2020

SaaS Security and Management

SURVEY REPORT

AppOmni

Executive Summary

Detecting and managing the growing number of risks that threaten a company's network are extremely important priorities for a variety of IT security professionals with responsibility and oversight for data security. These concerns existed long before the pandemic, of course, but as the number of remote workers around the world has spiked in a short time frame, defending the enterprise against cyber risks has become even more critical. While most companies have solutions in place to mitigate against attacks at the perimeter level, they are still ill-prepared to fully detect and protect against the variety and sophistication of risks that can occur with cloud services.

COVID-19 has prompted massive changes to day-to-day operations, including an accelerated rate of cloud adoption by a vastly expanded remote and virtual workforce. Enterprises have leveraged SaaS to manage the transition from the traditional method of business operations to a cloud-first model. With an increase in adoption of SaaS applications, the focus on managing and securing these applications is critical. More organizations are investing in preventative solutions and gaining visibility into their cloud attack surface than ever before. With remote working expected to remain the norm for the long haul, now is the time to implement a strategy that includes mission-critical SaaS applications. Companies that wait until it's too late are going to find themselves behind the curve.

In the context of these fundamental operational shifts, AppOmni, the leading provider of SaaS Security Posture Management (SSPM), sought input and perspective from IT security executives across a variety of industry sectors. Through a September 2020 survey of more than 200 IT professionals in the U.S., AppOmni learned where emerging threats, misconfiguration risk, and SaaS vulnerabilities are converging and driving demand for new strategies due to the shift in remote work. The survey also revealed the need to take a more holistic approach to configuring SaaS applications in order to reduce risks to the business in this new normal of post-COVID-19 work environments.

Key Findings

- Nearly 90% of respondents said that they already have deployed or are deploying SaaS solutions due to COVID-19.
- 2/3rds of respondents said that their ability to manage and secure SaaS applications has been negatively impacted by COVID-19.
- Only 13% of respondents said that they rely solely on a Cloud Access Security Broker (CASB) for their cloud security, with the majority of respondents saying that they deploy multiple solutions.
- Only 32% of respondents said that they employ a type of tooling to ensure data security in SaaS.
- A majority of respondents (52%) said that their existing cloud security solutions are reactive in nature. These solutions only alert security teams of a problem when an incident has already been detected.
- 66% of organizations believe that their current SaaS application would cause the greatest disruption to their business should there be an outage.

About the Survey

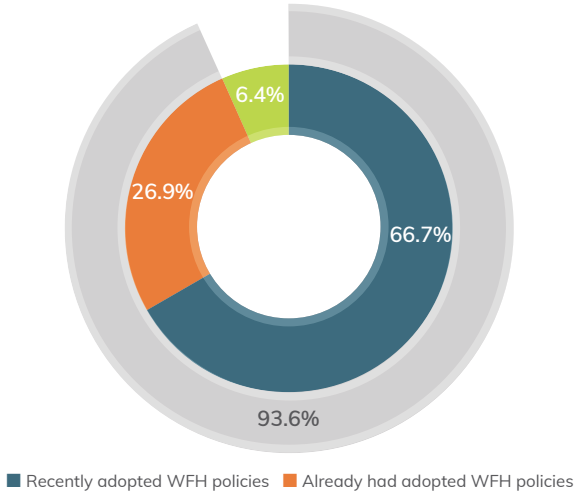
AppOmni worked with Upwave, a brand intelligence platform based in San Francisco, to conduct a survey of more than 200 IT professionals in September 2020. Through Upwave's Digital Network, IT professionals were interviewed in exchange for access to content or a service. Participants received no monetary payment for their participation.

