cynet

The Guide for

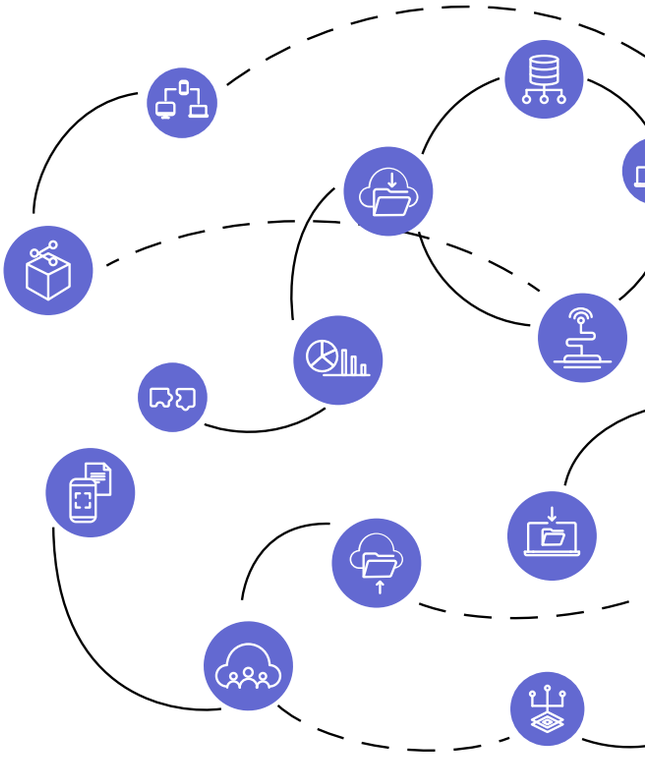
Reducing SaaS Applications Risk

for Lean IT Security Teams

Learn

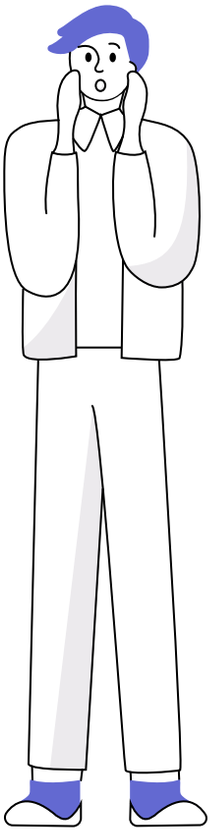
- How organizations are increasingly relying on SaaS applications.
- The key risks surrounding SaaS application.
- How to minimize the security risks associated with SaaS applications and vendors.
- How tools like SaaS Security Posture Management (SSPM) help organizations reduce SaaS risk that is under their control.

Intro



Software as a service (SaaS) applications have undergone a remarkable evolution over the last two decades. The first online applications offered an innovative approach to IT. As the SaaS ecosystem expanded and improved, these applications leapt outside the realm of IT to become the centerpiece of the enterprise strategy. It's not an overstatement to say that most of today's companies run on SaaS.

To put this evolution in context: By 2017 nearly 40% of companies relied entirely on SaaS, and 73% planned to by 2020. Rates of adoption are likely even higher than anticipated due to the Covid-19 pandemic, which accelerated SaaS usage as companies rushed to adapt operations to remote work and social distancing. Everyone understands that businesses run on technology- and SaaS is increasingly seen as the first, best, and only viable option.



The average midsize company now uses 185 SaaS apps, while the average enterprise uses 288. Diving deeper, the number of app-to-person connections, which track how multiple employees use multiple apps, was 4,406 at midsize companies and 21,580 at enterprises. As these metrics make clear, companies are deeply dependent on SaaS to accommodate every workload in every department. Take away these apps...and everything grinds to a halt.

Which brings us to the subject of this eBook. As SaaS becomes intertwined with operations and ever more work shifts into the cloud, the risk of a digital disaster is impossible to ignore. We will explore that risk in the following pages, highlighting how it puts extra stress on lean security teams and then outlining measures every team should take to ensure that SaaS applications aren't ticking time bombs.

Understanding SaaS Risk

Let's begin with a discussion of risk in general. Contrary to popular opinion, risk is not "things that could go wrong." Vulnerabilities and weaknesses are important to identify, of course, but focusing on those alone underestimates how risk afflicts an organization. For something like SaaS that intersects with business outcomes at so many different points, companies need a more nuanced understanding of risk.

