AppOmni

2025 Report

The State of SaaS Security

with UserEvidence

Table of *Contents*

Foreword

We're proud to share AppOmni's third annual *The State of SaaS Security Report*. SaaS continues its enterprise transformation with a **projected** compounded annual growth rate of 20% between 2025 to 2032. The stakes for securing these platforms have never been higher. Today, nearly every organization relies on SaaS to operate, and attackers know it.

In the past year, SaaS security, together with concerns around the secure use of AI, has moved from a niche security initiative to a boardroom imperative. In its 2024 letter, **JPMorgan's CISO, Pat Opet,** explicitly named SaaS vulnerabilities as an area of utmost importance, noting the industry's increasing dependence on third-party providers and the growing threat of SaaS attacks. The **2025 Verizon Data Breach Investigations Report (DBIR)** called out a doubling of breaches involving third-party applications stemming from misconfigured SaaS platforms and unauthorized integrations, particularly those exploited by threat actors through scanning and credential stuffing.

SaaS is now one of the most actively targeted layers of the enterprise attack surface, and yet, it remains one of the least proactively defended. Adversary activity in SaaS apps prompted the government's watchdog—the Cybersecurity and Infrastructure Security Agency (CISA)—to issue a Binding Directive (BOD 25-01) to public sector agencies to secure their critical SaaS environments and urge the private sector to do the same.

At AppOmni, we see this play out every day. Our SaaS threat research team has published **multiple investigations** this past year alone, exposing critical misconfigurations and vulnerabilities across major SaaS platforms like Salesforce, ServiceNow, NetSuite, and Microsoft 365. These aren't theoretical risks—they're real-world exposures impacting the biggest brands in the world.

This year's State of SaaS Security report is based on insights from over 800 global security leaders. Their responses reveal a troubling disconnect: 91% of respondents express confidence in their SaaS security posture, yet 75% experienced a security incident in the past year—many involving the very issues our team and other industry experts have warned about. 89% of those impacted by incidents or breaches believed they had "appropriate visibility" into their environments at the time.

This is the illusion of control, and it's one of the most dangerous challenges facing security teams today. People are busy. Teams rely on dashboards and implicitly trust platform vendors. But visibility alone is not security. And trust without verification is not a strategy.

What we need now is clarity. SaaS security must evolve from an ad hoc, reactive process to a mature, repeatable discipline. That means embracing continuous monitoring over point-in-time audits, assigning clear ownership, and protecting the entire ecosystem, including users, configurations, and app-to-app connections alike.

This report is both a snapshot of where the industry stands and a call to action. **The attacks are already here. The question is: Are you ready?**

Brendan O'Connor

CEO & Co-Founder, AppOmni

Executive *Summary*

As organizations scale their use of cloud applications, they're also expanding their attack surface. The State of SaaS Security 2025 Report reveals a sharp increase in SaaS security incidents, a rising complexity in app ecosystems, and a persistent disconnect between perceived visibility and actual risk reduction.

As SaaS adoption accelerates, so too does the urgency for security teams to close the gap between visibility and actual control. This report set out to understand the realities behind that gap—and to challenge assumptions about maturity, confidence, and level of control.

This report investigates:

- **Are security teams keeping pace with the rising complexity and interconnectivity of SaaS ecosystems?** We examined how organizations are managing risks from user permissions, app misconfigurations, and SaaS-to-SaaS connections—including how these risks are (or aren't) being prioritized.

- **What does "confidence" in SaaS security really mean, and is it justified?** With 91% of organizations reporting confidence in their SaaS security but 75% experiencing an incident, we investigated the source of that confidence and whether it reflects real-world resilience or a false sense of security.

- **How are organizations operationalizing SaaS security—or failing to?** We looked at whether visibility translates into enforcement, what tools and teams are actually being used, and how responsibility is shared across business and security functions.

- **Is the security mindset evolving fast enough to meet the moment?** While 96% say SaaS security is becoming more important, we tested whether that urgency is translating into more mature, continuous practices, or if legacy habits like point-in-time audits still dominate.

- **How are organizations responding to emerging challenges like AI governance and regulatory scrutiny?** We assessed how teams are preparing for the next wave of SaaS risks, including AI oversight, identity sprawl, and tightening regulations around SaaS oversight.

Our findings point to a simple yet powerful truth: SaaS security doesn't have to be complex, but strategies do need to adapt to meet the increased threats. With the right tools and clear ownership, organizations can transform reactive processes into scalable, repeatable programs. This report outlines a framework to simplify and operationalize SaaS security, turning complexity into clarity and risk into resilience. Now is the time for action.

Key *Findings*

75%

SaaS Under Siege: 75% of organizations experienced a SaaS-related security incident in the past year, a 33% increase over 2024. This sharp rise underscores increased threats to the SaaS layer.

91%

The Security Mirage: 91% of organizations express confidence in their SaaS security posture, yet 75% experienced a SaaS incident. The gap between belief and outcomes reveals a serious disconnect.

89%

Visibility ≠ Security: 89% of compromised organizations believed they had "appropriate visibility" into their SaaS environment, proving that visibility without enforcement or continuous validation creates a false sense of security.

52%

Old Strategies, New Threats: 52% continue to use periodic reviews to assess SaaS risk, despite the highly dynamic nature of SaaS environments. This approach leaves gaps where misconfigurations and threats can persist undetected.

43%

SaaS Risks Don't Wait for Audits: Only 43% have implemented continuous or near real-time oversight, leaving most organizations vulnerable to drift, app sprawl, and subtle configuration failures between audits.

53%

Hope Isn't a Security Strategy: 53% of confident respondents base their security posture on trust in SaaS vendors, rather than internal validation, highlighting a dangerous misunderstanding of the shared responsibility model.

16%

Everyone's Job = No One's Job: Only 16% assign SaaS security solely to security teams, while 43% leave it to business units. This fragmented model leads to unclear accountability and uneven coverage.

41%

Breached by Basics: 41% of incidents stemmed from permission issues, while 29% resulted from misconfigurations.

13%

Securing SaaS with Duct Tape: Just 13% of respondents currently use a dedicated SaaS Security Posture Management (SSPM) solution, even though nearly one-third say they need one.

61%

Can We Govern AI or Will It Govern Us?: 61% of respondents expect AI to dominate SaaS security discussions in the coming year, demanding better oversight of non-human identities and generative AI tool access within SaaS apps.

Section

01

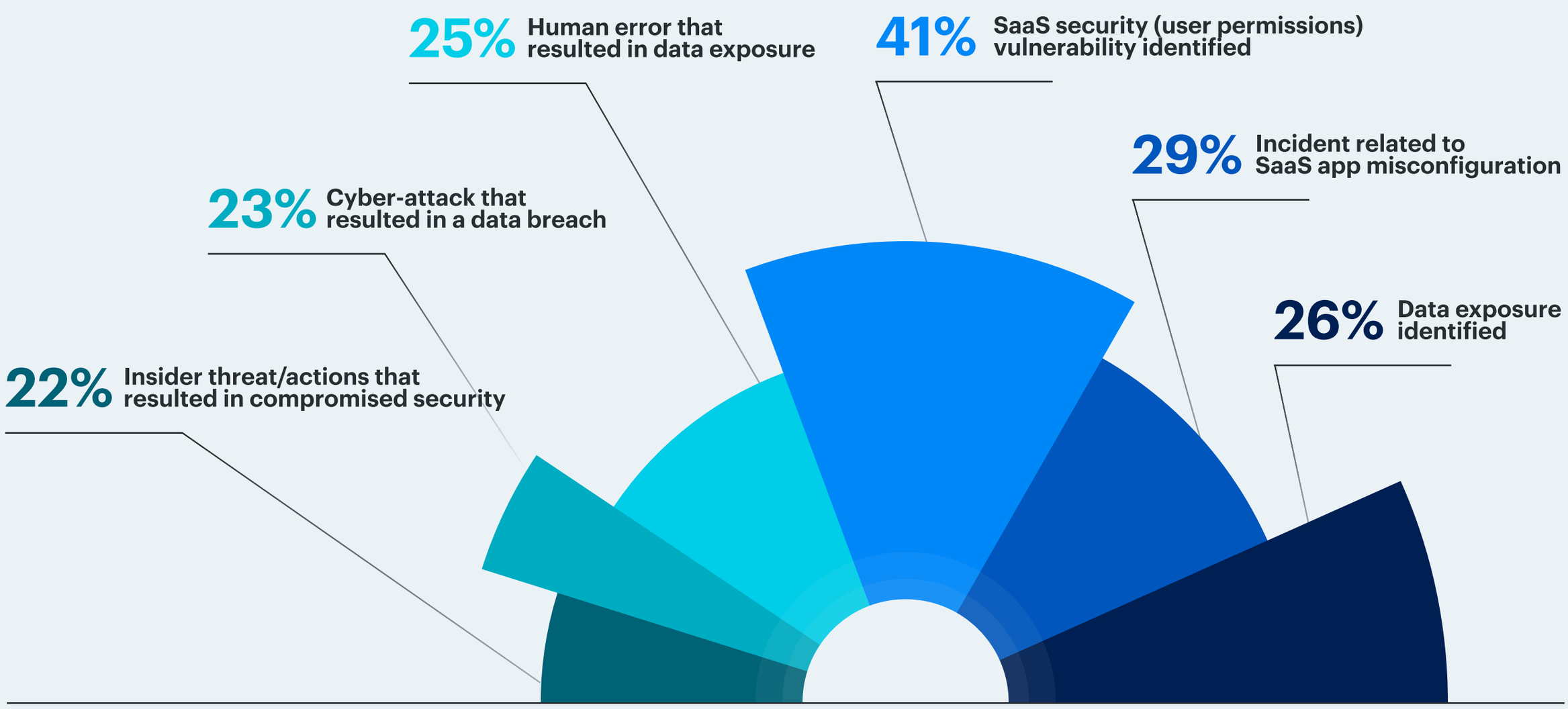
The SaaS Surge:
Growing Usage But Rising Security Incidents

