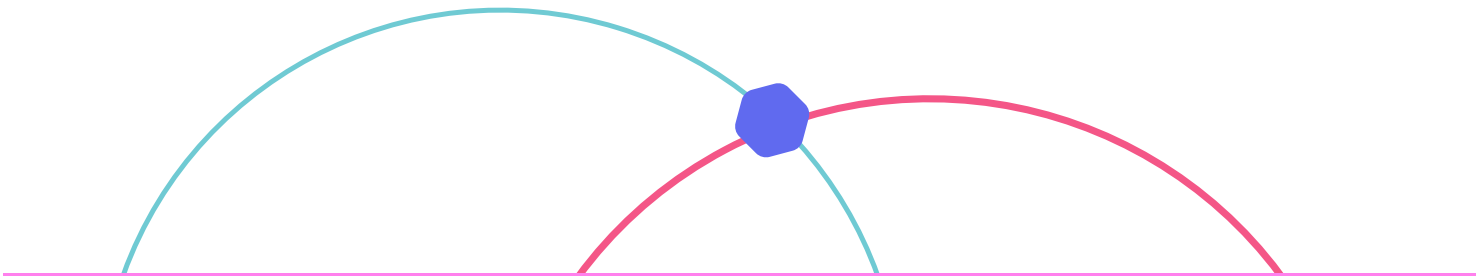

valence

# Contextualizing Supply Chain Risks In A SaaS Environment

Valence Threat Labs

# Table of Contents





# Intro

In the wake of the SolarWinds and Kaseya attacks, third-party cybersecurity risks remain top of mind, yet CISOs continue to experience significant friction with third-party risk management (TPRM).

According to the CISO Circuit report by YL Ventures, 70% of surveyed enterprise security leaders do not believe that TPRM solutions have helped them avoid risk. Much of their doubt is rooted in the lack of context in current TPRM processes. This is significant for a solution used by 83% of respondents.

In the meantime, bad actors have intensified their attacks on supply chains– transforming them into one of the most popular attack vectors. Compliance and board-level pressures around third-parties are rapidly mounting, placing further pressure on CISOs already struggling with the process. In the race to address these growing supply chain risks, it is worth investigating how we can optimize existing practices to better manage the potential risk to enterprise networks.

The CISO Circuit reveals two critical blind spots that keep us from actualizing the true potential of TPRM: how we interact with third parties and how they interact with each other in our own environments.

> "According to the latest edition of CISO Circuit by YL Ventures, 70% of the surveyed enterprise security leaders do not believe that TPRM solutions have meaningfully helped them avoid risk."

# The SaaS Boom

Third-party SaaS vendors have increasingly permeated every facet of our workflows and business processes. The adoption of SaaS applications and the race to optimize their use has led organizations to create more integrations between these applications to enable data flow and automated workflows.

Visually, we can imagine information passing through an interconnected web of SaaS solutions continuously pinging one another for access and data. These communications lie at the heart of our newly uber-streamlined workflows and accelerated productivity. They are also inherently risky gateways into our environments since they increase dependency on and interconnectivity with third-party vendors.

## Accounting for Dynamism

Lacking meaningful context, third-party risk management (TPRM) solutions are limited by critical blind spots that mute CISOs' confidence in their actual risk-mitigation. Where today's third-party integrations are continuous, widespread, and ever-evolving, current TPRM solutions tend to offer point-in-time assessments of the security posture of vendors, rather than assessing actual integrations with third-parties and vendor-customer relationships.

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, as business users quickly and indiscriminately connect their SaaS applications, the risk of unvetted supply chain access to business-critical applications like Salesforce, Microsoft 365 and Google Workspace increases dramatically. It then becomes a challenge for security and compliance teams to ensure proper coverage of their TPRM programs since they lack visibility into which vendors have access to their applications and the scope/context of such access in this ever-changing environment.

"As business users indiscriminately connect their SaaS applications,  the risk of unvetted supply chain access to business-critical applications like Salesforce, Microsoft 365 and Google Workspace increases dramatically."

## Current Best Practice Limitations

Best-practices, such as zero trust and proper data access protection, face limitations due to blind spots. They are impossible to implement without accounting for larger contexts and the often dynamic nature of third-party relationships and information. Even one misattribution can undermine zero trust, leading to over-privileged third-party access or to dormant vendors with unnecessary access. In addition, many enterprises suffer from "set-and-forget" third-party integrations that can either evade or bloat the supply-chain risk management process.  All of this means that an entire network of third parties is working with and exchanging enterprise data without adequate supervision and governance.

# Unlocking TPRM Potential

According to the CISO Circuit report by YL Ventures, CISOs are often more motivated by compliance than real security strategy when employing TPRM solutions. These findings underscore their lacking faith in TPRM efficacy.

It is possible to improve supply chain security and generate better third-party security best practices. However, solutions must demonstrate a better appreciation for actual implementation of third-party vendors and how that impacts the communication of our digital assets. Correspondingly, we must have a better understanding of integrations across every—or at least multiple—points of their lifetimes, to implement proper zero trust.

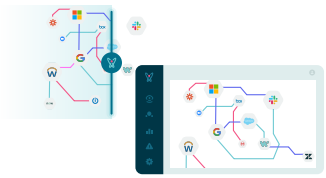
As we grow more dependent on third-party SaaS applications, we must extend third-party vendor risk assessments from their security controls to how we use and interact with the third-party itself. This does not negate the current utility of TPRM solutions; they are still among the most comprehensive approaches available to managing supply chain security. Nonetheless, without change, the persistence of these limitations all but guarantee that our supply chain protection remains incomplete.

"As we grow more dependent on third-party SaaS applications, we must extend third-party vendor risk assessments from their security controls to how we use and interact with the third-party itself."

To this end, acknowledging that it is ongoing and in need of more continuous attention is an important start. Extending the scope of third-party security risk factoring can, in turn, feedback into a more effective TPRM process. The more engaged we become in seeing, tracking and governing third-party integrations into enterprise networks, the more data we can offer to the risk scoring process. Though it may verge on the idealistic, this would likely improve the accuracy of TPRM results and consequential CISO confidence in TPRM reliability.

# The Valence Platform

Valence manages and secures your supply chain risks by delivering visibility, reducing unauthorized access, and preventing data loss. With Valence you can quickly and effectively:



## Map Your Supply Chain

Valence quickly identifies, inventories and maps your SaaS-to-SaaS supply chain to deliver full visibility into non-human integrations, OAuth access tokens, API Keys, permission scopes and workflows.

## Monitor Your Supply Chain

Valence monitors the topology, configuration and activity across your SaaS-to-SaaS supply chain to detect new connections, anomalous activities and data access, overprovisioned privileges and out-of-compliance workflows.

## Mitigate Your Supply Chain Risk

Valence extends zehtrust principles to your SaaS-to-SaaS supply chain, defining and enforcing policy controls such as least privilege access and revocation of compromised and outdated tokens.

Valence secures app interconnectivity, protecting a risk surface undetected by existing solutions that treat applications in isolation

Valence shines a light on business application shadow connectivity and assesses the supply chain risk surface of third-party vendors

Valence integrates with event management and security automation platforms to enable continuous monitoring and effective collaboration

## Secure Your SaaS-to-SaaS Supply Chain Today

Resquest a FREE Risk Assessment