Industry Trends

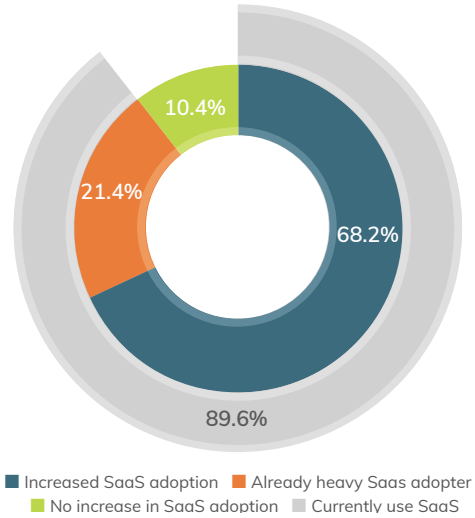
Rise in WFH Initiatives and SaaS Adoption

Earlier this year, in response to the coronavirus pandemic, corporate offices in many parts of the world emptied out as staff members were required or strongly encouraged to work from home. At the time, the systems and networks designed for remote workers mostly consisted of occasional remote access to emails and other applications via VPN backhaul. Very few companies had the IT systems in place to handle even 10% of employees working remotely at any given time. They certainly were not designed to handle a shift to a 100% remote workforce in a matter of weeks.

Have you adopted WFH policies?



Have you increased SaaS adoption due to WFH initiatives?



Our research has found that 66.7% of organizations have adopted work-from-home (WFH) policies. Coupled with nearly 27% of respondents who had already adopted such policies before the pandemic, nearly 94% of organizations today are implementing WFH policies.

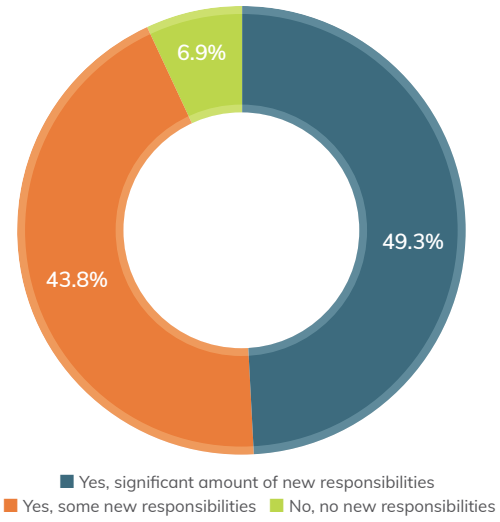
There are several technologies available to organizations that can help them scale up their WFH initiatives. Our research has found that the rate of SaaS adoption is closely correlated with the rate of WFH initiatives, with approximately 68% of organizations increasing their SaaS adoption. In total, close to 90% of organizations today employ SaaS to address the WFH initiatives.

With direct correlation between the increase in WFH initiatives and SaaS adoption, it's clear that organizations are leveraging SaaS to overcome the hurdles associated with transitioning rapidly away from the traditional methods of doing business.

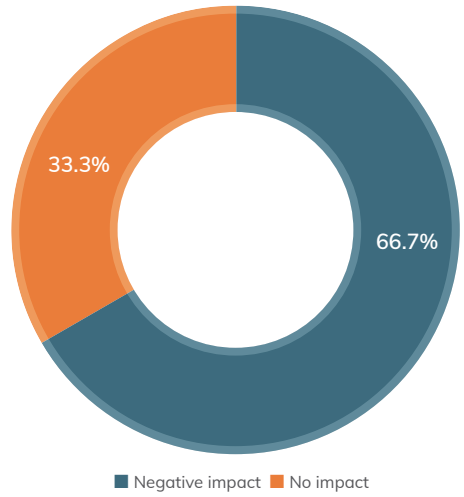
Shift to Remote Work Raises Security Concerns

Survey results indicate that the sudden shift to WFH initiatives caught much of the enterprise off guard, especially the IT staff. Not only do the IT staff now have to coordinate the rollout of new SaaS services, but they are also inevitably tasked with other projects involved in such a change to the way business is conducted. Survey results indicate that the sudden shift to WFH initiatives caught much of the enterprise off guard, especially the IT staff. Not only do the IT staff now have to coordinate the rollout of new SaaS services, but they are also inevitably tasked with other projects involved in such a change to the way business is conducted.