Incidents

Over the last year, data reveals significant SaaS security concerns. Specifically, 41% of those surveyed identified vulnerabilities in SaaS user permissions, while 29% reported incidents stemming from SaaS application misconfigurations. Further security findings include 26% of respondents encountering data exposure and 25% where human error led to data exposure.

Our data shows that 75% of respondents have experienced a SaaS security incident or data breach in the past 12 months. This is a substantial 33% increase compared to The State of SaaS Security 2024 Report.

SaaS security incidents or data breaches experienced in the past 12 months



Section

01

Concerns

Data security remains a paramount concern. A majority of respondents, at 57%, cited data breaches and the potential loss of intellectual property as their primary worry. Over a third (37%) expressed considerable apprehension about compromised customer data. More than a quarter (28%) highlighted their unease regarding the consequences of unintentional data exposure.

7% expressed concern about unintended input of data to AI / LLM based apps.

What are your top concerns around the security of SaaS applications?

57%
Data breaches / loss of Intellectual Property

28%
Unintended data exposure

24%
Configurations that deviate from intended policies over time

37%
Customer data being compromised

7%
Unintended input of data to AI / LLM based apps

Section

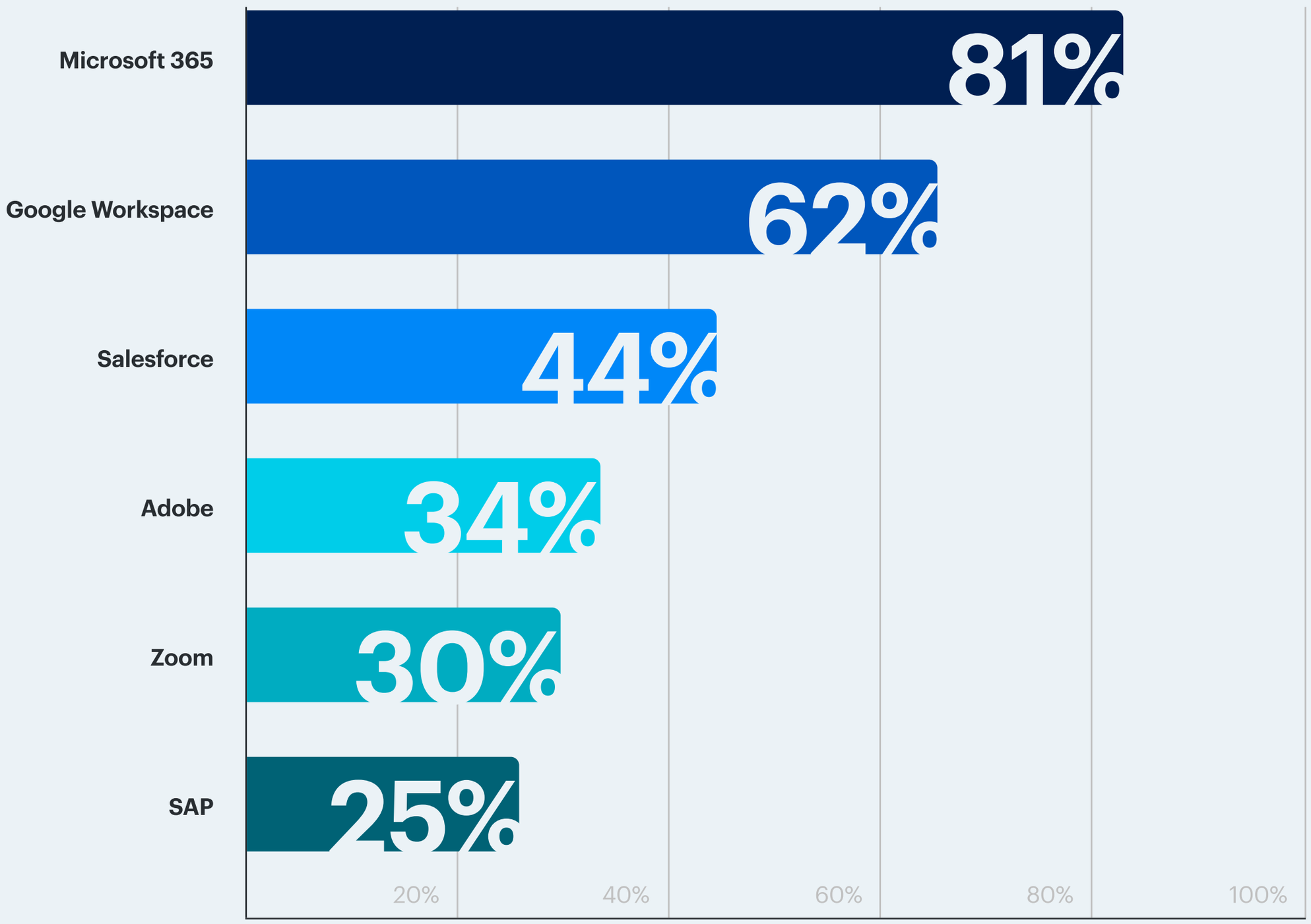
01

Deployed SaaS Applications

Most organizations are using dozens or even hundreds of SaaS applications. Over half (57%) of respondents say they're aware of 50 or more SaaS apps deployed in their organization's environment. Over a third (40%) report 100 or more apps. Since these totals only include the apps that respondents know about, the actual numbers (including **shadow SaaS**) may be higher.

The vast majority of organizations express strong assurances regarding the security of sanctioned SaaS apps. 88% rate their security level at least a four on a five-point scale, and 36% report the highest level of confidence (five on a five-point scale) in their sanctioned SaaS apps.

Most heavily used SaaS apps across your organization



> *Our biggest headache with SaaS security is the sheer [volume] of apps and the consistent changes in permission and configurations [...] What we really need is a smart automated tool that gives us a clear real-time view of our entire SaaS landscape.*
>
> **— IT Manager/Director/VP, Manufacturing & Production**