Jack Jones and Jack Freund, two of the leading thinkers on risk management, define risk as the probable frequency and probable magnitude of future loss. Risk, in those terms, is less about the cause than the effect. To put it differently, companies can only appreciate risk once they understand the full extent of the damage.

Applying that definition to SaaS reveals how risky it really is. The enterprise-wide footprint of SaaS means that issues can (and do) happen frequently, repeatedly, and often with little to no warning. They range from temporary service disruptions to large scale data breaches. The importance of SaaS also means that any issue poses great risk of loss – whether that's productivity, compliance, or customers. When companies depend on SaaS for everything they do, it represents one of the greatest risks they face. Something seen as the key asset for the modern enterprise must also be seen in a different context: As a liability that casts a shadow over everything.

Where SaaS Risk Originates From

Losses resulting from SaaS risks can take countless forms that are unique to each company. It would be impossible to outline everything in one document. However, one way to encapsulate the consequences is to explore where SaaS risk originates from. Two decades of heavy reliance on cloud-based software leaves few doubts about the drawbacks. Some frequent sources of SaaS risk include:

- **SaaS as an Attack Vector** – There are more SaaS providers than ever, some with inadequate security controls. Hackers may breach a SaaS provider to gain easy entry to their clients. The practicality of SaaS as an attack vector helps explain the steady uptick in supply chain attacks where threats arrive through trusted third parties – like SaaS providers.

- **Provider Data Breaches** – The service aspect of SaaS often involves storing or processing data for clients. That means a company's data is at the mercy of the provider's protections, which may not be up to par.

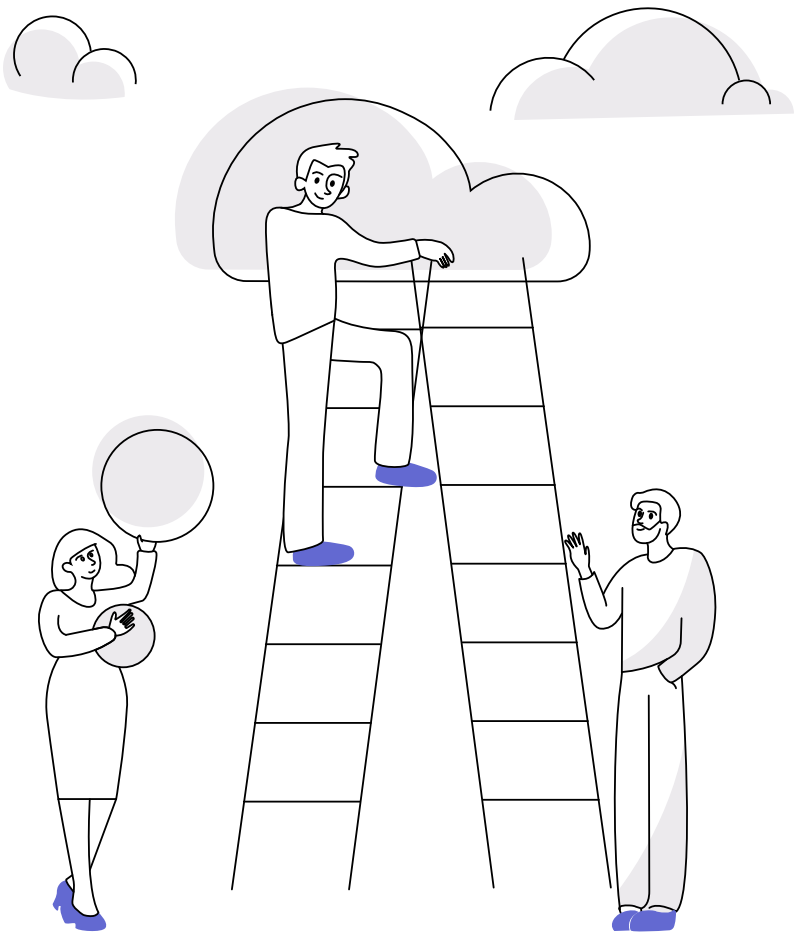
- **Misconfigured Access Controls** – When SaaS apps aren't configured properly – by the IT team or the vendor – it opens the door to cyber-attacks or user-created problems.

