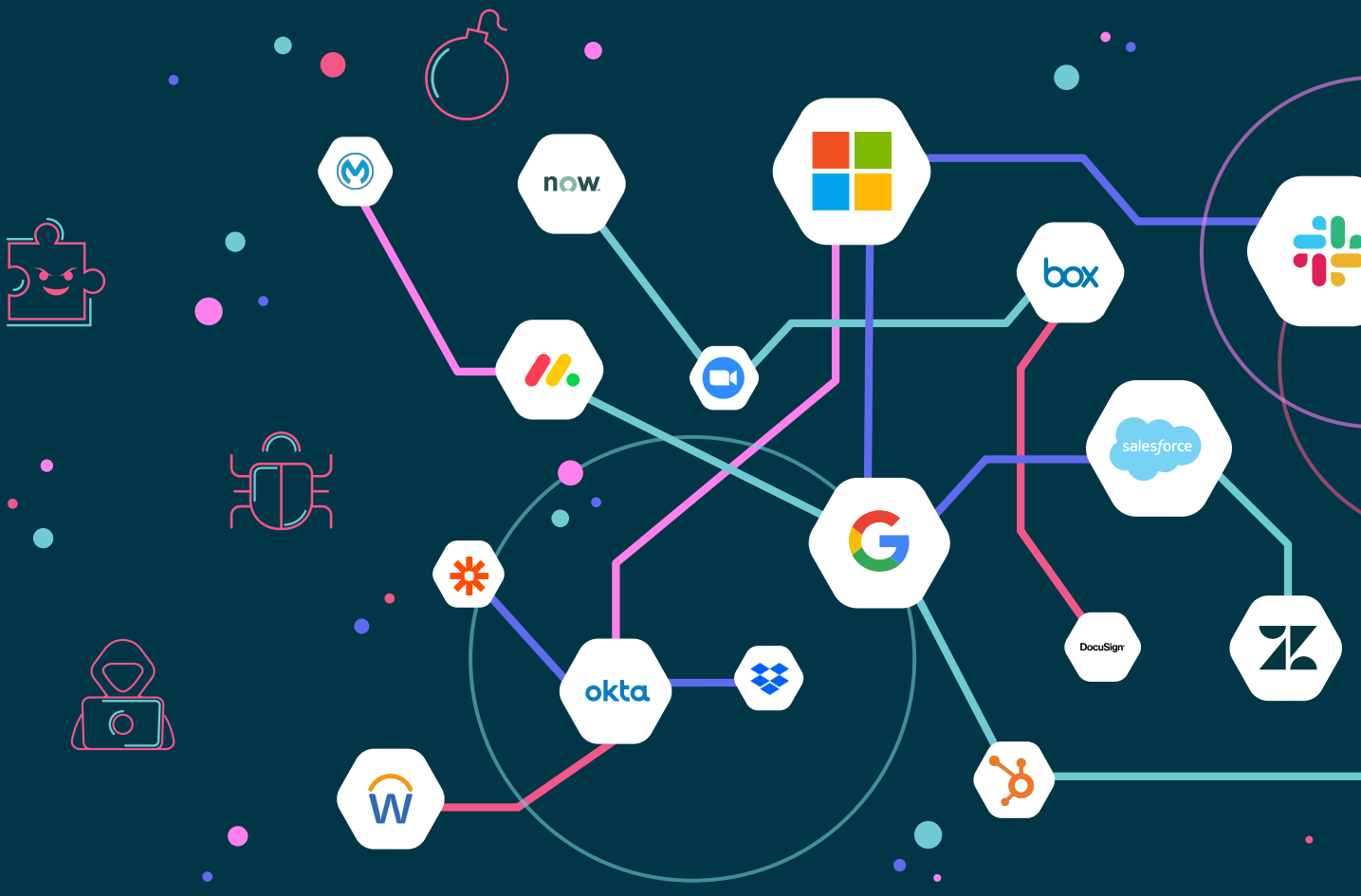
valence

# The SaaS-to-SaaS Supply Chain Threat Landscape

White Paper




valencesecurity.com

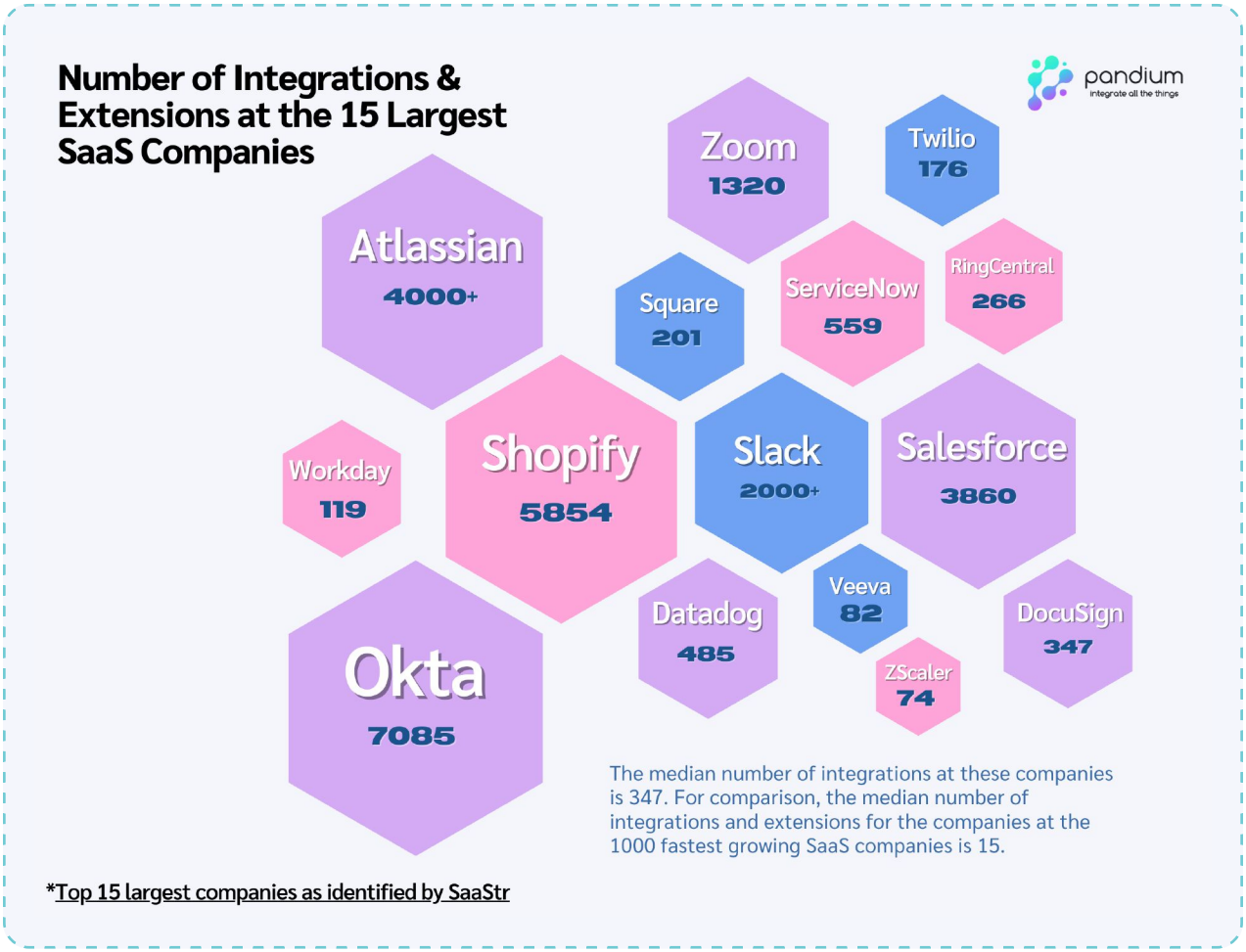
# Table of Contents

# The SaaS-to-SaaS Supply Chain

As the number of SaaS applications used by organizations rises, so do the benefits inherent in the ever-growing SaaS sprawl. Connectivity and transparency are fundamental in today's business environment and are the vehicles for improved information sharing, scalable workflows, agility, and efficiency.