Section

02

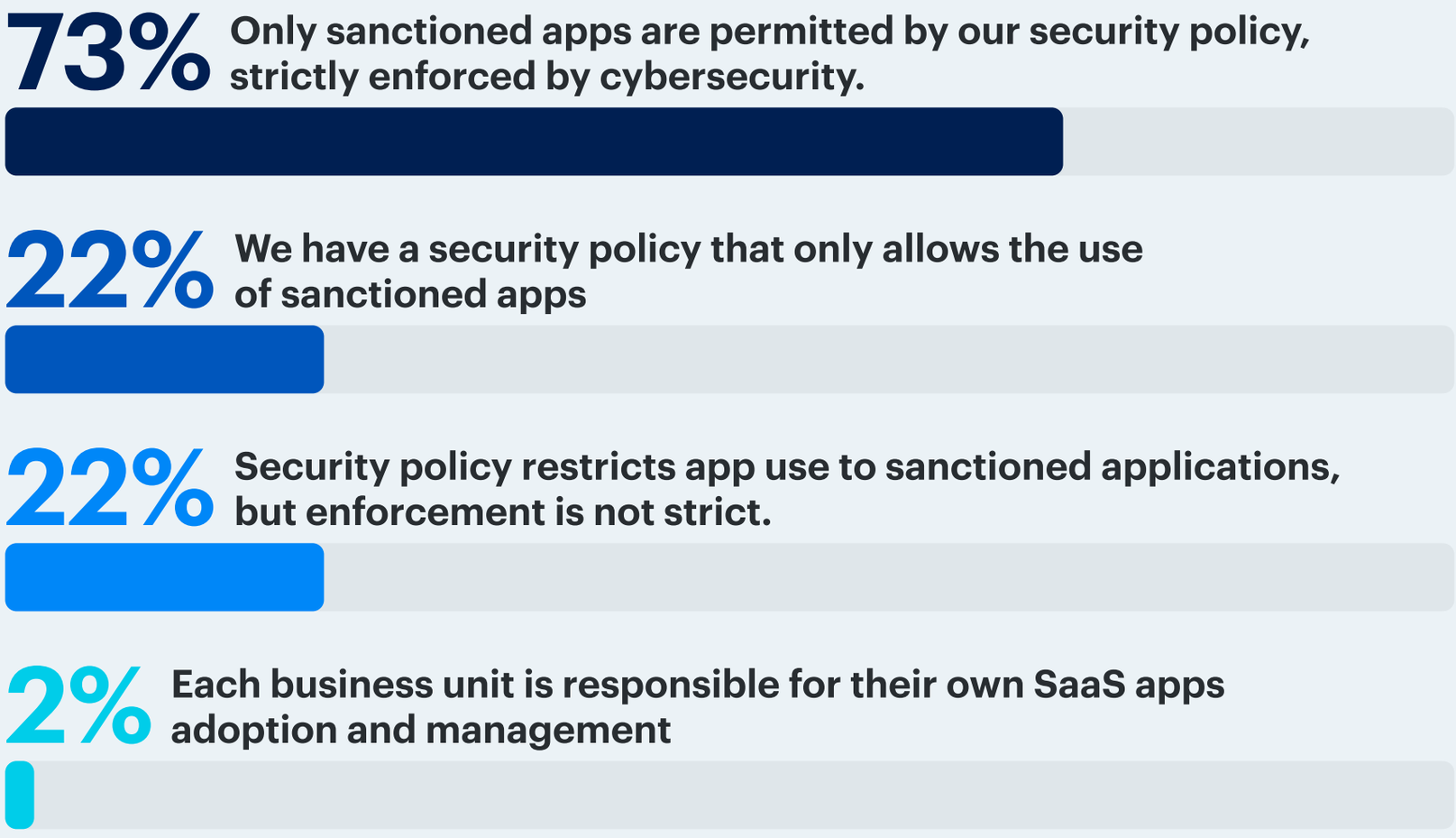
Sanctioned ≠ Secure:
The Illusion of Oversight in SaaS Environments

Nearly three-quarters of respondents report having a policy that only permits the use of sanctioned SaaS applications, and that policy is "strictly controlled by the cybersecurity team." This suggests that the most common approach is a top-down model, in which a centralized cybersecurity function approves and enforces which SaaS apps (and extensions) may be used.

A sizable minority (one in five or 22%) have a policy but lack strict enforcement. These organizations have the right policy on paper, yet enforcement (e.g., blocking unapproved apps, monitoring usage, revoking access) is inconsistent or largely advisory rather than mandatory. This appears to be an improvement compared to The State of SaaS Security 2024 Report, which found that 34% believed their organization didn't strictly enforce security policies for sanctioned apps.

A small fraction leaves SaaS decisions to individual business units. This implies that decentralized ownership of SaaS risk is rare.

Policies and Controls in Place for App Adoption



To detect and monitor third-party apps connected to corporate SaaS environments, two-thirds of respondents (63%) indicated use of dedicated security tooling or log-analysis processes, such as SSPM, SSE/CASB, and SIEMified logs. This suggests that a majority rely on automated or semi-automated mechanisms rather than purely manual oversight. This could mean the use of scripts, tools, or platforms to handle security tasks with little to no human involvement (e.g. Vulnerability scanning that runs on a schedule or playbooks in security orchestration tools like SOAR that execute predefined steps but pause for human confirmation).

17% still manually review app connections. In an environment where integrations can proliferate rapidly, this high percentage of human inspection may indicate potential resource strain. Policy-only enforcement (10%) is the least common single approach.

Section

02

Security Levels of Sanctioned & Unsanctioned SaaS

Respondents show high confidence in the security of their sanctioned SaaS apps: 88% assign at least a four on a five-point scale and over a third (36%) assign the highest security rating (level 5). This strong perception of security stems from factors such as trust in the SaaS provider, routine app audits for industry standard compliance, thorough visibility into apps, and guaranteed secure deployment configurations.

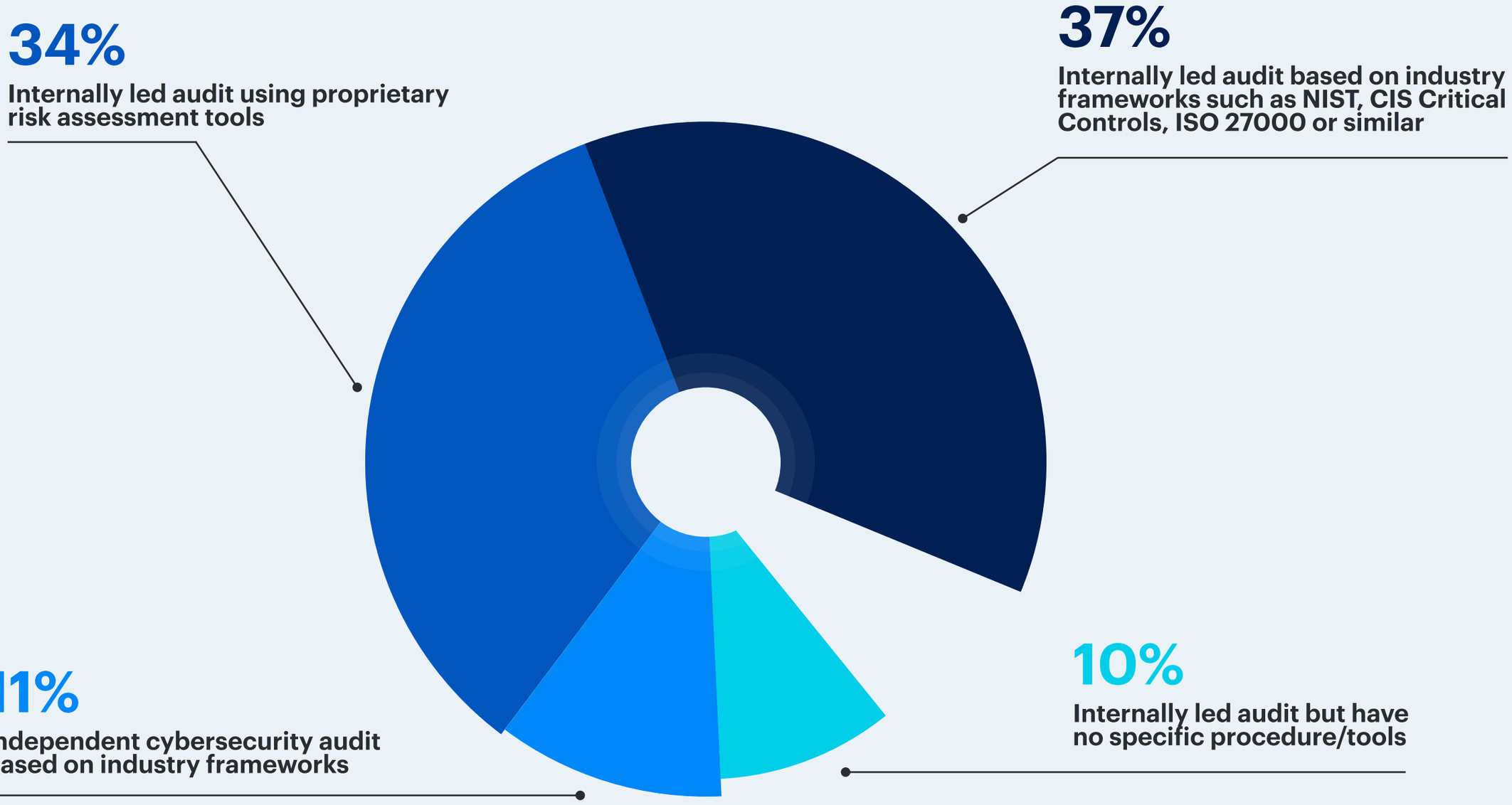
Unsanctioned app deployments persist even with strict enforcement. This often stems from lengthy approval procedures (29%). Lack of employee awareness (19%) and the need for apps addressing unsupported use cases (16%) further contribute to this trend.