Have you received additional responsibilities due to WFH initiatives?



How have WFH initiatives impacted your ability to manage and secure SaaS?



Our research has found that almost half of the leaders surveyed said their IT departments have recently received a significant number of new responsibilities. In total, 93% of these IT staff members have recently received additional responsibilities due to WFH initiatives. It's evident that the rapid increase in responsibilities has not enabled organizations to staff up their IT teams accordingly, resulting in existing staff having to absorb much of the new workload.

Not surprisingly, two-thirds of respondents said that their IT staff were impacted negatively from the rise in WFH initiatives in recent months, with a lack of available time to effectively manage and secure SaaS a top concern.

The negative impact on IT teams' abilities to effectively manage and secure SaaS poses a significant risk for organizations. Although SaaS offers the benefit and simplicity of "anywhere, any device" access, the features and complexity behind the scenes continue to mount.

For example, the latest release notes from Salesforce, the leading public enterprise SaaS solution provider, is over 500 pages long. The importance of getting the key steps right — including onboarding new users, creating new access policies, and deploying new features — cannot be overstated. Without the necessary time, resources, and tools, organizations are putting their critical data and entire operations at risk.

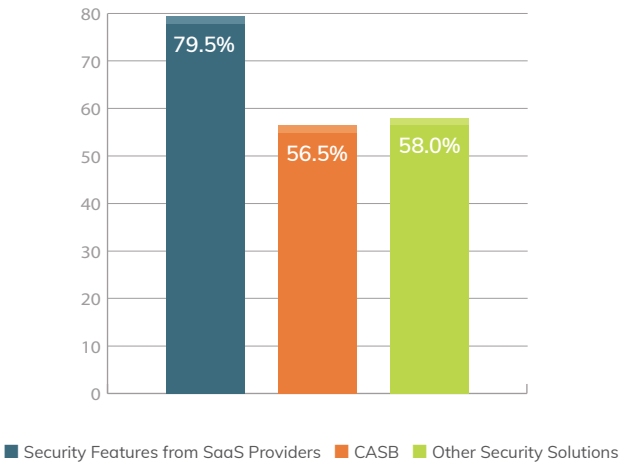
State of Current Cloud Security Solutions

CASB Alone Is Not Enough to Solve Security Issues

2020's massive global shift to remote work has not gone unnoticed by hackers and bad actors, who have shifted their focus to cloud services. Organizations need to deploy appropriate security solutions in order to minimize service disruptions and keep their sensitive data secure. This makes a proper, cloud-focused security stack more critical than ever for today's organizations.

Cloud Access Security Broker (CASB) solutions are the most widely recognized security option for cloud services. According to our survey, however, CASB solutions are not currently the leading security approach deployed. Also, more often than not, IT leaders deploy CASBs alongside complementary security solutions.

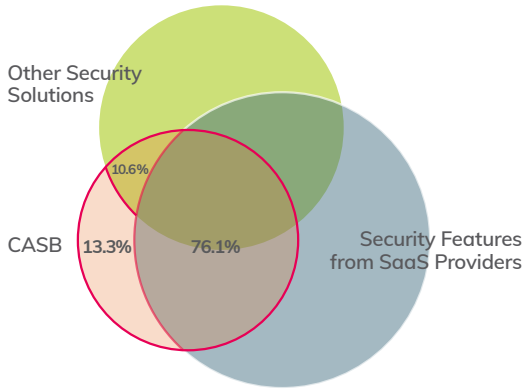
What cloud security solution(s) are currently deployed at your organization?



Our research found that the leading cloud security solutions deployed are those offered by SaaS providers, with close to 80% of organizations surveyed relying on such solutions. Approximately 56% of organizations surveyed are leveraging CASB solutions.

Surprisingly, our survey indicated that organizations are deploying multiple solutions with significant overlap. Over 76% of enterprise IT leaders surveyed who deploy CASB solutions are pairing them with SaaS providers' security offerings. Only 13% of organizations surveyed are relying on CASB as their sole cloud security solution.