In the SaaS age, these benefits are multiplied as organizations are able to choose their best-of-breed SaaS applications and use hyperautomation no/low code platforms (like Workato, Zapier, etc.) to integrate them with other applications, creating the convoluted and ever-growing **SaaS-to-SaaS supply chain.**

Pandium's 2020 report on "The State of Product Integrations at the SaaS 1000" indicates that the 15 largest SaaS companies (including Zoom, Shopify, Salesforce, Slack and Okta) each have an average of 347 integrations and extensions available.



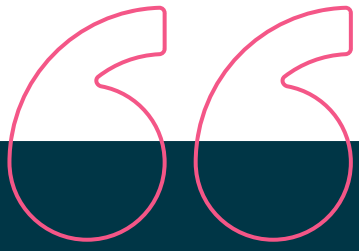

The State of Product Integrations at the SaaS 1000

The ability to seamlessly integrate business applications using organization-wide API integrations, no/low-code platforms and SaaS marketplaces is crucial for enterprises. Zoom has recently announced that it has created a dedicated fund of $100M to expand its communication ecosystem and extend Zoom's platform play by encouraging third-party developers to build applications and integration extensions.

SaaS platforms have intrinsic motivation to encourage users to subscribe to as many applications as possible. This creates vendor lock-in effects, as enterprises find themselves entrenched deeper into the platform feature set, and make switching to a different vendor cost-prohibitive.

This causes those platforms to tend to implement more and more features that encourage integrations and make them simpler to create (for example, Slack actively promotes relevant applications for subscription when you paste a URL, and it usually takes only two additional clicks to complete the subscription).

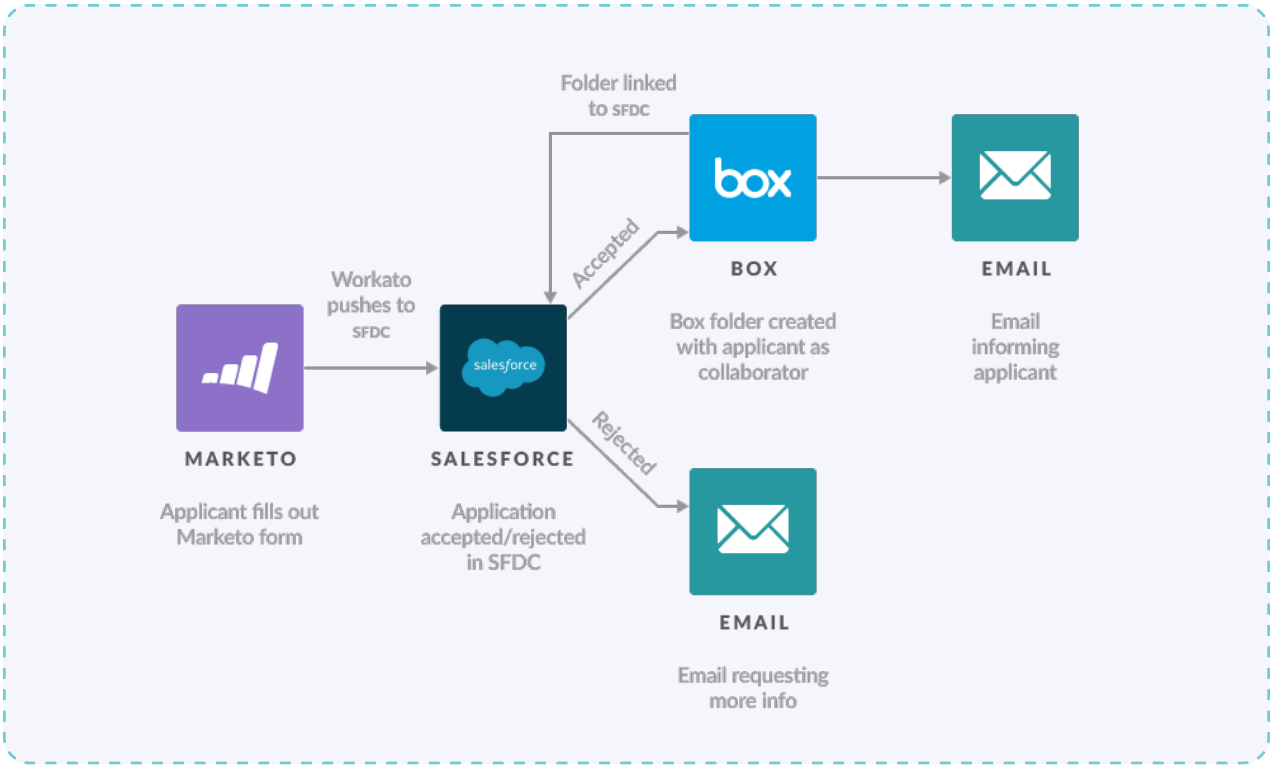
Facilitating communication and providing seamless collaboration opportunities in an automated fashion is becoming the standard for the modern workplace, as Gartner estimates that over 70% of large commercial organizations have dozens of hyperautomation initiatives underway.