Onboarding New SaaS Apps & Evaluating Risks

When adopting a new SaaS app, the majority (82%) rely on internally led audits to evaluate risks. To lead these assessments, 37% use industry frameworks, while 34% use proprietary risk assessment tools. Evaluating security risks during SaaS app onboarding lacks a universal, standardized approach. Each organization may develop their own unique operational protocols for this process.

However, 10% of respondents lack both a specific procedure and a dedicated tool for these internal audits. While this segment is relatively small, it could become susceptible to significant security gaps without a consistent workflow or continuous monitoring.

SaaS App Risk Evaluation Strategies



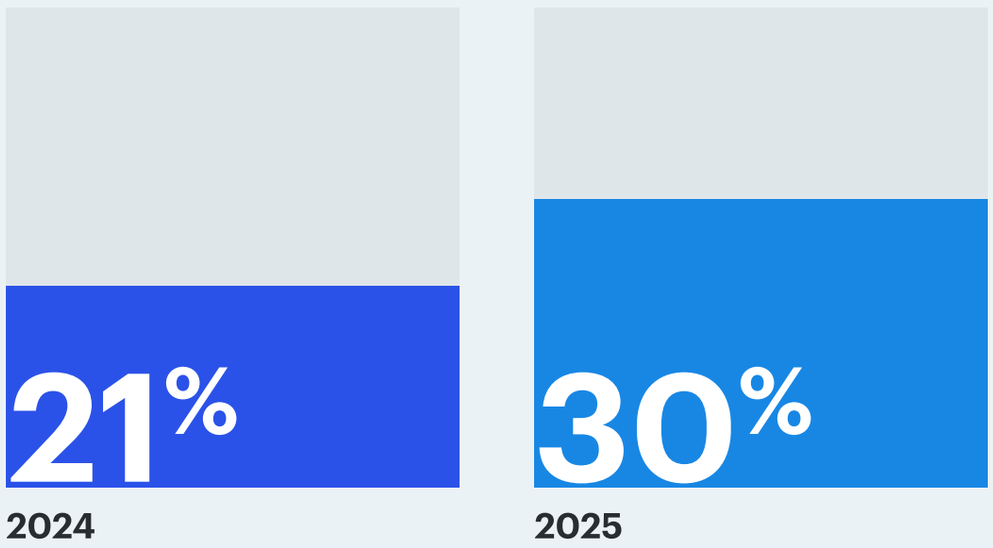
Section

02

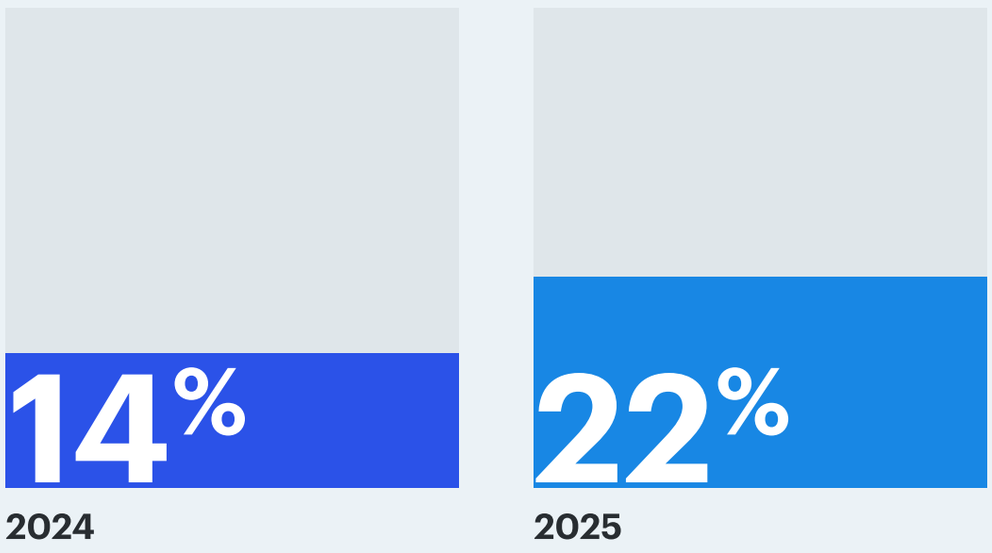
For continuous monitoring of third-party SaaS applications and compliance with industry- and region-specific regulations (such as GDPR, HIPAA, CCPA, and APPI), 43% use a SaaS security posture management (SSPM) suite.

SaaS Security Compliance Approaches

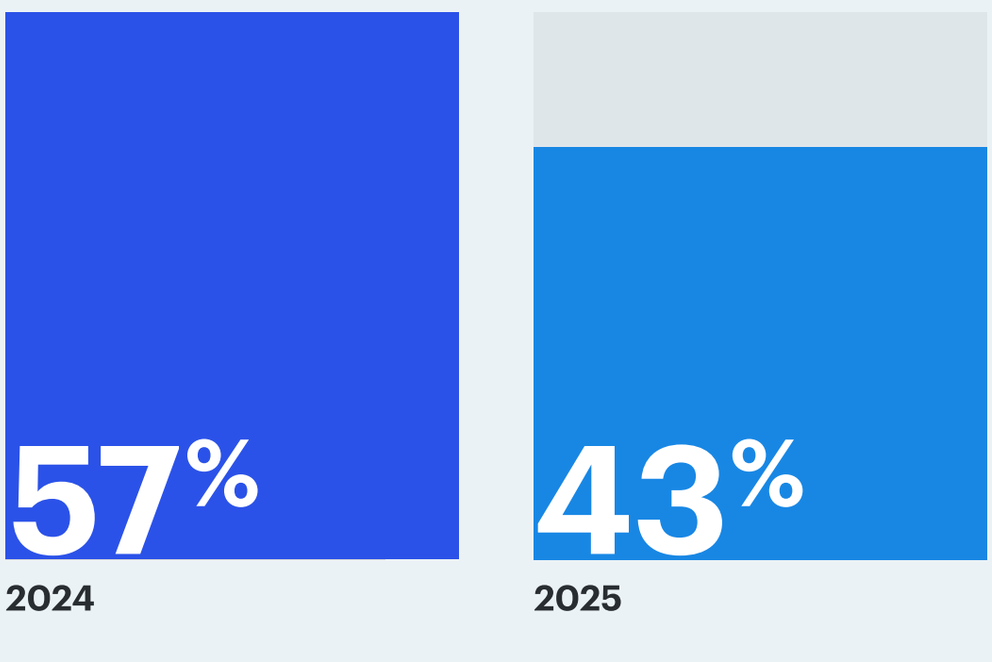
Manual SaaS compliance audits carried out on a regular basis



Manual SaaS compliance audits carried out on an ad-hoc basis



Continuous SaaS compliance assessment and reporting via a SSPM tool



Section

03

The SaaS Security Org. Chart:
Who Owns What

Most organizations in the survey demonstrate a clear commitment to specialized cybersecurity functions. Nearly two-thirds (65%) maintain a dedicated Cloud Security Team, and over half (55%) have a SaaS Security Team. Core defensive functions such as Network Security (50%) and Compliance (45%) are also widely staffed. Mid-tier specialist areas, notably Identity & Access Management, Threat Intelligence, and Third-Party Risk, each appear in roughly 27–30% of respondents, indicating growing but not universal investment.

Although business and compliance roles like Legal/Compliance Director are present, they appear less frequently. Specialized cybersecurity practitioners such as DevSecOps, Incident Response, Product Security, and Data Security have limited representation.

Fewer than one-quarter of organizations have standalone Incident Response (22%), Application Security (20%), or Endpoint Security (19%) teams. Only 4% manage cybersecurity purely within general IT, and almost no one (0.4%) operates without any dedicated specialist teams.

85% noted they are the final decision maker when it comes to selecting IT security / cybersecurity solutions for their organization.

Which of the following specialist cybersecurity teams exist in your company/organization?

Section

03

Are mid-market orgs more likely to lack incident response teams? Do enterprises rely more on orchestration and rules engines or have different spending priorities?