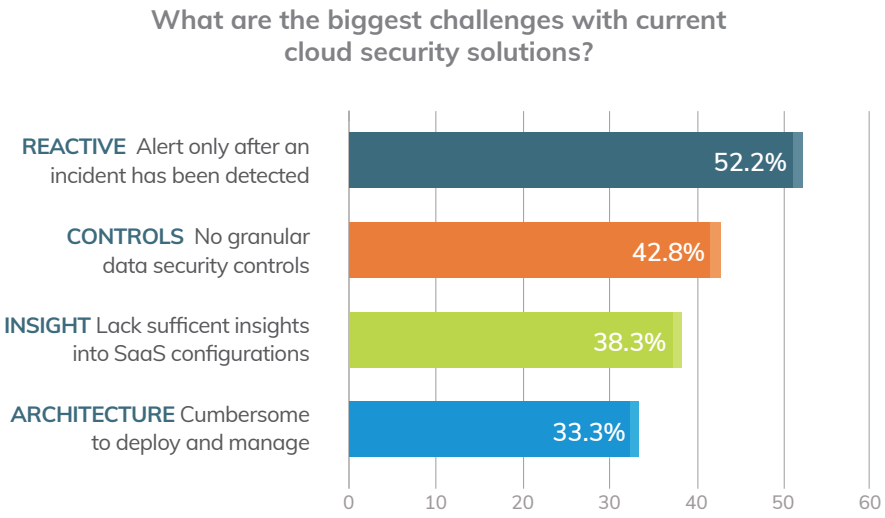
How are cloud security solutions deployed at your organization?



It's evident that security teams believe CASB solutions alone cannot adequately secure SaaS solutions. CASB solutions evolved from several disciplines, including shadow IT detection, data encryption, and Data Loss Prevetion (DLP). The attacker methodologies have also evolved, but differently, leveraging the "anywhere, any device" access of cloud services to gain the upper hand. The traditional security approaches, such as defense-in-depth or perimeter security, simply no longer apply to cloud services.

Biggest Challenges with Existing Security Solutions

With today's rapid pace of SaaS adoption, many organizations are quickly recognizing the drawbacks of available cloud security solutions. While some solutions offer a new approach to cloud security, many continue to leverage legacy architecture that's simply updated to "work" with cloud services. These solutions leave much to be desired by IT teams. With today's rapid pace of SaaS adoption, many organizations are quickly recognizing the drawbacks of available cloud security solutions. While some solutions offer a new approach to cloud security, many continue to leverage legacy architecture that's simply updated to "work" with cloud services. These solutions leave much to be desired by IT teams.



A majority of survey respondents (52%) said that the reactive nature of their existing cloud security solutions is the biggest challenge they have. These solutions only alert security teams of a problem when an incident has already been detected. A carry-over from the legacy security model, these reactive approaches do not allow IT staff to get ahead of each problem. Instead, they require IT to be on standby, with success measured by the fastest reaction time. Ideally, organizations can leverage their IT resources to proactively monitor and keep incidents from occurring in the first place.

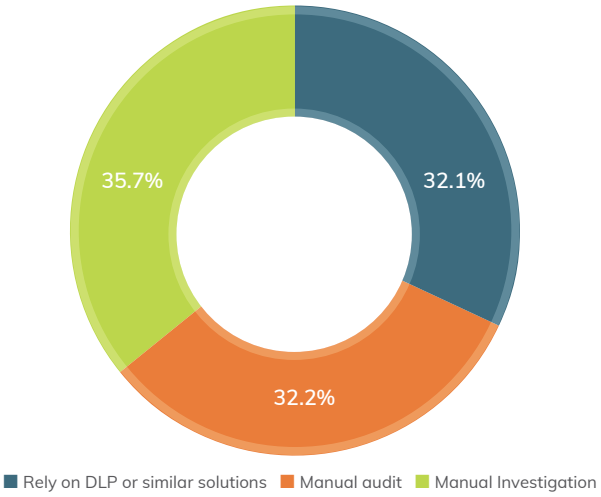
The second and third most common challenges mentioned by respondents are the lack of granular data security controls and SaaS configurations, respectively. Unfortunately, the lack of granular insight and controls plague solutions that attempt to provide broad coverage across a large number of applications. With this approach, it's not possible for a security solution to articulate a critical configuration for data between, for example, a CRM solution like Salesforce versus an HR solution like Workday.