- **Adverse Software Updates** – Complex SaaS ecosystems are fragile enough that a software update can disrupt the balance unexpectedly. It may create new vulnerabilities or disable important functions.

- **Service Downtime** – When a problem affects the SaaS service provider – financial collapse, data center disaster, rogue staff, etc. – it causes problems for every subscriber. Mission- critical services that run on SaaS are at risk of being delayed, disrupted, or disabled completely.

- **Insider Threats** – Since SaaS providers have full access to a company's data, someone could potentially misuse that privilege for criminal purposes. Insider threats could also be employees who use unauthorized SaaS apps in defiance of IT protocols.

Any of these could result in a cyber-attack or IT incident that brings a company to its knees. And even when they don't result in complete disaster, SaaS issues can compromise performance and complicate security on a constant basis. Whether or not SaaS proves to be an asset or a liability depends on one thing: the security team.



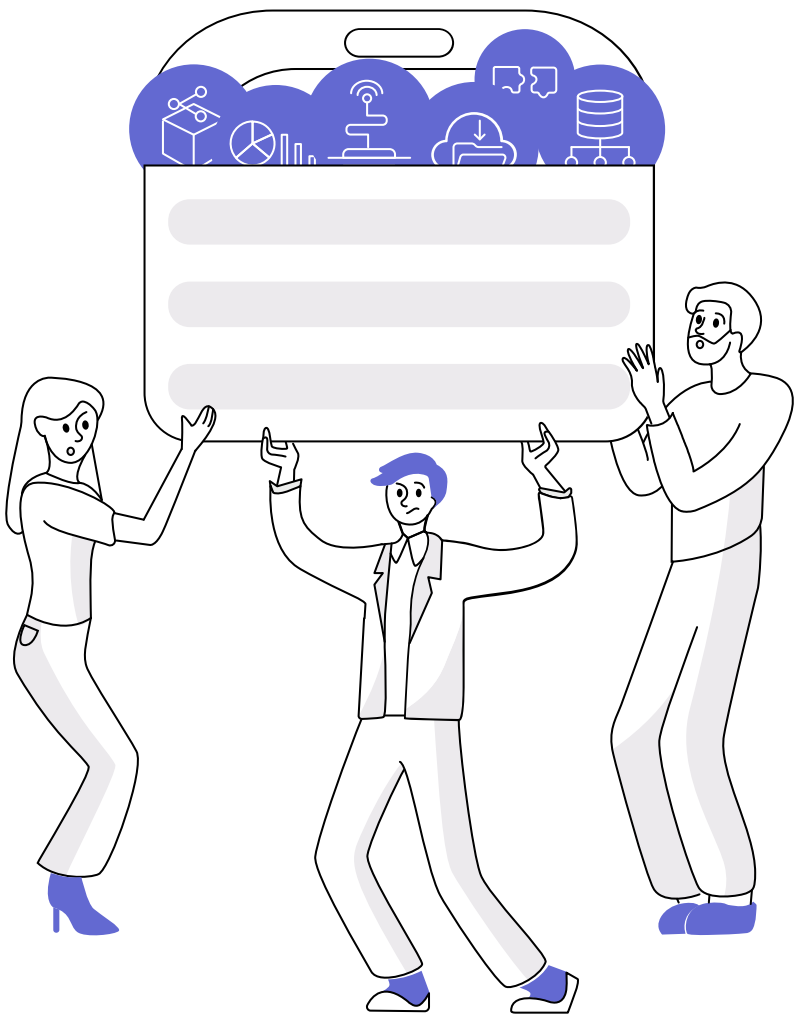
Lean IT Teams and SaaS Risk

SaaS apps were supposed to streamline cybersecurity by shifting obligations from the security team to the service provider. The provider would secure the software and the data within so that companies could benefit from stronger security measures without having to build or manage them internally. This was seen as a boon for all, lean security teams especially. They could “subscribe” to the security they needed.

The reality, however, looks different than advertised. As SaaS apps have come to dominate the tech stack, they have created unexpected security challenges. Security teams must correctly configure and reconfigure controls for hundreds of different apps. They must account for a complex environment consisting of interconnected software and shared data. And they must work within a cloud framework that complicates the meaning of trusted traffic.