Enterprise vs. Mid-Market

Overall, mid-market organizations account for roughly three-quarters of all dedicated cybersecurity teams, especially foundational functions like Cloud Security (72% mid-market) and SaaS Security (74%). Enterprise firms, by contrast, represent a larger share of certain advanced and operational roles: for example, 37% of Incident Response teams and 36% of Application Security teams reside in enterprises, compared with 28–30% for broad compliance or advisory functions.

This suggests that larger organizations invest proportionally more in mature, reactive capabilities—such as incident response and secure development—while mid-market companies focus relatively more on preventive and advisory roles like cloud, network, and compliance security. Note: Since some specialist teams (for example, those with an Application Security team) had limited responses, these proportions are broad indicators.

Shared Responsibilities

Should ownership be everyone's problem, or should a specific team be in charge?

Strong executive support doesn’t always translate to clearly defined stakeholders, which may mean no one truly takes ownership.

The SaaS platform owner shares security responsibilities most heavily with the SaaS Security Team (60%), Cloud Security Team (47%), and Cybersecurity Compliance Team (33%), highlighting a focus on application-layer security, cloud infrastructure, and regulatory adherence. The SaaS Security Team likely functions within the purview of a security leader such as an IT Manager.

Significant involvement from the Security Operations Centre (32%) and Network Security Team (31%) points to a strong emphasis on threat detection and network-layer defenses. Identity and Access Management (22%) also plays a key role, reflecting the need for robust access controls.

Section

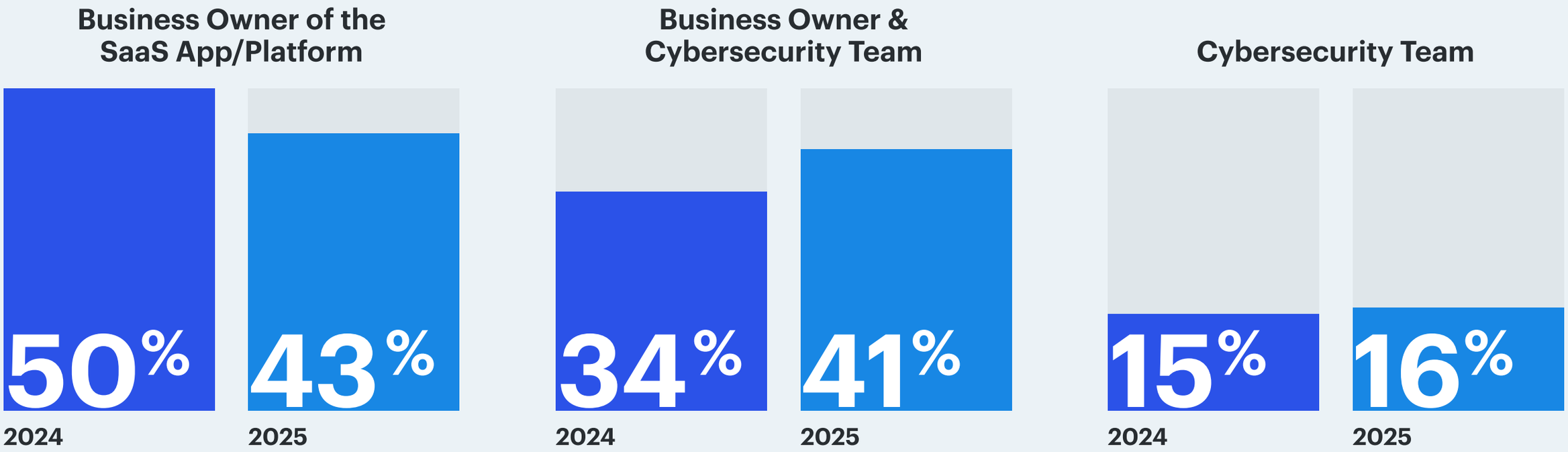
03

Other teams, like Data Security, Cyber Risk, Application Security, and Policy, support operational and strategic areas, while lower involvement from incident response, endpoint security, and audit suggests more specialized or reactive engagement. Overall, the SaaS owner's responsibilities span a broad spectrum, with the heaviest collaboration required across cloud, SaaS, and compliance teams.

When it comes to security responsibility, many organizations take a decentralized approach to SaaS security. 43% of respondents say that within their organization, the business owner of the SaaS app takes full responsibility, while 41% report that the cybersecurity team and the business owner share responsibility.

> *"We've adopted this tagline that many have: cybersecurity is a shared responsibility. If somebody sees something, they say something. We reward them with a cybersecurity challenge coin. We've gamified it in that way.*
>
> **Dennis Tomlin**
> Chief Information Security Officer, Multnomah County

SaaS Cybersecurity Responsibility Ownership



This data shows that SaaS security ownership continues the trend of decentralized responsibility increasing by 7 points compared to 2024. While this divided approach increases the total number of responsible stakeholders, it also tends to decrease the perception of ownership. This can lower stakeholder urgency, potentially leading to inconsistent practices and security gaps.

Section

03

> *The real game-changer I've seen? When security teams stop talking tech and start speaking business. Too often we march in with these massive vulnerability lists: 'Here's 200 things to fix!' without explaining which ones actually matter to their goals. It's no wonder we get pushback.*
>
> *What works? Roll up your sleeves first. Really understand how teams use their SaaS apps day-to-day. When you can say, 'Hey, I see this Salesforce setting could expose customer data during your big quarterly push. Let's fix it in a way that won't slow you down,' suddenly you're not the security cop anymore. You're the enabler who gets it.*
>
> *That's the shift — from handing down edicts to solving problems together.*
>
> **Vishal Chawla**
> **CEO & Founder, BluOcean Cyber**

When it comes to the cybersecurity teams who have the responsibility of securing SaaS platforms, many have established specialist cybersecurity teams to oversee SaaS security. Nearly two-thirds (65%) report having a cloud security team, while about half have a SaaS security team (55%) or a cybersecurity compliance team (45%).

These specialized teams are well-equipped to manage SaaS security, from ensuring data security to evaluating new apps. However, the data shows that these specialized teams are more likely to be involved in collaborative ownership models than they are to hold exclusive responsibility.

The responsibility for SaaS security differs widely from one organization to another. This lack of uniformity could suggest that many organizations haven't adequately prioritized or resourced SaaS security. But this also could indicate innovation. It could reflect the creative ways organizations structure SaaS security ownership, especially as they recognize the critical nature of the challenge.

The cybersecurity compliance team is the main stakeholder in 37% of organizations. Traditional security teams take ownership more often. Responsibility rests on the SOC team in 47% of organizations, and in 40%, the network security team has ownership.

When SaaS security responsibility is divided, the business owner is more likely to coordinate with specialized teams. Most often, the stakeholder collaborates with the SaaS security team (60%), the cloud security team (47%), or the cybersecurity compliance team (33%).

While this decentralized approach requires cross-functional collaboration, most organizations claim that they maintain strategic alignment for SaaS security. Within most organizations (82%), SaaS security strategy is an integrated part of the cybersecurity strategy and incident response plan.

Section

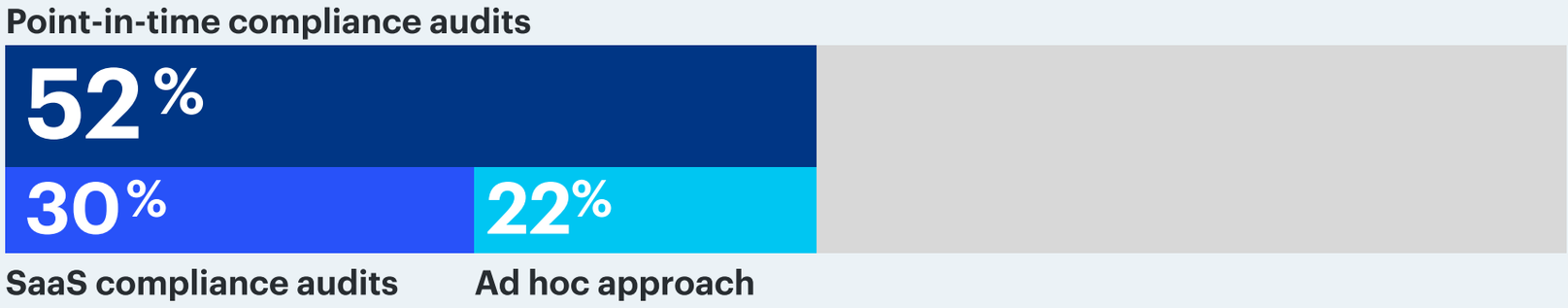
04

Good Enough or Just Lucky?

