Astrix

The Ultimate Guide to Securing App-to-App Integrations

Safely unlocking productivity for the hyper-connected enterprise

Table of contents

Introduction

The crippling recent attacks on Github, Okta, and Mailchimp demonstrate the severe risk posed by third-party apps integrations to your organization's security posture. These recent attacks demonstrate the extent in wich ungoverned app-to-app connections massively increase the likelihood of supply chain attacks, data breaches, and compliance violations. And the scenario is anything but hypothetical.

Imagine:

- A marketing operations manager trialing a new SaaS prospecting tool – and integrating it directly with your Salesforce instance to automatically sync leads.
- An engineering team lead using a new cloud-based productivity tool that relies on API access to your source code repositories.

IIn both cases (and many more), employees are freely adopting and integrating new technology – all in an effort to get their jobs done – without your knowledge. The result? Each of these connections extends your attack surface.

You might already be aware of the problem and looking for a way to close the security gap. If so, that's a great start – but you should know that you're probably only seeing a fraction of the challenge. In the era of product-led growth and bottom-up software adoption, it's virtually impossible for security leaders to have visibility into all the integrations between cloud applications deployed in their environment - as the average enterprise uses 1,400 cloud services.

And even if you're aware of the magnitude of the challenge and specifically tasked with handling this tangled web of app-to-app connectivity – it's no easy task. Current security approaches fall short in helping security leaders take control of a sprawling web of third-party application integrations.

This ebook will give you the tools to close the connectivity security gap and significantly improve your overall security posture. Keep reading to understand the exact risks involved in app-to-app connectivity, best practices to minimize your attack surface, and how Astrix can help.

Let's get going.

Five factors changing the game

By any measure, the adoption of third-party applications has increased exponentially over recent years. (See "third-party adoption by the numbers" for more details.)

1,400	+18%	70%
Average number of cloud services used by large enterprises (Source)	Annual growth rate of the market for SaaS applications (Source)	Percentage of CIO's who report adopting third-party applications for agility and scalability (Source)

Indeed, selecting and deploying third-party apps has become a cornerstone of many organization's IT strategy – as a way of augmenting in-house capabilities, filling gaps, or accelerating business outcomes. Forrester identifies software platform and application vendors as one of four key sources of partnership value embraced by future-fit companies.

But what's actually driving the breakneck adoption of third-party applications? Five macro factors have shaped an environment in which enterprises' reliance on third-party software and integration has become virtually essential to survival.

> ***"Innovation through ecosystems happens when organizations actively collaborate with their cloud, software, business, and services providers — value aligned through common purpose and financial incentives."***
>
> ***- Forrester***

Factor	What it means	Why it matters
1. The evolution of SaaS ecosystems	Monolithic applications have given way to a federation of micro-apps, increasingly organized into integration-first SaaS ecosystems and marketplaces	Enterprises will increasingly rely on webs of interconnected apps rather than a linear "stack"
2. The new digital workplace	The shift to supporting remote and hybrid work has meant empowering workers to adopt the tools they need to get the job done	In the workplace of the future, employees will increasingly expect the autonomy to adopt their own digital toolset
3. Product-led growth (PLG)	The traditional enterprise sales process has given way to a new user journey fueled by product trial and bottom-up adoption	The barriers to deployment and trial of new third-party applications has never been lower
4. The drive for hyper-automation	In the quest for growth and productivity, enterprises are increasingly relying on third-party applications to fill gaps or augment their capabilities	Any increasingly competitive global economy demands that enterprises identify and exploit any source of competitive advantage – often from third-party applications
5. Low-code and no-code integration platforms	Data and apps are only valuable in the enterprise if they are connected to one another. A new generation of iPaaS platforms focused on citizen integrators (including vendors as disparate as Zapier and Mulesoft) has made it easier than ever to keep the organization connected.	Third-party application usage will only increase as it becomes easier to link data and workflows from one to another

These trends aren't going away any time soon. Indeed, many industry observers believe that these will be among the defining features of the 2022 cloud adoption landscape.