It’s no coincidence the rise of SaaS happened in parallel with the escalation of cyber-attacks. Attacks became more sophisticated because they had more vulnerabilities and pathways to exploit. And they became more successful – both in terms of targets reached and damage caused – because SaaS made more assets open to attack. SaaS certainty resolved some security challenges, but the ones it created may be even more problematic.

SaaS risks weigh heavily on lean security teams in particular. As the numbers in the introduction demonstrate, smaller companies still use numerous SaaS apps, but they may not have the security staff, budgets, or defenses to manage the resulting risks. Visibility into what’s happening across the environment suffers with so many SaaS apps in play. So does the ability to identify, address, and recover from threats that only appear on the radar once the damage is done. Managing SaaS risk is a time, labor, and intelligence-intensive effort that, unfortunately, only gets harder as the security team gets smaller.



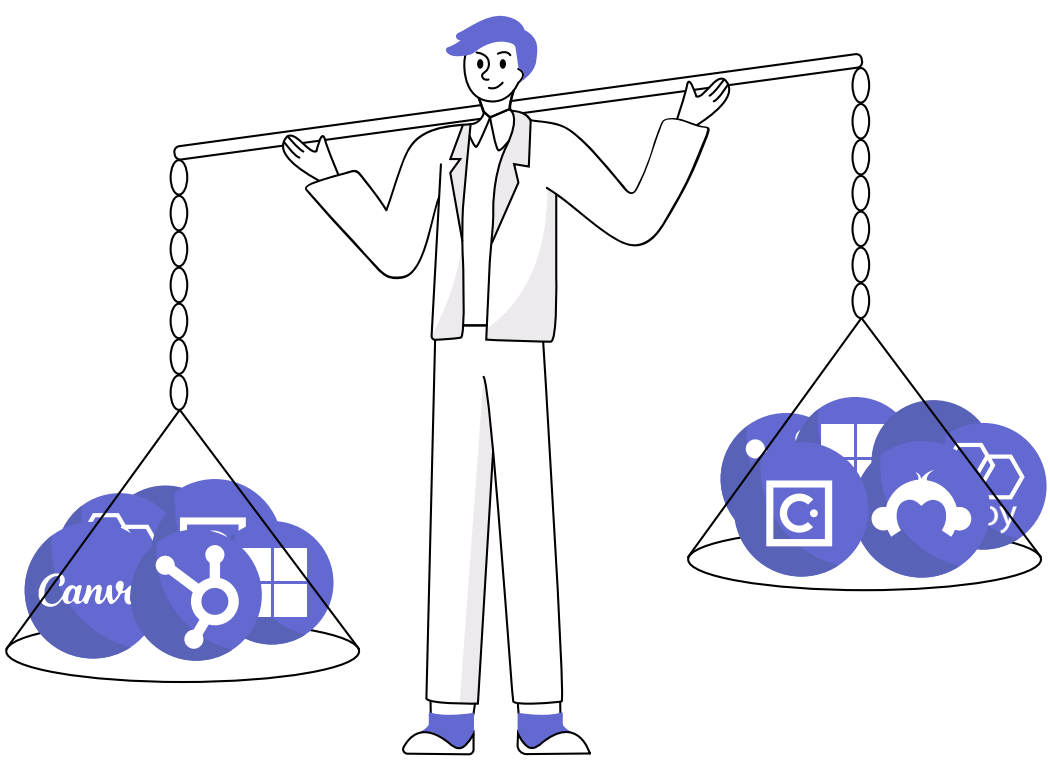
Managing SaaS Risk Starts With Vendors

SaaS risks have less to do with the product itself and more to do with the provider behind it. Since SaaS vendors develop, update, and manage the software – becoming active partners rather than passive providers – they're directly linked to the safety and security of that software. That can be a positive or a negative depending on the provider.

Anytime a security team relinquishes control to a third party, it needs to have complete confidence in that arrangement. For lean security teams, the choice of the right partner can help transcend their limited resources - but the wrong partner will only exacerbate SaaS risks. Therefore, managing those risks requires careful vetting of any SaaS vendor.