Gartner®

"Gartner estimates that more than 70% of large commercial organizations have dozens of hyperautomation initiatives underway"

Gartner Top Strategic Technology Trends for 2021

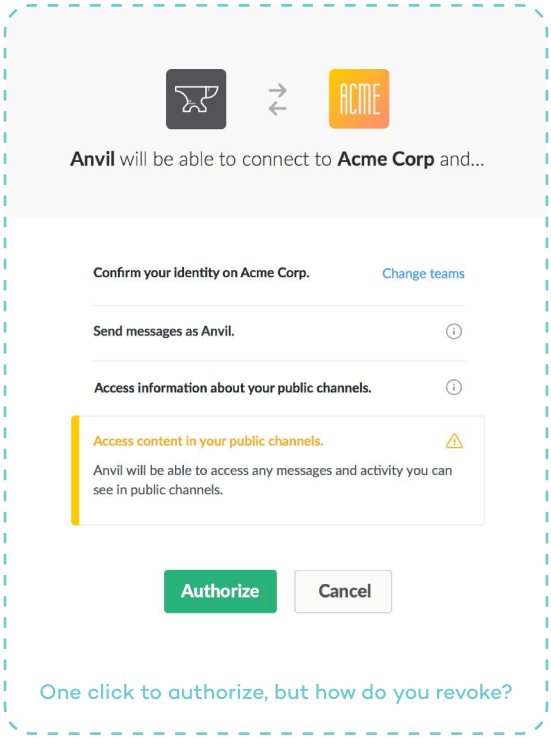



Workato automation workflow example

The limitations inherent in on-prem and network-based integrations and workflows allowed security teams to tightly control and govern the organization's applications integration portfolio but hindered users' ability to discover tools and platforms that benefit productivity, drive innovation and save time and resources for the organization.

As digitalization transforms business processes through the cloud, end-users now have the ability to onboard new third-party services independently, without organizational governance or security oversight, using "set and forget" integrations and lacking continuous validation or integration into TPRM processes.

However, revoking these integrations is usually a complex feature, hidden behind multiple screens in the settings screen. What this translates to is users almost never revoking access, so even a single-day experiment with a vendor turns into continuous and persistent access.