Ultimately, the need for growth and productivity have furnished the "why" for third-party application integration – while massive evolutions in technology and ways of working have supplied the "how."

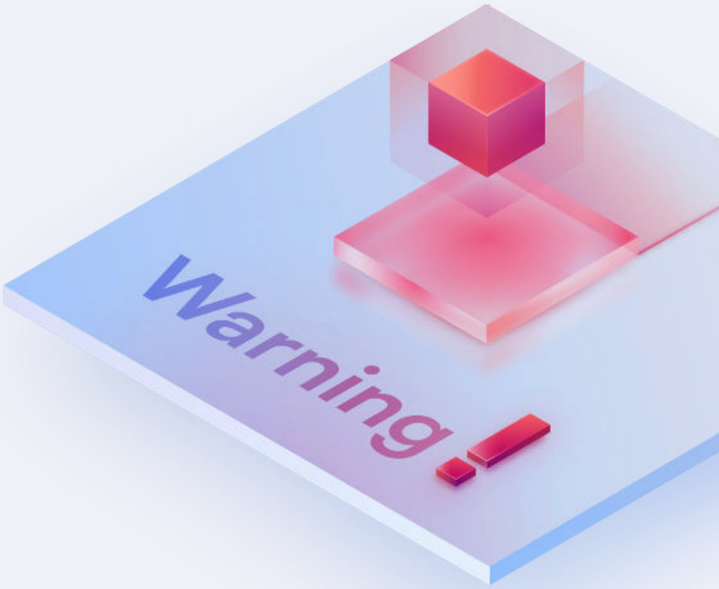
Top cyber risks of third-party integrations

While third-party applications integrated with core systems (like Google Workspace, Office 365, Salesforce, and Github) can help organizations achieve breakthrough growth and productivity, they also bring daunting new security challenges. These integrations effectively define a new cloud perimeter, one in which the interconnectivity between third-party applications and core systems has become the most vulnerable attack vector, threatening application posture, sensitive data, and compliance.

Case in point: 93% of companies [report](#) a cybersecurity breach in the past year related to weaknesses in their digital supply chain. What are some of the primary risks associated with third-party integrations?

Risk #1: Supply chain attacks

- **What it is:** A third-party app integrated to a trustworthy central platform may "leak" sensitive data into a less secure environment. Malicious actors abuse security vulnerabilities associated with a legitimate (but less secure) third-party application – and exploit its privileged access to sensitive information (like credentials or data).
- **Recent example:** Hackers [compromised the software development tool Codecov](#) to gain access to – and rapidly copy and export to an attacker-controlled server – sensitive secrets,credentials and IP associated with software accounts at thousands of clients.
- **Why third-party integrations increase the risk:** More and more, third-party applications hold the "keys to the kingdom": the most privileged credentials in the enterprise. Any third-party application that can be compromised opens up the possibility of unauthorized intrusion (and data extraction, ransoming, and more) by malicious actors.



Risk #2: Direct malicious access

- **What it is:** Malicious actors seek direct access to core platforms by tricking users into providing consent (via OAuth permissions rather than explicit credential phishing) or by taking advantage of leaked API keys, certificates, webhooks urls, etc.
- **Recent example:** Microsoft recently warned of a phishing attack in which Office 365 users received emails intended to trick them into granting OAuth permissions to a fake app.
- **Why third-party integrations increase the risk:** With third-party applications increasingly integrated to core platforms, access tokens enable malicious actors access to data and operations on organization critical systems.

Risk #3: Compliance violations

- **What it is:** An act that compromises an organization's ability to comply with relevant governmental, legal, or industry frameworks – for example, data privacy regulations (like GDPR) or security and governance (like SOC 2).
- **Recent example:** Ticketmaster received a $1.6 million fine for GDPR violations after hackers exploited vulnerabilities in the code of a third-party chat app vendor on its checkout page, exposing customers' personal and payment data.
- **Why third-party integrations increase the risk:** Any third-party application involved in data processing is part of an enterprise's regulatory purview – meaning that the organization is ultimately responsible (often financially and legally) for its handling of sensitive data.