The Cost of SaaS Security Tradeoffs

How often are you auditing SaaS application security? Do you have continuous SaaS application monitoring in between your audits?

More than half (52%) rely on point-in-time compliance audits: 30% conduct SaaS compliance audits on a regular basis, while 22% use an ad hoc approach.

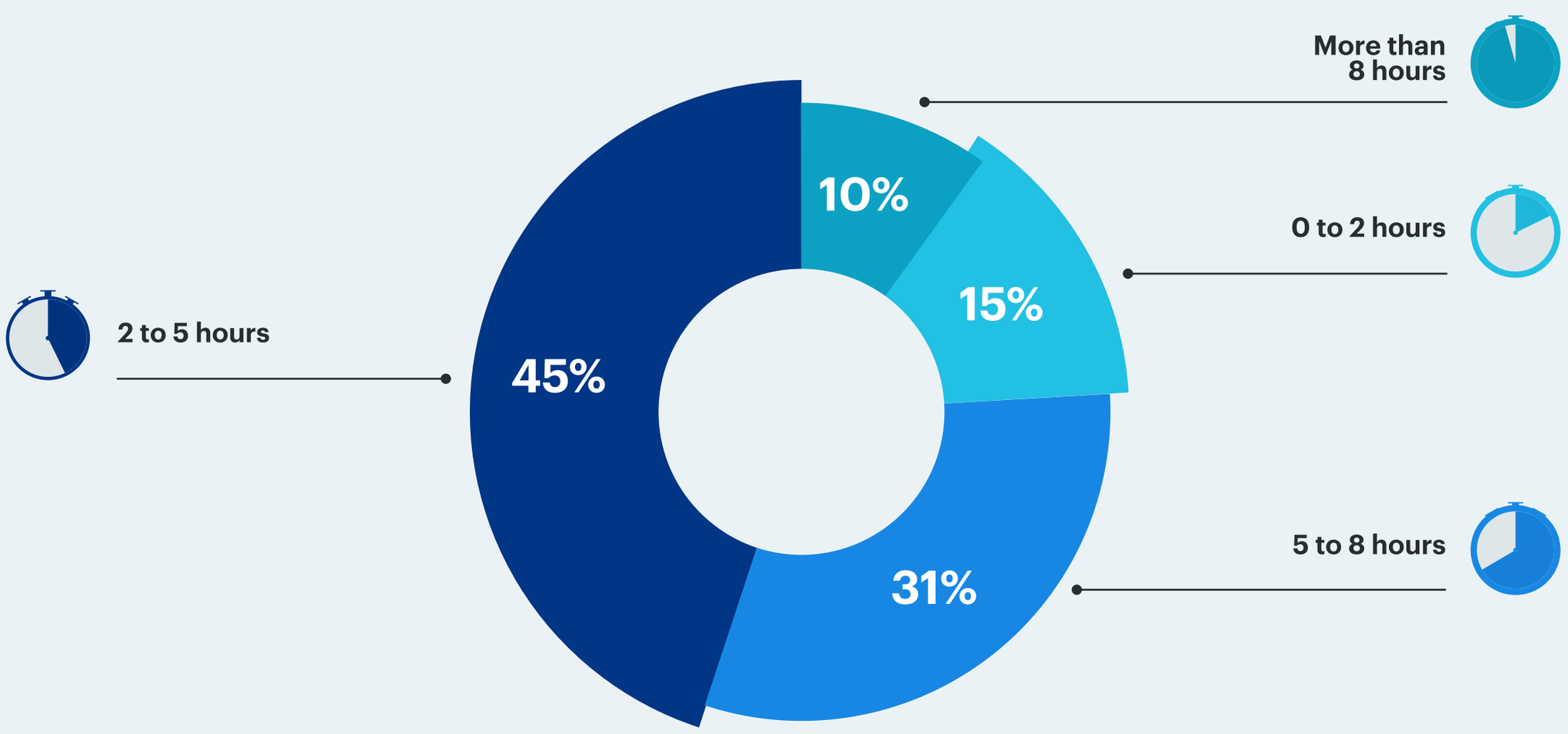


While quarterly or pre-deployment audits may seem sufficient, they tend to leave large gaps in visibility since SaaS apps are dynamic environments where configurations can change rapidly and user changes and feature upgrades occur almost every day. Even frequent periodic checks can create risk. As organizations continue to deploy SaaS apps, grapple with AI usage, and navigate an **uptick in cybersecurity incidents,** it's increasingly important to adopt a solution that provides sufficient monitoring and addresses risk in between audits.

Performing point-in-time compliance audits can also be time-consuming. The data shows that security admins already spend significant time reviewing SaaS security risks, detecting threats, and mitigating issues. 41% spend five or more hours on these tasks each week, while 10% dedicate more than one typical workday (eight hours) every week.

The bottom line: Periodic audits aren't enough anymore, and continuous monitoring is essential.

Time spent per week reviewing SaaS security risks, findings, detecting threats, and mitigating issues



Section

04

> *“Security improvements are easier to measure than ROI — ROI is difficult to measure when it comes to these types of tools. But if by improving your security posture, identifying vulnerabilities, being quick to patch vulnerabilities, you reduce your risk significantly. And if the investment in a tool is significantly less than the recovery from a bad day in the event of a breach or any type of incident — a simple incident can take up to six or seven combined people hours to resolve even if it's a benign incident.”*
>
> **Dennis Tomlin**
> Chief Information Security Officer, Multnomah County

Tooling Consolidation vs. Specialization

SSPM is steadily gaining traction across industries. Notably, **42% of organizations report having implemented a dedicated, productized SSPM solution,** signaling meaningful adoption and growing recognition of its value. While only **30% of survey respondents specifically seek best-of-breed SSPM capabilities,** this doesn't imply limited interest—rather, it could be a reflection of the diversity of strategies security teams are pursuing to reduce SaaS risk.

Some organizations are opting for broader platforms: 38% prefer to consolidate with security service edge (SSE) solutions, even if they don’t offer in-depth SaaS security capabilities. Another 30% believe SSE solutions offer “good enough” SSPM capabilities.

Respondents rely on consolidated solutions: 27% use a security service edge (SSE) or cloud access security broker (CASB) solution, while 23% monitor SaaS audit logs using in-app functionalities or ingest them in a security information and event management (SIEM) or other analytics tool.

Conflicting Priorities Create Dangerous Visibility Gaps

43%

When it comes to consolidation, the argument is rarely about “better security.” The “good-enough” camp: 43% are focused on competing cybersecurity priorities and may want to leverage rudimentary SSPM capabilities from existing tools (such as SSE or CASB).

45%

The I-don't-know-the risks camp: 45% struggle with the lack of visibility or clarity to SaaS specific risks and may make the argument that they will make-do with existing tools.

Section

04

Often, the difference between good-enough and best-of-breed is only one data breach. It is the reason that many enterprises are choosing to deploy a dedicated SSPM solution on top of SSE/CASB. By educating decision-makers on the SaaS security landscape and the continuous monitoring that full-featured SaaS security solutions provide, security teams have a better chance of moving implementation forward.

> *"This false sense of security is because they aren't necessarily utilizing their current toolset to report on the alert and contain it. Everyone that's been breached thought they were doing great and didn't know they'd been breached for a year. It's the same with this. It's a third-party risk story. It's a shadow IT story."*
>
> **Ernesto Pereira**
> **Information Security Manager, Episcopal Health Services**

A closer look at the 13% of organizations that have adopted an SSPM solution or equivalent reveals that not all prioritize best-of-breed, specialized tools.

Among these 105 respondents, 47% report using an identity and access management (IAM) solution, while 41% rely on a SIEM. Additionally, 44% lean on the built-in security features of their primary SaaS platforms.

Still, specialized tools haven't been entirely overlooked. Notably, 42% of this group (44 respondents) have implemented a dedicated, productized SSPM solution.

When selecting an SSPM solution, this subset of respondents tends to prioritize a few key capabilities: 61% cite threat detection as most important, followed by SaaS app inventory and discovery (54%), and the ability to detect unauthorized SaaS-to-SaaS connections, including third- and fourth-party integrations (52%).