Vetting starts by examining the contact language, often with the assistance of legal counsel. The contract will (or should) outline the provider's exact responsibilities in terms of security and availability, along with their liability for failures. Bear in mind that SaaS contracts are typically negotiable, even with major providers like Amazon and Microsoft. Anyone that won't negotiate raises red flags. Some of the specific things to explore/negotiate include:

- Whether the provider abides by all applicable regulations. Companies that operate in Europe need to be particularly concerned about GDPR and must sign a data protection agreement (DPA) with the provider.
- If the subscriber can export data at any time in any industry standard format to enable easy transition from one provider to another.
- What the service-level agreement (SLA) contains. SLAs should be well defined and establish clear penalties for non-compliance. They should also address both availability and utility.
- If the provider allows customers to perform unannounced penetration tests on the product. Providers should also be able to supply third-party penetration test reports to show they're actively looking for security gaps – bug bounties are not a substitute.
- To what extent the provider adheres to and supports appropriate standards. When the provider andsubscriber adhere to the same standards, it streamlines the integration and facilitates automation.
- How proactively the provider informs subscribers about software changes and security incidents. The more transparent the better, but providers should be fast as well as forthcoming. Insist on notification within 48 hours of anything happening.



Getting the Honest Trust About SaaS Providers

Lean security teams can learn a lot about a SaaS vendor's strengths and weaknesses by scrutinizing the contract. That said, contractual terms alone aren't enough to evaluate a vendor's commitment to security and ability to manage threats. Quality vendors are aware of this fact and go to greater lengths to establish their security credentials. Depending on the circumstance, SaaS providers should participate in one or more of the following programs.

SOC-2 Audits

Preparing for the next attack, whatever form it takes, involves creating an organizational security policy, conducting a risk assessment, cataloging sensitive assets, and ranking security threats. It's especially important to recruit an incident response team and get them ready for action.

ISO 27001 Audits

ISO 27001 is a set of internationally accepted standards for governing information assets, with a heavy emphasis on security and risk management. An ISO 27001 audit assesses whether a SaaS provider architects a product securely and operates it reliably. A company can fail one of these audits, but they can also avoid failing by defining narrow audit parameters that omit vulnerabilities. Once again, a closer look at the audit details is in order.

CSA Star

Cloud Security Alliance (CSA) STAR certification is considered the industry standard for SaaS security. With Level-Once certification, a provider undergoes a self-assessment of their security and compliance controls and publishes the results in an online registry. This registry can be a valuable resource, unless the sales and marketing team embellished the self-assessment. Level-Two certification involves a third-party audit, which SaaS providers can also use to attest to SOC-2 or ISO 27001 compliance.

OWASP Verification Standard

The OWASP verification standard provides guidance and standards for the development of secure web applications. It seeks to standardize practices and turn application security into a measurable metric. All reputable developers will follow this standard, and the SaaS contract should make it mandatory.

Third Parties

Third party evaluators can audit specific SaaS providers and products to fully-assess their underlying security. These audits can be helpful, and companies should include the right to audit in the contract, but it's important to choose the right evaluator. Some use high-pressure tactics or reach dubious conclusions that call the audit into question.