Critical capabilities for securing app-to-app integrations

The interconnectivity between apps and critical systems clearly opens up a vast, exploitable new attack surface. Security leaders looking to minimize the risks arising from the new app-to-app connectivity web must ensure that they have three critical capabilities.

Secure all your critical systems:

From business apps and engineering systems, to data warehouses and low code/no-code platforms, it is essential you continuously monitor all your critical systems across SaaS, PaaS and IaaS environments to ensure they securely communicate with third-party applications and with each other.

Secure all types of app-to-app integrations:

While critical systems like Salesforce and Office 365 are usually integrated with Marketplace third-party apps, engineering systems like Github and Big Query are often connected to third-party services through advanced integrations created by developers and DevOps engineers.

It is essential you monitor all types of integration including:

- Third-party service integrations
- Indirect integrations enabled via no-code / low code automation platforms
- Issued tokens, API keys, service accounts

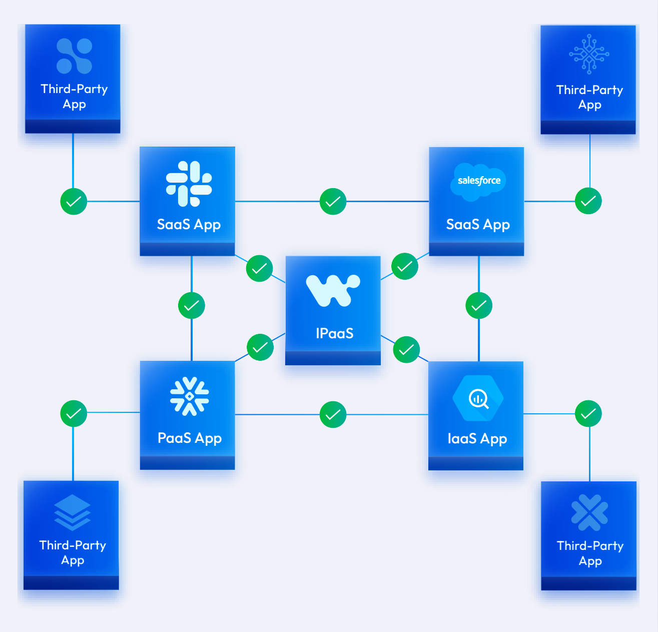
Continuous threat detection & remediation:

it is essential you have the ability to quickly uncover and remediate integration risks threatening your application posture, sensitive data, and compliance as soon as they emerge.

That includes:

- Malicious third-party integrations such as impersonating applications, API account takeover, and OAuth attacks.
- Anomalies and suspicious integration behavior (e.g. a suspicious source IP location)
- Misconfigured / over-permissive integrations
- Redundant apps, tokens, and keys (of past employees/ invalid applications)

See Graphic 1 for a breakdown of what is actually needed to close the app-to-app security gap.



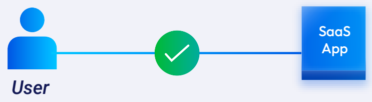
***Graphic 1:** Critical capabilities for securing app-to-app integrations*

Why current security solutions fall short

Existing security solutions can't keep up with the rapidly-growing challenges of third-party app interconnectivity. Legacy approaches often address user (rather than application) access, as this was previously the primary threat vector. They also tend to focus on the vulnerabilities of standalone applications – not the connectivity between the apps – and are built to address limited environments, like SaaS business applications alone. These solutions were also intended to match a slower pace of cloud adoption, such that all third-party services could undergo a thorough, lengthy manual review process.

Today, as app-to-app connectivity proliferates rapidly, these solutions simply fall short. See Graphic 2 to better understand why.