> *We aim for strategic consolidation where it enhances efficiency and visibility without compromising the necessary depth of security for our most critical SaaS assets. This often involves a hybrid approach, prioritizing deep capabilities for key applications and leveraging versatile platforms for broader coverage and streamlined management.*
>
> Chief Information Security Officer, Business Services

Section

05

Secure in Theory, Breached in Practice

75% of organizations experienced a SaaS-related security incident in the past year, a 44-point increase over 2024. However, 91% of teams say they're very confident in their data security, and 89% report that they have the appropriate level of cybersecurity visibility and monitoring for deployed SaaS apps.

The most common reason for this high confidence is trust in their SaaS provider (53%). While 36% of organizations also report that they've confirmed secure configuration at deployment.

> *"They have confidence because they think they've outsourced the risk. But they may not have thought about how the risk is just transferred to this other entity who now has all the other customers' data as well as their own. [...] Do they just accept that risk when they outsource? They must think through it, because once you put data in another company's hands, you have less control over it. So you may have some confidence. But, you need to recognize that when it's out, it's out of the bag. That Pandora box doesn't close."*
>
> **Brian Wasko**
> **Principal, Microsoft Security**

However, some teams' confidence stems from successfully expanding their SaaS security capabilities. 37% say they have high visibility into sanctioned applications, and 23% report that they have ongoing configuration management.

This suggests that respondents may not understand that effective SaaS security requires both proactive configuration management and continuous monitoring to work together. Monitoring without configuration enforcement results in alert fatigue. Configuration without monitoring leads to blind spots.

Are organizations delegating too much security-related responsibility to vendors, or should cloud security providers follow a shared responsibility model?

Section

05

> *We stress the fact that no matter if it's a SaaS application or in-house, it's a shared model. I could teach you so much. A lot of it I could protect through many different tools. But ultimately, it's going to be the user's attention to detail and carefulness that's going to prevent an issue from arising.*
>
> **Ernesto Pereira**
> Information Security Manager, Episcopal Health Services

Regardless of the reason, this confidence is worth a second look. SaaS environments are complex and have high stakes, as the average cost of a data breach in the United States is $9.36 million, according to the **IBM Cost of a Data Breach Report 2024**. SaaS environments are complex, and they're evolving rapidly. Even the most mature security teams are discovering gaps they didn't know were there.

> *In many cases, the reporting that comes up from an office like mine, tries to sugarcoat things, maybe a little more than things really are. My approach has always been, I want to paint the worst picture possible because I want more [funding] ... I want to tell things the way they are. We do gap analysis. We hire an accounting firm to come in every two years and do a posture assessment and we use that as a roadmap to move us forward into the next two years.*
>
> **Dennis Tomlin**
> Chief Information Security Officer, Multnomah County

Section

06

AI and the New SaaS Security Agenda

Respondents expect several cybersecurity issues to become more prominent in the coming months, with AI at the top of the list of priorities. 61% anticipate more discussions about AI-powered efficiency, pointing to a growing interest in AI-enabled security monitoring and automation.

> *If you're building an AI agent, you're going to have direct connections to make API calls, so you're basically attaching it to an LLM model. And unless that LLM model is yours or from an approved tenant of your own organization, you're basically giving your data away. This is shadow IT. You have likely no BAA agreement. So in the [event] of a breach, you are fully liable. It goes back to utilizing firewall rules for on-prem things and DLP protections. With the newer capabilities that are AI specific within that same tooling, complement it with a solid SaaS protection platform. Because it's that off-network activity that you need to be able to policy and see as well.*
>
> **Ernesto Pereira**
> Information Security Manager, Episcopal Health Services

In addition, 55% expect conversations around securing the use of AI and mitigating the risks it creates. This reflects the reality of the expanded security considerations that AI deployments create and the challenges with monitoring AI tools.

AI also acts as a user, as AI models and tools can access, process, and internalize potentially sensitive data. This can create new opportunities for data exposure and security breaches beyond traditional user access patterns.

> *AI agents now need their own non-human identities. They need to be thought of as users, where the information that they have access to is tightly controlled, just like John Doe, Sally Smith, etc."*
>
> **Brian Wasko**
> Principal, Microsoft Security

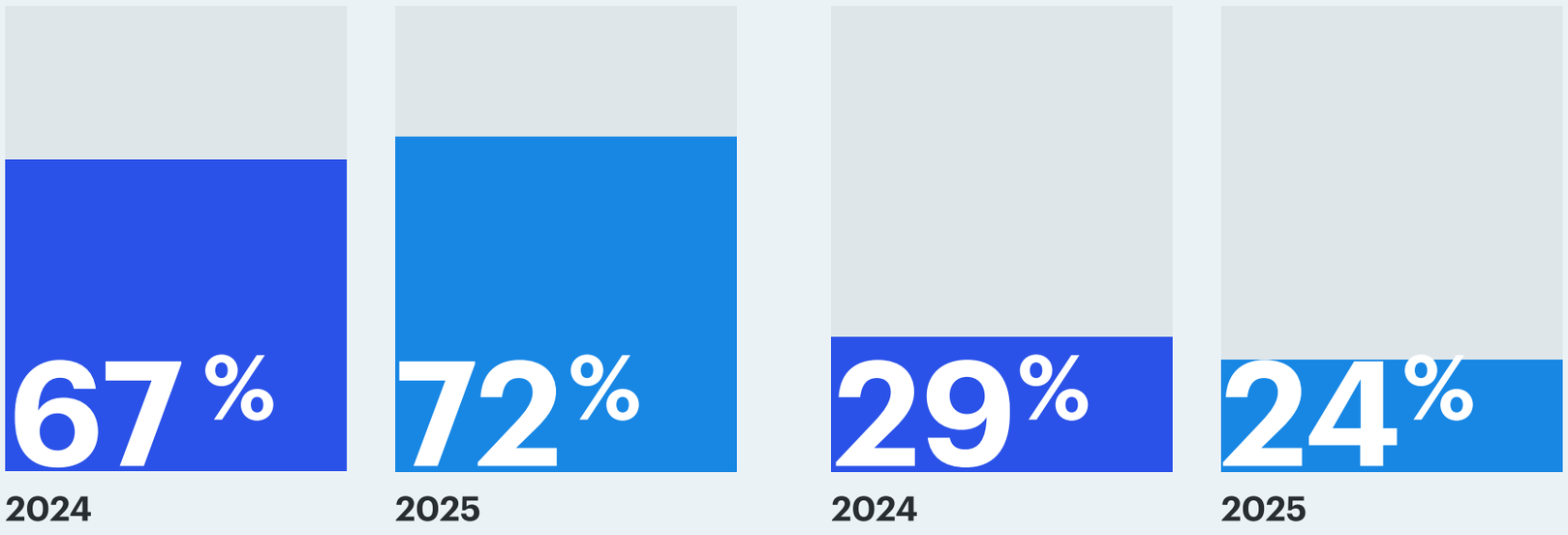
Section

06

As the **Verizon Business 2025 Data Breach Investigations Report** details, corporate data leakage to generative AI platforms and generative AI integrations with mobile device operating systems are both growing concerns.
To guide how AI interfaces with enterprise data, organizations need to manage specific governance.

Securing SaaS apps is at the forefront for virtually all organizations in the near future. Over the next one to three years, nearly all respondents (96%) see SaaS cybersecurity becoming more important, and 72% think it will be one of the top three cybersecurity priorities.

SaaS Security Prioritization Forecast



Compared to 2024 data, this shows that more organizations are focusing on SaaS security, representing a steady increase in this area as a top priority.

The proof is in the numbers. Most organizations' budget allocations already anticipate this shift. In the coming year, most (82%) are planning increases in cybersecurity spending, reflecting the expanding cybersecurity threat landscape and the growing reliance on SaaS apps. The numbers also reveal an evolving perspective. Once an operational concern, SaaS security is now a strategic priority.

Key *Recommendations*

As SaaS adoption deepens and attack surfaces expand, security leaders must reimagine their strategies. The findings from this year's survey reveal a widening gap between perceived and actual security posture, driven by misplaced confidence, inconsistent ownership, and outdated monitoring practices.

Here are our recommendations for overcoming these SaaS security challenges, grounded in the research data and designed to help you future-proof your SaaS security program.

1. Gain Visibility and Control Across Your Expanding SaaS Footprint

While most respondents believe they have appropriate visibility into their SaaS security, 89% of compromised organizations said the same. This illusion of control and safety has become a risk in itself.