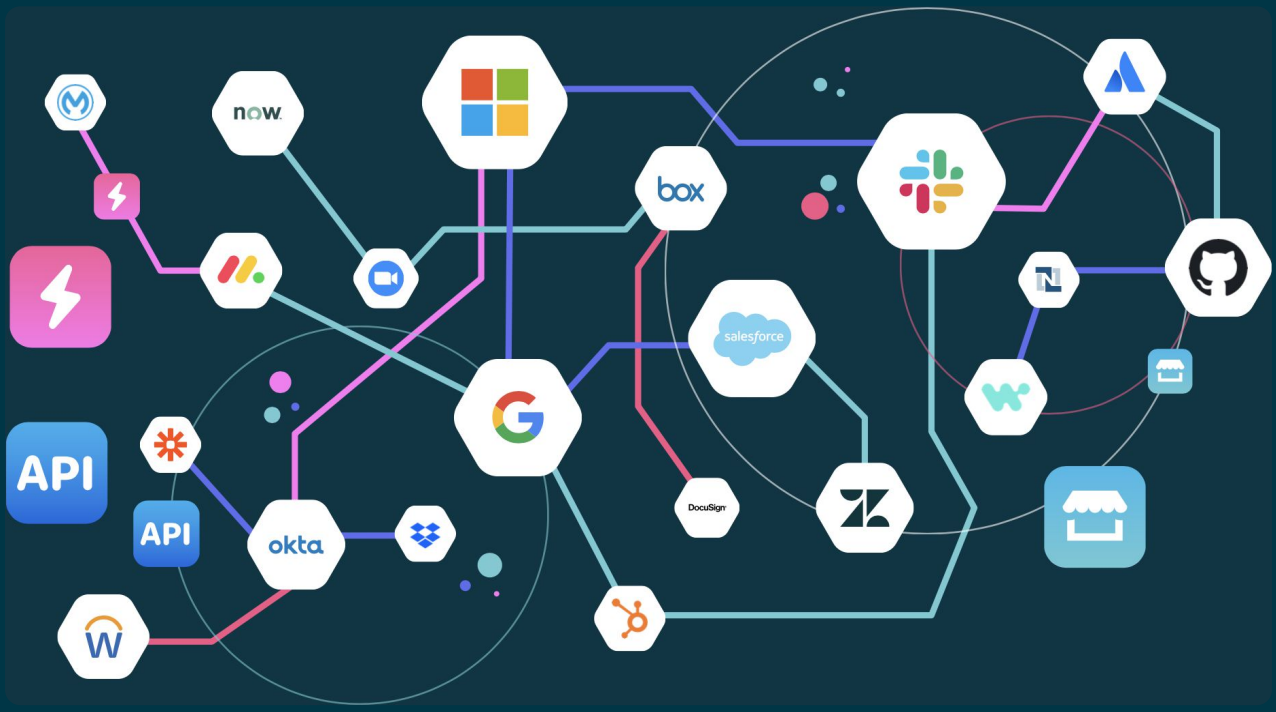



One click to authorize, but how do you revoke?

This drive to connect and the ensuing benefits for both users and enterprises cannot overshadow the risks inherent in automated processes involving third parties and indiscriminate shadow connectivity, which security teams may be completely blind to.

At Valence, we strive to raise the awareness of both security teams and executives to this new and constantly expanding supply chain risk surface, and provide remediation tools to map, manage and mitigate the SaaS-to-SaaS supply chain.

The following report offers a comprehensive review of what security teams should know about the SaaS-to-SaaS supply chin and its challenges.

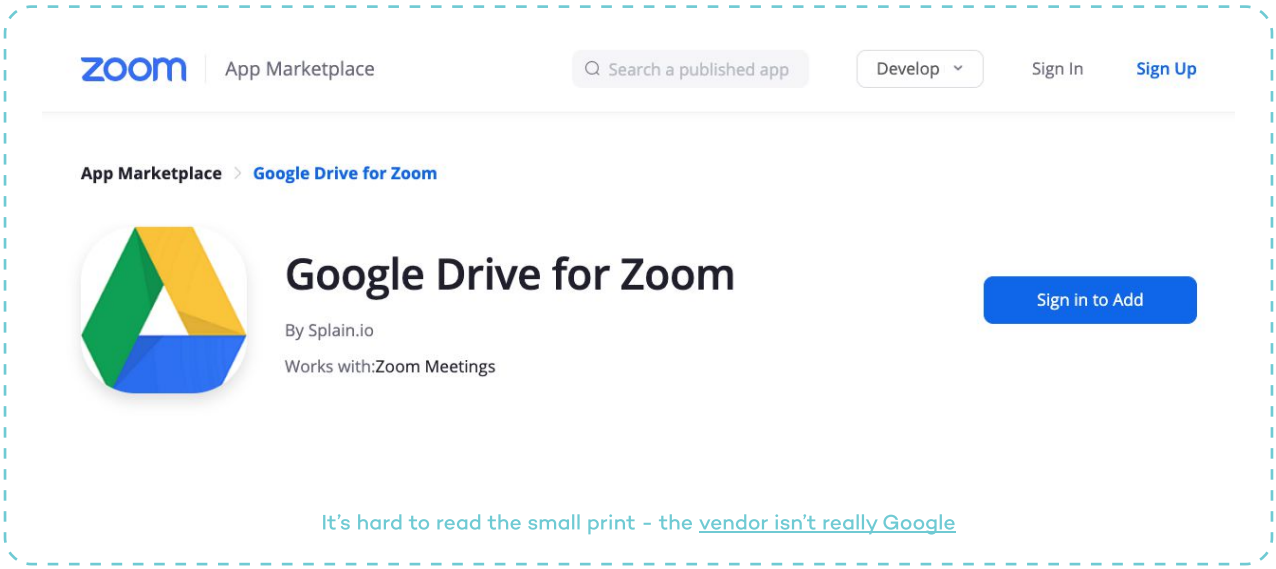


# SaaS-to-SaaS Supply Chain Security Risks

Essentially, it all comes down to managing trust. While every new integration takes business to a new, streamlined and efficient level, security teams should be wary of developing an organizational dependency on external entities and expect them to secure their internal assets.