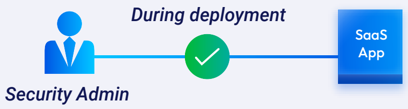
User Access Management



Authenticates user identity and provides tools to govern user access to cloud-based apps and services.
Enables security teams to easily provision the right access for the right user.

Limitations:
Only addresses user access – not app-to-app connectivity

Third-Party Risk Management (TPRM)

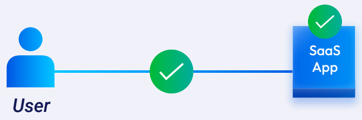


Tools and practices (e.g., questionnaires) designed to score third party providers based on the cybersecurity risk they pose to an organization. Enables security teams to easily provision the right access fo the right user.

Limitations:

- Assess the third-party integrationsecurityevel only during the deployment, rather than continually monitoring its behavior afterward.
- Manually-intensive and not well suited to bottom-up software adoption (e.g., PLG)

Cloud Access Security Broker (CASB)

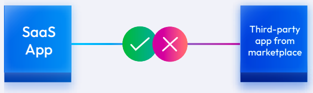


Enables secure user access to SaaS application and secure user activity within the apps themselves by alerting on anomalous or suspicious behavior.
Helps security teams compile a SaaS inventory, classify the risk associated with each, and enforce policy guidelines and compliance requirements.

Limitations:

- Focus on user access policies to standalone applications – not on points of integration and connectivity between diverse cloud apps
- Partially identify integration risks - without providing sufficient threat context for mitigation

SaaS Security Posture Management (SSPM)



Monitors cloud-based SaaS tools to ensure proper configuration and prevent compliance drift.

Limitations:

- Only covers SaaS applications – not other sources of third-party integration (IaaS, Data services, iPaaS, etc)
- Partial support in third-party integrations (focused on marketplace apps)
- Lacking real-time behavior analysis indicating malicious or suspicious integrations

***Graphic 2:** Why current solutions don't close the app-to-app security gap*

Four steps to reduce the app-to-app integration attack surface

Given the gaps in existing technology, what should third-party integration access management look like?

Whether you are partnering with a vendor or architecting your own approach in-house, there are four steps that security teams should follow to go from gatekeepers to growth partners.

Step 1: Assemble a clear picture

Compile a one-stop inventory of all of your organization's third-party connections – across not just SaaS deployments, but all critical environments. This shouldn't be a "flat" report of third-party integrations.. Rather, it should leverage contextual analysis to identify the actual exposure of each app's connections. (For example, a given app might have many connections to a core system – all of which have low levels of permission. In contrast, another might have a small number of highly privileged permissions connected, some of which are deprecated.) Consider using exposure scoring as a way of ingesting the app-to-app connectivity landscape at a glance.