Action: Implement effective security tools that do more than aggregate dashboards. Make sure they enforce policy alignment, detect misconfigurations, and provide context on real exposure. Apply the 80/20 rule, also known as the Pareto Principle. This is the idea that a bulk of sensitive data lives within a handful of SaaS apps (20% of SaaS apps account for 80% of the risks). Instead of trying to secure every application, prioritize the critical 20% that store 80% of your organization's sensitive information. This targeted approach will save you from analysis paralysis and maximize operational efficiency.

2. Clarify and Codify SaaS Security Ownership Across Teams

Shared responsibility doesn't mean shared accountability. In 43% of organizations, business units own SaaS security with minimal security team involvement.

Action: Establish and document ownership frameworks between business stakeholders and cybersecurity teams. Embed SaaS security into broader incident response plans and ensure it's not treated as a siloed initiative.

Key *Recommendations*

3. Shift from Periodic Audits to Continuous SaaS Monitoring

Point-in-time assessments are still the norm for 52% of organizations, yet they offer fleeting value in dynamic SaaS environments where posture drift is inevitable.

Action: Replace periodic reviews with continuous monitoring that catches issues as they emerge. Real-time misconfiguration detection, posture validation, and compliance reporting close the gap between audits.

4. Prioritize Mission-Critical Apps, Reduce Alert Fatigue, and Minimize Human Errors

Among organizations that experienced an incident or breach, 66% spend five or more hours each week, yet those hours aren't translating to safer environments. But it doesn't have to be this hard.

Action: Prioritize the apps to secure based on data sensitivity, use the power of AI to identify risks, and monitor continuously to triage alerts, enforce policies, and scan for compliance issues. Free your security teams from tedious, low-value tasks so they can focus on threat response, risk reduction, and strategic alignment.

5. Augment SSE and Threat Detection with SSPM for Deeper, App-Layer Protection

SSE tools are often selected for consolidation and zero-trust network access, but they weren't built to secure SaaS data or configurations. Of those breached or compromised, 39.4% of respondents relied on SSE tools labeled "good enough," while only 9.9% had an SSPM in place.

Action: Integrate a dedicated SSPM solution that extends protection beyond access control to SaaS—into identity governance, threat detection, and continuous compliance monitoring. Prioritize deep coverage for high-risk apps and extend visibility to third-party integrations.

Key *Recommendations*

6. Trust, But Verify: Validate SaaS Posture Instead of Assuming It

91% of respondents expressed confidence in their SaaS security, yet 75% suffered incidents. Notably, 53% of that confidence was based on trust in the SaaS vendor, not internal validation.

Action: Confidence must be earned, not assumed. Conduct routine assessments of app configurations, identity entitlements, and external integrations. Use dedicated SaaS security tools that go beyond surface skimming of policies to surface silent misconfigurations and validate against known best practices.

7. Treat AI Like Any Other Identity: Govern Access and Monitor Usage Continuously

AI is quickly emerging as both a powerful tool and a significant risk vector. 61% of respondents identified AI as the most important topic in cybersecurity for the coming year.

Action: Apply identity governance principles to AI agents, especially those with access to sensitive systems or datasets. Inventory AI usage, enforce least privilege, and ensure AI follows the same access controls and monitoring policies as human users.

Final *Thoughts*

The path to effective SaaS security isn't more complexity; it's clarity, depth, and continuous action. As organizations embrace SaaS as the backbone of their operations and the threat landscape continues to intensify, the time to move from reactive fixes to proactive programs is now. **The data is clear: Simplicity scales, and well-structured strategies win.**

Methodology *& Demographics*

UserEvidence conducted comprehensive research on behalf of AppOmni to understand the current state of SaaS security practices across organizations. This report provides critical insights into how IT and security leaders are addressing SaaS security challenges in 2025.

This report was compiled through a mixed-methods approach combining quantitative survey data with qualitative insights gathered through in-depth video interviews and email questionnaires. The research was conducted from March 15 through April 15, 2025.

RESEARCH DATA SET

- **803 total respondents** across quantitative survey
- **85% are final decision-makers** in IT/security purchasing decisions
- **Mixed methods approach:** Web-based survey supplemented with video interviews and email questionnaires for deeper qualitative insights
- **Double-blind research methodology** to ensure unbiased, authentic responses
- **Verified participants:** All respondents were confirmed as active practitioners in their respective fields through our trusted industry partner network

SURVEY DEMOGRAPHICS & FIRMOGRAPHICS

Geography

Respondents came from a variety of different countries around the globe:

- United States: 60%
- United Kingdom: 12%
- Germany: 11%
- Australia: 9%
- Japan: 8%

Industry Representation

Our respondents represent a diverse cross-section of industries, with the largest segments being:

- IT Services: 30%
- Manufacturing: 15%
- Finance and Insurance: 9%
- Software and Application Development: 9%
- Additional 9% from other sectors

Methodology *& Demographics*

Organizational Size

The research captures perspectives from enterprises of varying sizes:

- 74% work for companies with 2,000+ employees
- 30% work for organizations with 5,000+ employees
- This distribution ensures insights relevant to both mid-market and enterprise organizations

Respondent Roles

Over 61% of respondents hold senior IT-oriented leadership positions, ensuring strategic-level insights:

- IT Manager / Director / VP: 16%
- Managing Director/General Manager: 14%
- IT Administrator / Specialist / Engineer: 11%
- IT Security Manager: 11%
- Chief Technology Officer: 11%
- IT Analyst: 4%
- Head of Cybersecurity: 4%

DATA INTEGRITY & STATISTICAL SIGNIFICANCE

With 803 respondents representing decision-makers across major industries and enterprise sizes, this research provides a statistically robust sample of the IT/security leadership landscape. The large sample size and diverse representation ensure findings are indicative of broader market trends and challenges.

About *UserEvidence*

UserEvidence is a software company and independent research partner that helps B2B technology companies produce original research content from practitioners in their industry. All research completed by UserEvidence is verified and authentic according to their research principles: Identity verification, significance and representation, quality and independence, and transparency. All UserEvidence research is based on real user feedback without interference, bias, or spin from our clients.

UserEvidence Research Principles

These principles guide all research efforts at UserEvidence—whether working with a vendor's users for our Customer Evidence offering, or industry practitioners in a specific field for our Research Content offering. The goal of these principles is to give buyers trust and confidence that you are viewing authentic and verified research based on real user feedback, without interference, bias, and spin from the vendor.

1. **Identity Verification**
   In every study we conduct, UserEvidence independently verifies that a participant in our research study is a real user of a vendor (in the case of Customer Evidence) or an industry practitioner (in the case of Research Content). We use a variety of human and algorithmic verification mechanisms, including corporate email domain verification (i.e., so a vendor can't just create 17 Gmail addresses that all give positive reviews), and pattern-based bot and AI deflection.

2. **Significance and Representation**
   UserEvidence believes trust is built by showing an honest and complete representation of the success (or lack thereof) of users. We pursue statistical significance in our research, and substantiate our findings with a large and representative set of user responses to create more confidence in our analysis. We aim to canvas a diverse swatch of users across industries, seniorities, personas—to provide the whole picture of usage, and allow buyers to find relevant data from other users in their segment, not just a handful of vendor-curated happy customers.

3. **Quality and Independence**
   UserEvidence is committed to producing quality and independent research at all times. This starts at the beginning of the research process with survey and questionnaire design to drive accurate and substantive responses. We aim to reduce bias in our study design, and use large sample sizes of respondents where possible. While UserEvidence is compensated by the vendor for conducting the research, trust is our business and our priority, and we do not allow vendors to change, influence, or misrepresent the results (even if they are unfavorable) at any time.

4. **Transparency**
   We believe research should not be done in a black box. For transparency, all UserEvidence research includes the statistical N (number of respondents), and buyers can explore the underlying blinded (de-identified) raw data and responses associated with any statistic, chart, or study. UserEvidence provides clear citation guidelines for clients when leveraging research that includes guidelines on sharing research methodology and sample size.

About AppOmni

AppOmni is the leader in SaaS Security and enables customers to achieve secure productivity with their SaaS applications. With AppOmni, security teams and SaaS application owners quickly secure their mission-critical and sensitive data from attackers and insider threats.

The AppOmni Platform continuously scans SaaS APIs, configurations, and ingested audit logs to deliver complete data access visibility, secure identities and SaaS-to-SaaS connections, detect threats, prioritize insights, and simplify compliance reporting. The largest global enterprises across industries trust AppOmni to secure their SaaS applications.

Request a customized demo →

American Airlines

airbnb

Google

Meta

Johnson & Johnson

sprinklr

AppOmni