Emerging Solutions for SaaS Excellence

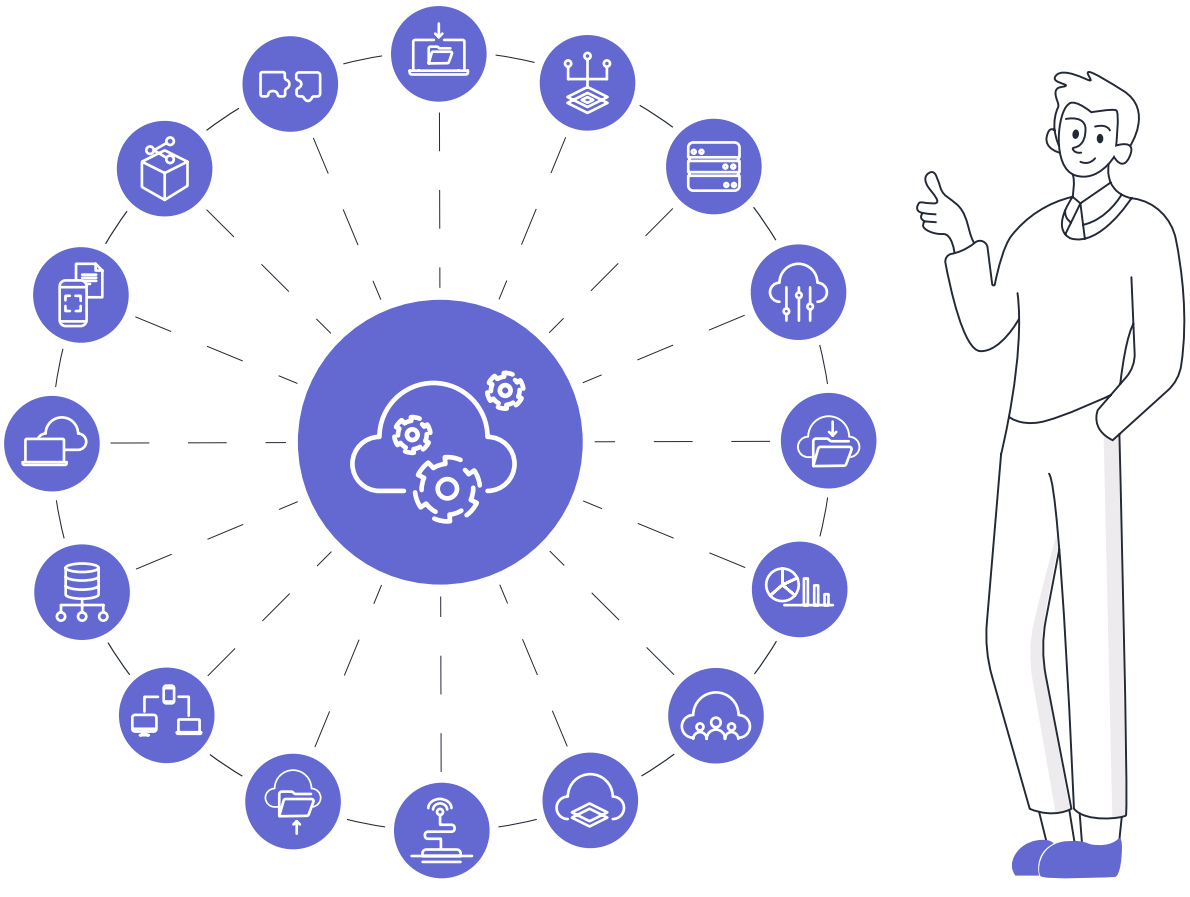
Security teams can only spend so much time vetting vendors, especially when even the largest SaaS offerings struggle with security issues. Furthermore, security teams can't rely on vendors alone to handle SaaS security; it's an internal effort as well. To help teams, lean or otherwise, manage all the SaaS apps in their orbit, various platforms for SaaS management have emerged onto the market.

SaaS Management Platforms (SMPs)

With an increasing number of SaaS apps in action, security teams need a better way to track these apps individually and collectively. SMPs combine multiple capabilities: app discovery, administrative automation, centralized security management, usage and cost analysis, and more. Companies need this kind of top-down view on SaaS sprawl, but what that encompasses varies by platform. True SMPs deliver the three pillars of centralized administration, automation, and discovery – anything less isn't adequate. However, even true SMPs can only do so much to reduce SaaS risks. The enhanced visibility SMPs provide helps a security team accelerate time to response and reduce event frequency. But in order to significantly reduce risks, teams need to prevent incidents in the first place, which SMPs struggle to do. Still, SMPs are a valuable investment for enhanced visibility alone.

SaaS Security Posture Management (SSPM)

Cloud misconfigurations were found in 93% of the deployments studied and blamed for nearly 20% of all data breaches. They're also increasing as SaaS apps proliferate. SSPMs provide a centralized management platform for all SaaS configurations that security teams can use to keep apps properly configured even as the various vendor platforms undergo successive changes. Using a SSPM tool, risk of a breach related to misconfiguration drops dramatically. So does the risk of noncompliance with industry standards like HIPAA or CIS CSC because centralized management enables consistent policy enforcement. SOC-2 reporting improves as well. By minimizing a primary cause of SaaS incidents (misconfigurations), SSPMs reduce the frequency and magnitude of loss – otherwise known as risk.

