Locking Down SaaS Risk With SaaS Security Management

Pathfinder

November 2021

Commissioned by

AppOmni

451 Research

S&P Global
Market Intelligence

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About the Author

Garrett Bekker

Senior Research Analyst, Security

Garrett Bekker is a Senior Research Analyst in the Information Security Channel at 451 Research, a part of S&P Global Market Intelligence. He has viewed enterprise security from a variety of perspectives over the past 20 years. Garrett started his career in security as an equity research analyst at several investment banking firms, most recently Merrill Lynch, where he covered information security, infrastructure software and networking companies. Garrett has also worked with early stage enterprise security vendors in sales and marketing roles, including Bat Blue (acquired by OPAQ Networks). Prior to joining 451 Research, he also worked at a boutique investment bank focused on M&A and fundraising for small-to-midsized technology companies.

Garrett has focused on a wide variety of subsectors within enterprise security during his career, and is now focusing primarily on identity and access management (IAM), cloud security and data security. Garrett is also a member of 451 Research's Center of Excellence for Quantum Technologies.

Garrett holds a BA in international studies (with honors) from the University at Buffalo, where he was a member of the varsity ice hockey team and learned how to drive a Zamboni. He also completed all coursework for a PhD in economics from the New School University and has completed undergraduate and graduate studies at McGill University and Cambridge University (Queens' College).

Executive Summary

Most discussions of 'cloud security' tend to either focus only on security for IaaS and PaaS, or treat IaaS/PaaS security and security for SaaS applications collectively as a homogeneous market, with similar requirements, drivers and use cases. But the market for SaaS security is quite different and brings its own set of challenges and requirements. SaaS applications are more widely used, and adoption is growing faster than IaaS adoption. So why is security for these different technologies treated the same?

The simple fact is that SaaS and IaaS security aren't the same, and shouldn't be treated as such. For starters, there are many more SaaS apps than public cloud platforms. Many firms have tens, if not hundreds, of SaaS apps in their environment, vs. just one or two IaaS providers. Additionally, SaaS platforms often have more end users across the entire business, which sometimes includes every employee. For example, applications such as Workday, Slack, Microsoft 365 and Zoom are often provided to all employees, and even to some external users as part of a partner or customer portal or a help forum.

Additionally, the adopters and end users of SaaS apps are often line-of-business employees in functional groups like marketing or finance, with nontechnical roles. These users are, not surprisingly, less aware of security issues than the developers and engineers using and administering IaaS and PaaS resources. In other words, it's not often clear where the responsibility for securing SaaS applications lies. SaaS app administrators are often unaware of security requirements because security isn't part of their job, while security teams often don't include SaaS apps in their scope of coverage since these apps have historically been purchased and 'owned' by the business units.

On the technical side, each SaaS app has its own security model, with different settings, schemas, permissions hierarchies, etc., which makes it difficult for organizations to keep up with security for every app in their environment. The characteristics of SaaS apps also make them extremely prone to 'configuration drift' as new releases come out, new users are added and previous users leave the company. This paper seeks to explain how an emerging cloud security category, SaaS security management (SSM), can help firms get a better handle on managing the risk of their overall cloud strategy.