Step 2: Detect risks

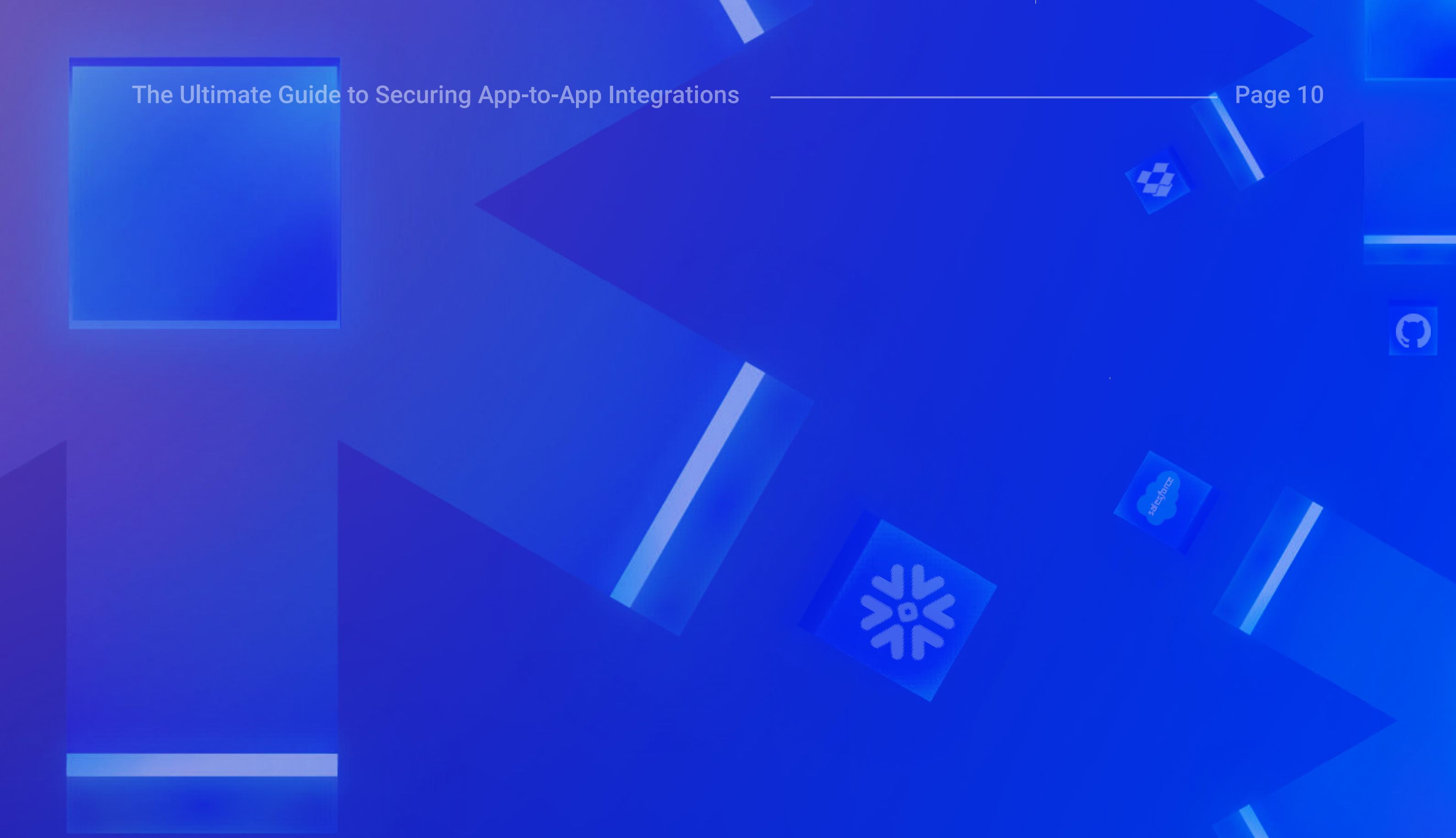
Identify external connection threats, integration misuse, and anomalies. It can often be challenging to parse the nuances of specific third-party integrations; a vendor may be able to help with a logic engine built for the complexities of third-party integration.

Step 3: Remediate gaps

Deliver actionable mitigations to address emerging threats and to reduce attack surface. Which over-privileged third-party integrations should be immediately de-provisioned? Which should be reconfigured to less permissive settings?

Step 4: Manage the integration lifecycle

User access management provides a blueprint for managing the full user cycle. Modern security teams focused on third-party integration risk seek out out-of-the-box and zero-trust-inspired security tools to gain control over all app-layer access, set enforcement guardrails and prevent policy drifts.



Moving forward: the age of hyperconnectivity

Ultimately, security leaders need a technology solution that is built to manage the growing web of third-party integrations – providing control over the entire lifecycle of app-to-app connectivity.

That's where Astrix Security comes in. With agentless, one-click deployment, Astrix enables security teams to instantly see through the fog of connections, detect redundant, misconfigured and malicious third-party exposure to their critical systems – enabling their business to unleash the power of integrations and automation while seamlessly controlling their security and compliance.

Interested in learning more?
Feel free to contact us for a demo.