The fourth biggest challenge reported in our survey relate to solution architecture. Many solutions require the use of gateways to route all cloud traffic and/or the use of device clients. But gateways aren't much of a departure from traditional VPN backhaul architecture. In fact, using gateways to aggregate traffic counteracts the main benefit of cloud services — allowing users to connect directly with the SaaS application using the most efficient method.

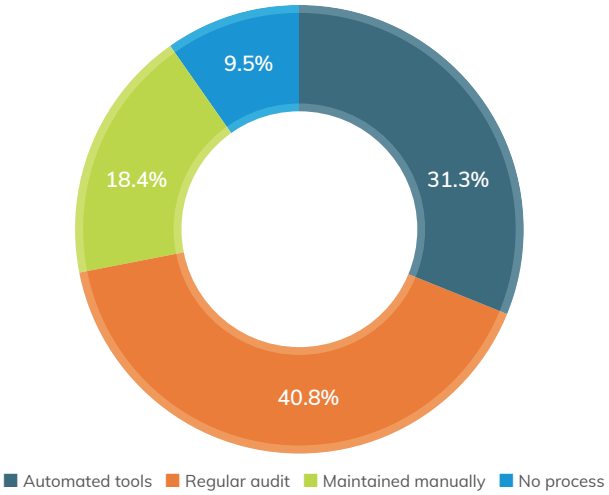
SaaS Security and Management Operations Issues

Phishing attacks, advanced persistent threats (APTs), and malware are some of the common types of cyberattacks cited by IT teams. However, when it comes to securing the cloud, the misconfiguration of services is by far the most prevalent problem. In fact, according to Gartner, Inc., "Through 2025, 99% of cloud security failures will be the customer's fault."[1] Not surprisingly, our survey showed that 77% of IT professionals agree with Gartner that practically all cloud security failures are the result of cloud service customers.

How do you ensure data security in SaaS applications?



How do you ensure SaaS configurations do not deviate from best practices?



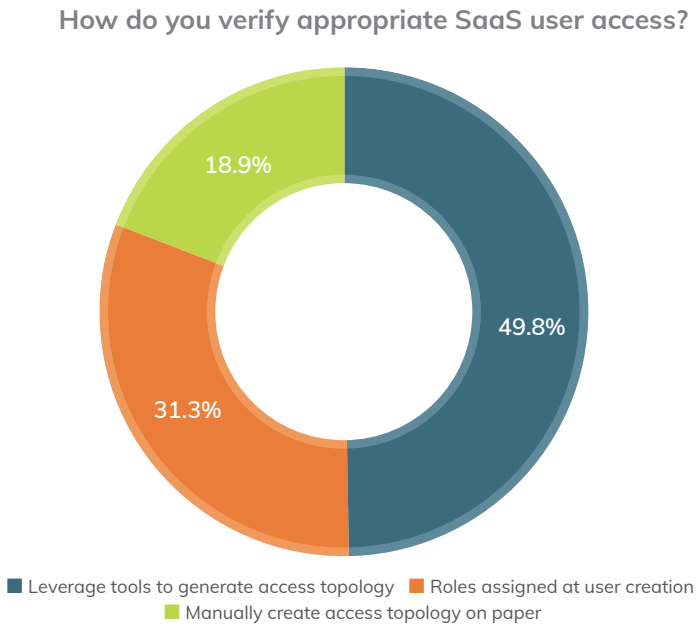
Despite the growing complexity of cloud services, only 32% of organizations in our survey employ automated tooling to ensure SaaS data security. The vast majority continue to rely on manual efforts, such as audits and manual investigation methods like bug bounty programs.