Methodology

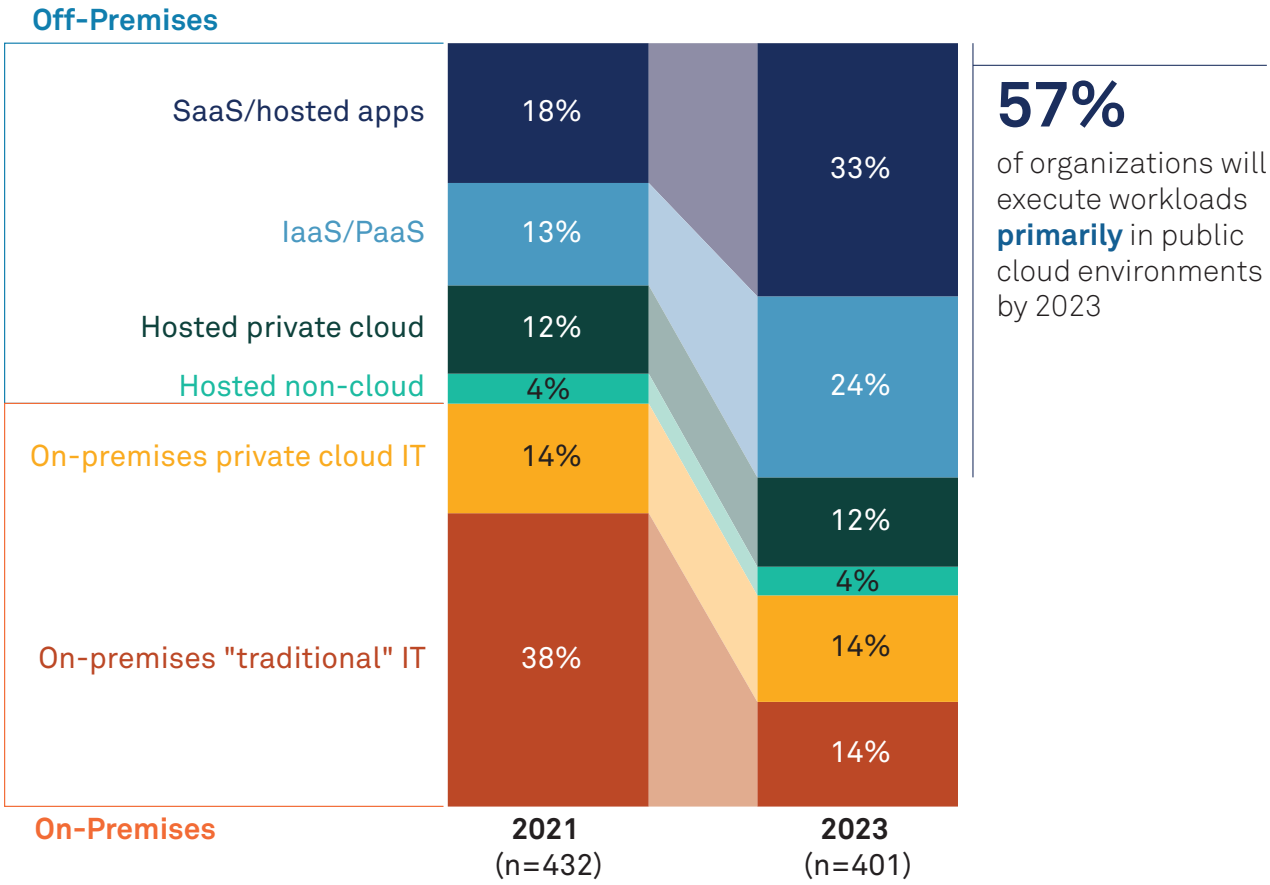
A Pathfinder paper helps decision-makers navigate the issues surrounding a specific technology or business case, explores the business value of technology adoption, and examines the business problems that may be solved by a new technology. Throughout this paper, we cite data from 451 Research's Voice of the Enterprise service, which combines industry-leading analysis with insights from an extensive community of IT and line-of-business professionals, drawing on surveys of IT decision-makers with specific knowledge of their organizations' security strategies.

Key Findings

- Applications are no longer confined to the corporate network. They can be run anywhere – in the public cloud, in private clouds (both hosted and non-hosted), in traditional datacenters and as SaaS apps. Now that our apps, data, infrastructure and users can be basically anywhere, the older perimeter-based security model is becoming less relevant. This implies that our security policies and enforcement points must be everywhere, too.
- Security concerns have long been a primary impediment to broader cloud adoption. While most firms have some degree of cloud services deployed – and are arguably becoming more comfortable with putting critical data, applications and workloads in the cloud – security remains a top organizational concern.
- Much of the discussion around cloud security has historically been focused on securing IaaS and PaaS environments such as AWS, Azure and Google Cloud. Yet SaaS applications are the most widely deployed form of cloud service. According to 451 Research's Voice of the Enterprise data, more than three-quarters of organizations use SaaS applications, which have their own distinct security challenges and requirements. This suggests that security for SaaS applications should be a core part of any organization's overall security strategy.