Digital interaction in the cloud era is predicated upon user identities, establishing privileges and controls for their access to data and assets. Traditional access control solutions such as managed devices, IdP, CASB, and ZTNA have been relatively successful in securing human-to-app integrations.

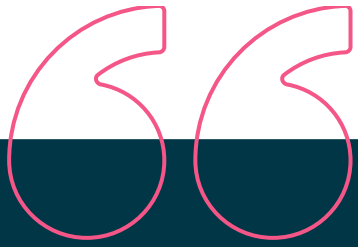
Security teams focus on these integrations, controlling user accounts that expose data intentionally or not. Non-human or app-to-app integrations operate and act in the background, connecting through service accounts, constantly 'logged in' and available to malicious actors.




While onboarding common applications such as Google Drive for Zoom Marketplace may seem secure to the user, a closer look at the onboarding process may uncover third-party integrations that are obfuscated or cunningly hidden as the end-user unwittingly approves access to new, unauthorized third-party vendors.

Similarly, an organization's development pipeline may be fraught with citizen developers who use no-code tools to assemble automated configurable workflows with no security involvement or awareness. As an organization scales, so does its SaaS-to-SaaS supply chain - and the shadow connectivity generated by users' blind trust in these services and their integrations.

A simple case of using a popular third-party email client, EdisonMail, jeopardized users' personal data as well as any information stored on their Gmail, Microsoft or iCloud accounts due to the email client's integrations. Marketplaces like Google Workspace and others host business applications that are critical for businesses, but users are not aware that they provide privileges and scopes to external applications and possible malicious third-party apps.



"Return Path employees read about 8,000 unredacted emails to help train the company's software... Letting employees read user emails has become "common practice" for companies"

Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail, The Wall Street Journel

The free flow of data in the supply chain and its constant growth result in over-privileged API integrations, shadow OAuth tokens and ungoverned automated workflows, forming a new risk surface. Malicious actors abuse these integrations and take advantage of the SaaS-to-SaaS supply chain in order to leverage non-human identities and shadow connectivity.

An example of such leverageable loopholes are applications developed by Google Workspace users. Using Google's Apps Scripts platform, users can develop business applications that integrate with Google Workspace, using a highly optimized serverless script for automating Google services.

These home-grown applications interact with Google Workspace users via Google OAuth 2.0 to receive consent, permanent access privileges into these users' Google suite of services. These privileges can be garnered through consent phishing, and are also attractive for backdooring accounts as App Scripts lie beyond the purview and sight of standard security controls and on-device monitoring, in a completely serverless environment.

Hyperautomation platforms like Microsoft Power Platform, Zapier and Workato have become increasingly popular, as they improve data sharing across various applications in the business environment, adding to the ease of data flows within the SaaS-to-SaaS supply chain. Additionally, hyperautomation breaks down data silos and communication barriers and contributes to scalability and profitability as it replaces manual workflows.

However, the use of these platforms without appropriate security oversight may lead to shadow connectivity, over-provisioned privileges and possible misconfigurations as was the case with Microsoft Power Apps.

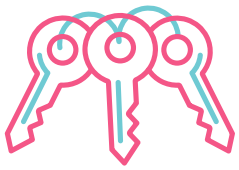
> "Misconfigured Power Apps from Microsoft led to more than a thousand web apps accessible to anyone who found them"
>
> 38M Records Were Exposed Online—Including Contact-Tracing Info, Wired

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. The extended ownership citizen developers receive increases the likelihood of human error, making it easier for attackers to leverage them in order to steal the keys to the kingdom.