This trend towards manual security management was also evident when it came to ensuring SaaS configurations. Only 31% of organizations surveyed employ any type of tooling to ensure SaaS configurations do not deviate from best practices. Alarmingly, 10% of respondents said they do not have any process to ensure sound SaaS configurations.

While SaaS applications are incredibly powerful as they integrate with a variety of APIs and data sources, this capability also creates complexity. Security teams need to assess and manage the configuration of these applications across multiple instances and environments. It's terribly time-consuming to track and manage this manually, which is why mistakes are made so frequently.

[1] Source: Panetta, K. (2019, Oct 10). Is the Cloud Secure? Gartner Inc. Accessed October 26, 2020. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

SaaS solutions are constantly morphing as new users and data are added. Over-privileging users as a result of frequently-shifting, complex roles is one of the biggest challenges that IT teams face. With SaaS applications being used to provision a wide range of users, from employees and contractors to partners and customers, a misconfiguration of a user's role can result in exposure of sensitive data. Verifying appropriate user access has become an arduous task for many IT staff.



Our survey found that approximately half the organizations surveyed leverage tools to ensure appropriate user access. Unfortunately, the other half rely on manual methods. 31% of respondents said that they only verify a user's role when the user profile is created. As roles continue to expand, simply assessing the user's access levels at the time of profile creation will most certainly lead to inappropriate access rights in the near future. Approximately 19% of leaders surveyed said that their IT teams re-create user access topology on paper from the combination of roles assigned. This is a laborious and time-consuming task that many IT staff still resort to today.

We are seeing an increasing awareness around the risks of SaaS technologies. Security, privacy, and governance, risk management, and compliance (GRC) teams are now discovering that the data accessed and stored in these systems is critically important to their company. As such, they want to make sure that there are proper protections in place.

We see companies looking to better understand their SaaS security posture, including how these applications are configured, who has access to them, and what types of business-critical data is being stored within them. Enterprises are also looking to educate their SaaS teams with security best practices or compliance requirements while implementing technical configuration safeguards.

Conclusion

With the pandemic causing a widespread, rapid shift to remote work around the globe, many businesses have been forced to make major technology changes very quickly. It's unimaginable that a technology shift that big, made that quickly, wouldn't create new avenues of exposure. We are seeing two main factors contributing to increased risk.

The first is complexity. The simple-to-use, "any device, anywhere" approach to accessing cloud services is powered by rather complex configurations and settings. The rapid adoption of SaaS and the lack of in-house expertise for both SaaS and cybersecurity have resulted in a perfect storm in which organizations inadvertently but routinely expose sensitive data. Reliance on legacy/traditional security solutions, with their reactive architecture and lack of granular controls, has done very little to offset the complexity of SaaS applications that IT staff face.

The second is tooling — or the lack thereof. Many organizations continue to throw money and manual resources at these problems in hopes of a quick fix. Unfortunately, the SasS risk we face today cannot be addressed simply by leveraging more resources, a strategy that will hit the point of diminishing return rather quickly. The lack of automation and tooling employed today is particularly alarming as organizations ratchet up their SaaS deployments even further. Tools that not only assist in configuring SaaS services but also help monitor and maintain the service are key requirements.

Security leaders need to make SaaS applications first-class citizens in their security programs. A crucial step in that direction is adopting a new breed of security solutions designed specifically for the cloud. IT must scan cloud APIs looking for data exposures and excessive privileges. They need to assess and analyze the configurations of these applications against best practices. They must ensure that the right security controls are in place — and stay that way. They need security baselines for their mission-critical applications, and they need to detect configuration drift when it occurs so they can remediate it, or prevent it from occurring in the first place. These are no longer nice-to-haves but rather necessary requirements as part of any SaaS deployment.

642 Harrison Street
San Francisco CA 94107
info@appomni.com
appomni.com