IaaS, PaaS, SaaS and On-Prem – Workloads Are Everywhere

Figure 1: Primary Workload Execution Venue, 2021 and 2023 (Aggregate)



Q. Which of the following best describes the primary environment used to operate your organization's workloads/applications today?

Q. Which of the following best describes the primary environment in which your organization's workloads/applications will be operated two years from now?

Base: Respondents with workloads/applications

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads & Key Projects 2021

It may seem fairly obvious to state that cloud adoption is growing, but each year even more workloads are moving to the cloud. As organizations continue to migrate to the cloud, security will remain a front-burner issue. In fact, according to 451 Research Voice of the Enterprise data, more than half of all workloads will run in some form of public cloud in the next two years, while workloads that run on-premises in traditional datacenters will be cut sharply.

More specifically, the top choice for running workloads is as SaaS applications, followed closely by IaaS/PaaS. The movement to the cloud itself presents security issues, driven by the architecture of cloud environments and the fact that the underlying infrastructure, data and applications no longer reside on-premises. Many enterprises are now turning to SaaS as the preferred means of deployment for mission-critical applications in finance, HR, CRM and other areas.

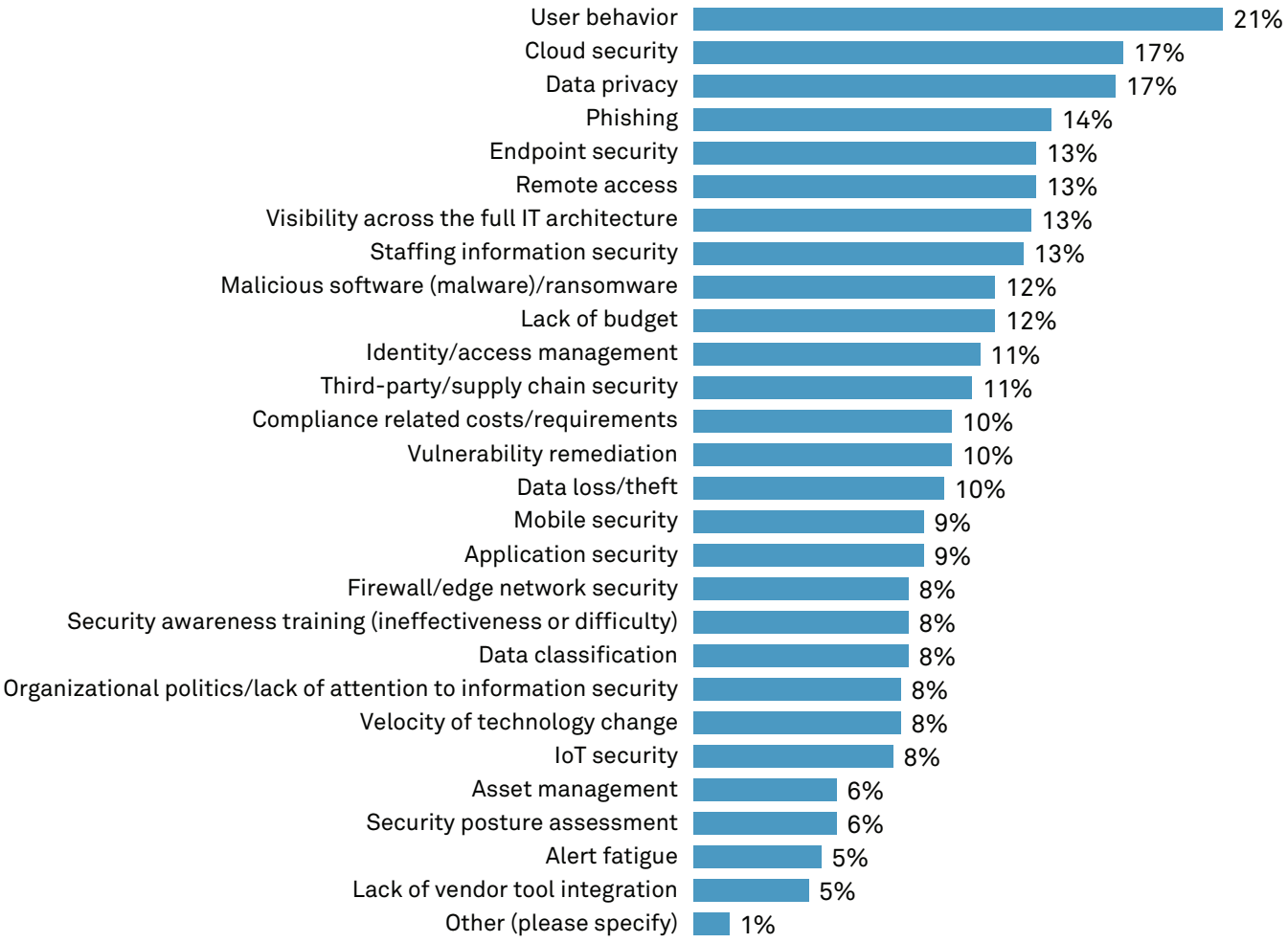
But it's also important to note that the distribution of workloads remains fairly wide and spans a variety of architectures, which means organizations need to maintain a variety of security tooling and approaches. In other words, applications are no longer confined to the corporate network. They can be run anywhere – in the public cloud, as SaaS apps, in private clouds (both hosted and non-hosted) and, yes, in traditional datacenters – which implies that our security policies and enforcement points must be everywhere, too.