Example record for Microsoft Global Payroll Services collection

By Design: How Default Permissions on Microsoft Power Apps Exposed Millions, UpGuard

# The Anatomy of SaaS-to SaaS Supply Chain Attacks

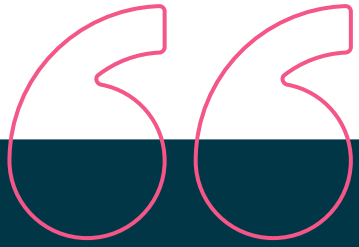


## 1 | Supply Chain API Takeovers

Supply chain API takeovers: Arguably the most famous attack of recent years, the SolarWinds campaign also targeted the Microsoft 365 accounts of Mimecast customers.

The attackers abused Mimecast's high privileges to gain unauthorized access to Mimecast certificates and keys, and obtain sensitive data well beyond the Mimecast environment.

A similar breach occurred when attackers leveraged a vulnerability found in Waydev, an analytics platform and third-party tool used by software companies, to steal GitHub and GitLab OAuth tokens after gaining access to the platform's databases.



> "Hackers had compromised a certificate used to authenticate Mimecast's... products to Microsoft 365 Exchange Web Services"
>
> Mimecast Breach Linked To SolarWinds Hack, Allowed Cloud Services Access, CRN

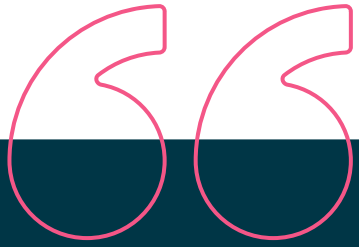
# The Anatomy of SaaS-to-SaaS Supply Chain Attacks

## 2 | Malicious 3rd Party Apps and Consent Phishing

With heightened adoption of MFA, classic phishing attacks have grown ineffective - a username and password will not grant attackers access any longer. Therefore, attackers attempt to trick users into consenting to malicious 3rd party apps and OAuth tokens.

According to a warning by Microsoft from 2020, they leverage the ease of authorizing new plugins and extensions with limited visibility for security teams.

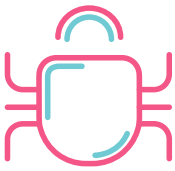
This technique was used to gain unauthorized access to the SANS Institute emails and to steal users' contacts and mail by APT groups.



"A data breach that exposed roughly 28,000 records containing personally identifiable information to a malicious Office 365 add-on"

SANS Institute Breach Proves Anyone Can Fall Victim to a 'Consent Phishing' Scam

# The Anatomy of SaaS-to SaaS Supply Chain Attacks

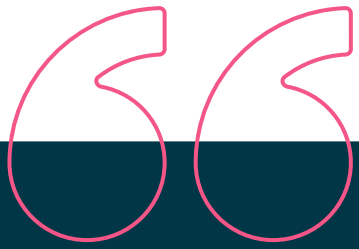


**3 | Non-human Identity Based Attacks**

Attackers leverage the increased usage of non-human identities and app-to-app connectivity to execute exfiltration, lateral movement and privilege escalation techniques.

In the SolarWinds breach, attackers manipulated Microsoft OAuth app certificates to abuse app-to-app trust and gain unauthorized access to sensitive data.

In another case, Microsoft published that attackers used Microsoft's low-code platform, Power Platform, to maintain persistence and exfiltrate sensitive data.



"The SolarWinds supply chain attackers manipulated OAuth app certificates to maintain persistence and access privileged resources including email"

SolarWinds Attackers Manipulated OAuth App Certificates, BankInfoSecurity

# Introducing Valence

Valence is the first security platform that helps organizations manage the risks associated with SaaS interconnectivity. The platform connects to core business applications, analyzing configurations and activity logs. Within minutes, Valence provides organizations with visibility, continuous monitoring, and automatic policy enforcement and remediation.

First, the platform generates an inventory of all SaaS-to-SaaS connectivity, mapping third-party integrations, OAuth tokens, and automated workflows.

The platform then continuously monitors topology changes and activities to detect anomalies, compromised tokens, and track how PII and sensitive data flows between applications. Finally, the platform allows security teams to mitigate risks by providing a self-serve platform that applies zero trust principles, enforces least privilege access, and ensures compliance of all automated workflows.

Valence helps you gain contextual visibility and reduce risks associated with your third-party integrations and app-to-app connectivity.