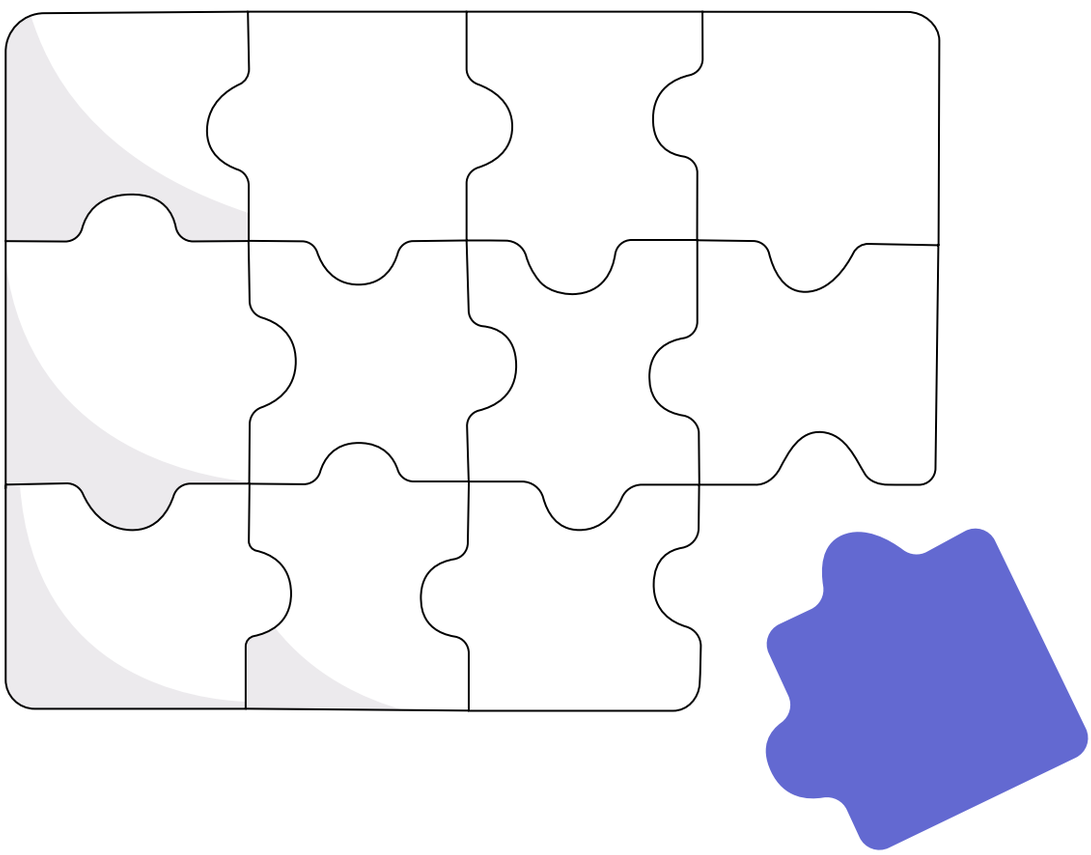


SaaS Risk in the Broader Context of Cybersecurity

Significant as SaaS risks may be, they're just one of many responsibilities confronting today's security teams. Attackers can choose SaaS as their target or choose from countless others. The challenge facing every security team is managing SaaS risks alongside network security, endpoint protection, threat remediation and everything else that demands their attention and resources. It takes a careful balancing act. Most of all, it requires seeing SaaS risk as just one facet of a comprehensive cybersecurity strategy.

Carefully vetting vendors, negotiating service contracts, and leveraging SaaS management platforms are all necessary steps. That said, preventing SaaS risks from becoming either an inevitable disaster or an unmanageable obligation takes a new approach to cybersecurity entirely.

Integration and automation are key to that approach. Modern security teams of any size need a suite of defensive technologies (NGAV, EDR, NDR, UEBA, and others) to ward off all threats. Integrating those technologies creates a sum greater than its parts, enhancing visibility and extending security controls into all corners of the environment. Following integration, cumbersome obligations can be automated so the security team only gets involved when their input is essential. That leaves teams with more time to focus on SaaS risks (along with all others) and more tools to remediate those risks.



Cynet – On the Cutting Edge of SaaS Security

Cynet offers a complete solution for SaaS security. Cynet's innovative SSPM tool gives lean security teams total visibility into the SaaS environment along with complete control over the configurations it runs on. When SaaS misconfigurations are discovered, suggested changes are offered which can be automatically implemented in the SaaS app with a single click. SSPM is fully integrated into the Cynet dashboard so security analysts don't have to access yet another siloed security tool.

Cynet has also created the world's first autonomous breach protection platform, which natively unifies mission-critical defenses and puts their key features on autopilot. SaaS risk may be inevitable, but now it's manageable – with solutions and strategies from Cynet.

Learn More