Cloud Security Remains a Barrier to Further Cloud Usage

Despite rapid adoption of cloud-based architecture and services, organizations still harbor concerns about the security of their cloud environments. Security concerns have long been a primary impediment to broader cloud adoption. While most firms have some degree of cloud services deployed – and are arguably becoming more comfortable with putting critical data, applications and workloads in the cloud – security remains a top-level concern.

In 451 Research's most recent Voice of the Enterprise survey, cloud security was cited by roughly 17% of respondents as a top security pain point, trailing only user behavior – and ranking ahead of data privacy and even phishing attacks.

Figure 2: Top Information Security Pain Points



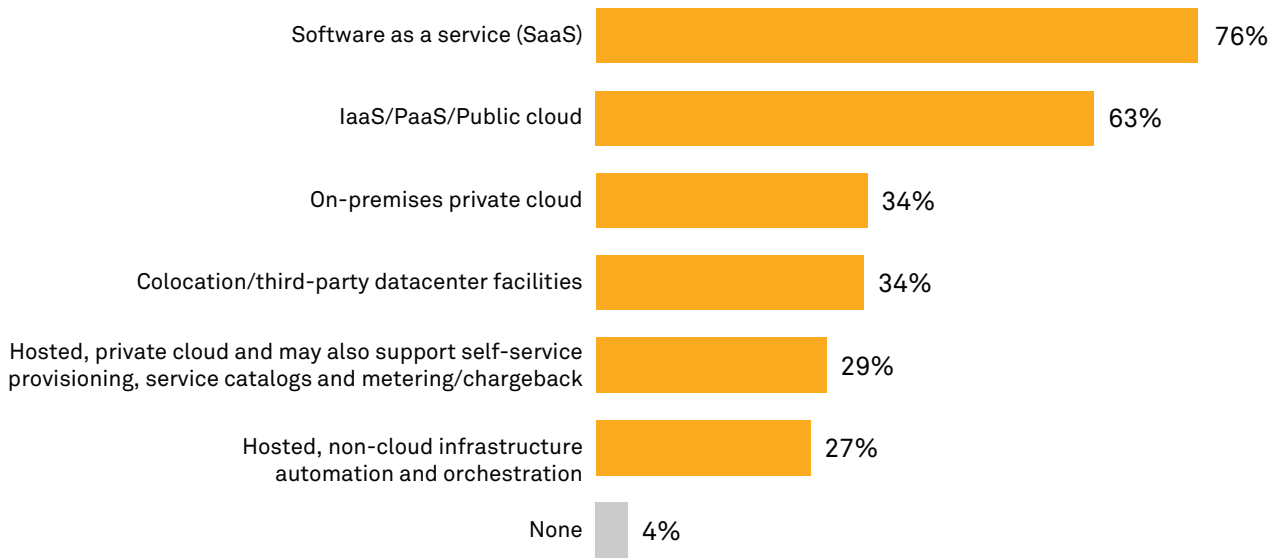
Q. What are your organization's top three information security pain points? Please select up to 3.
Base: All respondents, abbreviated fielding (n=357)
Source: 451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects 2021

Cloud Security Isn't Just About AWS, Azure and Google Cloud

Much of the discussion around cloud security has historically been focused on securing infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) environments offered by the US hyperscale cloud providers – AWS, Microsoft Azure and Google Cloud. While this is understandable, security for SaaS applications can be easily overlooked at worst or, at best, conflated with security requirements for IaaS/PaaS. Yet SaaS applications have arguably been around the longest and are the most widely deployed form of cloud service.

The 451 Research Voice of the Enterprise: Cloud, Hosting and Managed Services, Workloads & Key Projects 2021 study found that more than three-quarters of organizations have deployed SaaS applications. That fact alone should help make the case that security for SaaS applications should be a core part of any organization's overall cloud security strategy, particularly because SaaS applications increasingly store sensitive data that presents immediate and near-term security risks.

Figure 3: Cloud and Hosted Services in Use



Q: Which of the following types of cloud or hosted services, if any, does your organization currently use?
Base: All respondents (n=444)
Source: 451 Research's Voice of the Enterprise: Cloud, Hosting and Managed Services, Workloads & Key Projects 2021

Securing SaaS Apps Is Not Trivial

SaaS applications also have their own distinct security challenges and requirements compared with IaaS/PaaS. For example, under the shared responsibility model, SaaS providers control more of the overall environment, which limits what organizations can control on their own. In an IaaS environment, the cloud provider will generally assume responsibility for things like physical infrastructure, network connectivity, compute, storage and virtualization – while items such as the OS layer, applications, data and identities are largely up to the organization to worry about.

In a SaaS model, however, the OS and application layers are also managed by the app provider, leaving organizations to deal mainly with their data and user identities. Simply put, organizations have less ability to interact with the underlying technological framework of a SaaS app, and are generally left to manage only what they can – data, identities, configurations, settings and permissions. As a result, companies frequently rely on 'default' configurations and settings, which may not be appropriate for that firm. Those defaults can also change over time.

SaaS apps are now mission-critical. Ten years ago, perhaps, SaaS apps were used but were not the nexus of business operations or integral to the success of the organization. Today, organizations cannot simply turn off resources such as Okta, Salesforce, ServiceNow, GitHub, Workday or Microsoft 365, or the business would essentially grind to a halt. SaaS apps are also growing more complex. In the past, licenses were often limited to specific teams, like sales or HR. Many more teams now have licenses – as well as partners, suppliers and customers – which makes managing access for all of these user groups more complex.

Another challenge in securing SaaS apps is the sheer volume of them. There are thousands of SaaS apps in existence, and many organizations use dozens, or even hundreds, of them. Each of those apps is architected differently, which makes it a sizable challenge to cover the most critical ones. Added to that, each application provider has its own lens on the shared responsibility model. And not only are there many SaaS apps, but they are also dynamic. Each SaaS app is unique, with constant new releases, new functionality, and users continually being added and dropped. How do you then manage security for, say, 100 unique SaaS apps? Meanwhile, SaaS apps are often stitched together via automation and integration, which creates new risk vectors for attackers.

One of the biggest security challenges posed by SaaS applications is misconfigured security settings. Many of the most common SaaS apps can be quite complex, with a high number of settings and API calls. That complexity makes it surprisingly easy to leave sensitive data accidentally exposed to the public internet.

A potentially bigger challenge is managing all of the identities, entitlements and permissions that are associated with each SaaS app. Given the number of apps and the increasing complexity, this can't be done manually – it's physically impossible to have expertise in 100 different SaaS apps or platforms in-house. If each app were updated once per year, that's 100 updates to manage – and it's unlikely that apps will update only once per year. In other words, automation needs to be a primary component of the overall solution because it's no longer realistic to have in-house expertise in a multitude of SaaS apps.

Overview of the Cloud Security Market

The cloud security market has been around for approximately 10 years. In that time, it has grown to well over 100 vendors focused solely on cloud security, thanks to a considerable amount of venture capital funding and some sizable sums spent on M&A. At a high level, the market for cloud security can be divided between those vendors that address IaaS/PaaS, and those that address security for SaaS applications. The remainder of this report will focus primarily on the history and evolution of SaaS security, after a brief overview of IaaS/PaaS security is provided for context.

IaaS/PaaS Security

The market for IaaS and PaaS security is relatively broad, and includes a variety of sub-categories, including cloud infrastructure security (CIS), cloud workload protection (CWP), container security, cloud security posture management (CSPM), and cloud infrastructure entitlement management (CIEM).

CIS essentially helps organizations secure and monitor access to IaaS admin consoles, while CWP vendors offer agent-based technology that can monitor workloads running on public cloud platforms for malware, violations and other anomalies. At a high level, CSPM helps firms manage the security configurations and settings in their public cloud environments, while CIEM is focused on managing identities and entitlements for cloud resources

History and Evolution of SaaS Security

Securing data in SaaS applications presents some specific challenges. This is mainly because, unlike IaaS, SaaS providers completely control their own back-end infrastructure and typically offer limited access to third-party vendors.

Some of the first efforts at SaaS security provided access management for SaaS apps in what would come to be known as identity-as-a-service (IDaaS). Vendors in that category, such as Okta and OneLogin, initially focused on providing single-sign-on (SSO) functionality for a handful of the most critical SaaS apps, and later expanded to provide full catalogs of thousands of SaaS apps. Over time, IDaaS vendors branched out to address new customer requirements by adding multifactor authentication (MFA), identity provisioning and governance, privileged access management (PAM), and customer identity and access management (CIAM).

Another early SaaS security category was that of cloud encryption gateways, offered by the likes of CipherCloud, Perspecsys and Vaultive. Such vendors typically functioned as proxies that sat between an organization's network and their SaaS apps to encrypt traffic in transit to and from the SaaS app. The challenge of such an approach was that it typically interfered with the functionality of the apps – including things like search, sort, indexing, etc. – and frequent application updates would often 'break' the app until the proxy could be updated.

Cloud encryption gateways evolved into cloud access security brokers (CASBs), which started out focused on 'shadow IT' discovery and risk scoring of SaaS apps. With respect to shadow IT, most firms today have hundreds, or even thousands, of 'rogue' SaaS apps running in their networks that have not been sanctioned by corporate IT, and that may be completely unknown to IT. As the old adage goes, "You can't secure what you don't know about." For early CASB vendors, discovering these unsanctioned SaaS apps and then performing risk analysis on them was a necessary first step toward providing some degree of security for cloud resources. That's fine, although once you have a handle on what SaaS apps your users have running, the obvious question is "Now what?" So most CASBs later added data loss prevention (DLP), encryption, threat protection and other features.

Early CASBs were also proxy-based and faced some of the same challenges as the cloud encryption gateways, so many added API-based functionality as a complement. APIs are less intrusive than proxies, but aren't capable of real-time blocking, only detection. There are also no API standards, so the capabilities available for each SaaS app depend on the richness of the API the SaaS provider offers.

Both of these product categories faced an issue that many SaaS security vendors must address, which is the technical challenge of covering more than a handful of the thousands of SaaS apps out there. Most cloud encryption gateways have limited their coverage to just the most critical SaaS apps – typically widely used offerings such as Salesforce, Office 365, etc. Another challenge for CASBs in particular is that they don't cover third-party apps, which are connected directly cloud-to-cloud, and directly to an organization's SaaS environment.

Due to some of the limitations of IDaaS and CASB platforms, several new areas of SaaS security have emerged, including cloud identity entitlement management (CIEM), SaaS security posture management (SSPM), and SaaS security management (SSM).

SSPM essentially does for SaaS apps what cloud security posture management (CSPM) does for public cloud environments – namely, prevent misconfigurations that unintentionally leave sensitive data exposed. To address these types of issues, SSPM can manage user access to SaaS applications and provide monitoring, detection and continuous compliance to help firms get a handle on who has access to the data in their critical SaaS applications.

CIEM, meanwhile, deals primarily with managing identities, permissions and entitlements for cloud resources, rather than configuration and posture management. CIEM technology spans both IaaS/PaaS and SaaS, and most vendors in this emerging category specialize in one or the other. Some of the functionality provided by CIEM vendors is discovering all machine and human identities in a public cloud or SaaS environment – as well as their privileges, actions and the resources they can access, and what actions they are taking. The CIEM vendor then attempts to identify and remove excessive privileges. In that sense, CIEM is conceptually similar to providing identity governance and administration (IGA) for the cloud.

How Does SaaS Security Management Fit in With SSPM, CSPM and CIEM?

In a sense, SSPM can be viewed as a subset of SaaS security management (SSM), since it is largely limited to analyzing configurations, settings and other aspects of security posture. In addition to configuration management, SSM also deals with entitlement management, access, permissions, API security monitoring and detection, SaaS risk identification and management, automated remediation workflows, and continuous compliance. SSM can help determine who has direct access to your data, which apps are sanctioned by IT, and whether permissions are overprovisioned for certain users. And given the growing complexity of SaaS apps and the various access scenarios mentioned earlier, this all needs to be automated.

It's quickly becoming physically impossible to manage all SaaS security manually as more SaaS apps are added to an environment and more users are provisioned for each SaaS app. Automation can also help deal with well-known skills shortages in the security industry, free up existing teams to focus on more value-added functions, and perhaps most importantly, improve overall security by ensuring that critical tasks or settings aren't overlooked.

Why SaaS Security Often Falls Through the Cracks

As firms continue to transition workloads to the cloud as part of their overall digital transformation journey, they inevitably have more involvement with SaaS apps, DevOps and cloud-native strategies. In the past – even the recent past – SaaS apps were often procured and implemented by business units, leaving security teams unaware of the many apps in use and unable to access them (the well-known and highly documented 'shadow IT' problem). And those business units often don't prioritize security.

Now that SaaS has become a more integral part of the typical IT stack, a wider range of internal teams and personas are often involved in purchase decisions. Chief digital officers, digital transformation teams, SaaS admins, cloud engineers, security teams and DevOps specialists may all now be part of the procurement conversation.

Even as more organizational teams are involved in purchasing and using SaaS applications, it's still not always clear who is ultimately responsible for securing these apps. In some cases, this can mean SaaS security simply falls through the cracks. To avoid this scenario, organizations may look to appoint dedicated staff for SaaS security, an emerging trend that could have a positive impact on overall cloud security.

How Does SaaS Security Management Fit Into a Zero-Trust Model?

Now that our apps, data, infrastructure and users can be located basically anywhere, the older perimeter-based security model is certainly becoming less relevant. How do you provide security when the network isn't yours anymore (it's the public Internet); the devices aren't yours (some or all may be BYOD, even if you issue corporate-owned devices); the datacenter isn't yours (it's in the cloud); the application isn't yours (SaaS); and even some users (contractors, outsourcers, etc.) might not be yours?

A zero-trust strategy, where trust is not implicitly granted by default and access is primarily granted to specific resources (servers, applications, devices) utilizing the principle of least privilege – only have access to what you should, and nothing more – can help establish and maintain effective security practices in our increasingly distributed world.

But the principle of least privilege at some point intersects with the desire on the part of many businesses and business leaders for 'least friction' – and least friction usually wins! For example, CISOs are strongly aligned to least privilege, but CIOs are more interested in least friction. In sum, least privilege is great, but only if it doesn't impact least friction, and organizations that can figure out a middle ground can be on the golden path.

Conclusions

Applications can be run anywhere, which implies that security policies and enforcement points must be everywhere, too. While most firms have some degree of cloud services deployed, security remains a top organizational concern.

Much of the discussion around cloud security has historically been focused on securing IaaS and PaaS environments, even though SaaS applications have been deployed by more than three-quarters of surveyed organizations. This suggests that security for SaaS applications should be a core part of any organization's overall security strategy.

There are a variety of options for securing SaaS apps, although one of the toughest challenges is to somehow get a handle on the tangle of configurations, permissions and entitlements that come with each SaaS app. SSM is an emerging category that can help firms manage those entitlements and assess risks and permissions in an automated manner, with automated remediation workflows and continuous compliance.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence