AUGMENTT

2023 State of SaaS Report

As the Software as a Service (SaaS) market matures, MSPs who can build, scale and monetize their SaaS management and security stack will enjoy a bright and profitable future.

With the shadow of economic uncertainty affecting industries across the globe, organizations are finding varied pathways to navigate the present and prepare for the future. As a result, IT teams and business leaders are thinking about greater efficiency, integration and automation to best position their companies heading into 2023. However, one of the biggest challenges is correcting mistakes made by rushing to the cloud during the pandemic without following the proper procedures. Now they need to determine the best ways to get this technology to work for them rather than against them.

Here are some highlights of challenges organizations face going into the new year and opportunities for the IT channel.

THE SaaS-POWERED WORKPLACE IS HERE

SaaS applications have become an embedded part of enterprise computing, with **74% of respondents** in a global Axionius survey saying more than half of their applications are now SaaS. Additionally, the SaaS market is currently on a growth trajectory, with spending on cloud applications expected to reach $195.2 billion in 2023, **up from $146.3 billion in 2021**, according to an October 2022 forecast from Gartner. Further, the analyst firm predicts that 85% of organizations will embrace a cloud-first principle by 2025, evidenced by the growing number of SaaS-based applications in use today.

With Much SaaS Comes Many SaaSOps Challenges

The rush to the cloud at the height of the pandemic brought with it an imbalance in the following four areas:

1. **Efficiency.** With organizations now using an average of 130 applications, there are often dozens of apps that do the same thing (e.g., cloud storage, videoconferencing, project management). Although employees may have their personal app preferences, all these "little" subscriptions can add up to considerable costs, not to mention creating data silos that make automation, analytics and overall management nearly impossible.
2. **Security.** With the new hybrid work reality, more work is happening outside the office than ever. That means apps are being accessed, and sensitive information sharing occurs outside the corporate firewall. Cybercriminals are taking advantage of these new work arrangements, too. For example, The Verizon 2022 Data Breach Investigations Report cites **40% of ransomware incidents involve desktop-sharing software**.

   Inside security threats are another concern. For instance, employees storing sensitive company information in their cloud accounts is a common scenario. What happens to that data when the employee leaves the company?

   Per Cisco's 2022 Global Networking Trends Report, **76% of IT teams** said remote workers are harder to secure. Additionally, **51% of organizations** said they had had problems connecting workers to company resources over the past 18 months.

3. **Visibility.** There's often a significant disconnect between how easy it is to "go to the cloud" and achieving the desired results. Presidio's 2022 Cloud Transformation Benchmark Report, which surveyed 1,000+ IT decision-makers, found data source challenges were a common complaint from organizations that weren't united, lacked the right expertise or didn't plan their cloud migrations properly. Seventy percent of respondents reported difficulties with too many disparate data sources, and **almost two-thirds (65%)** said having actionable data and dashboards accessible to the right users was challenging. Additional serious data challenges include having **real-time access to data (62%)**, **finding meaningful insights from data (62%)** and **supporting machine learning (60%)**.

4. **IT Skills gap.** **Less than 1 in 5 organizations** say their teams are proficient with cloud operating models, and **just 14%** say they are proficient in artificial intelligence and machine learning, Presidio's research shows. Additionally, **less than a fifth (17%) of IT decision makers** say their team is currently proficient with DevOps and automation.

SAAS-BASED SECURITY VULNERABILITIES ARE A SERIOUS CONCERN

Popular SaaS applications, like Microsoft 365 (M365) which is used by nearly 880,000 US companies, continue to be common entry points for breaches and ransomware. For example, an Egress data loss prevention report found that 85% of organizations using Microsoft 365 had suffered email data breaches in the past 12 months. The report also confirmed how remote work had deepened the risk of an email data breach — a risk that was intensified for Microsoft 365 users. Specifically, **67% of IT leaders** reported an increase in data breaches due to remote work, versus **32% among IT leaders** whose organizations weren't using Microsoft 365.

Proactively Strengthen M365 Security

Besides implementing good cyber hygiene practices (e.g., strong passwords, multifactor authentication and Least Privilege Access), MSPs should take the following steps to ensure stronger M365 security:

1. Monitor how eDiscovery, Power Automate and other core tools in M365 are used each day. That way, administrators can identify suspicious or malicious activity immediately and potentially stop it before damage is done.
2. Adopt a SaaS security solution (like Augmentt Secure) to create a unified view of security across all environments to identify malicious behaviors that may appear within an IT network, SaaS cloud environment, data center or elsewhere.
3. Use an AI-powered network detection and response tool (like Augmentt Engage) to strategically cut through the noise and avoid being overwhelmed by too many false positive M365 alerts.

THE RIGHT MSP PARTNER IS VITAL TO A BETTER CLOUD EXPERIENCE

Many organizations (**94%, per Presidio's research**) report that it's essential to work with a partner with a broad range of security expertise and experience in modern network technologies that can handle all types of data and span on-premises and cloud. For a smoother, more effective digital transformation, organizations can work with an MSP partner with broad expertise who can help bridge the IT skills gap. Additionally, the right partner can provide a neutral third-party perspective, break down silos and help IT leaders drive business strategies that stimulate innovation and growth.

2023 CAN BE THE YEAR OF SAAS MONETIZATION FOR MSPs

MSPs have an opportunity to monetize SaaS security services, with the advantage they know the SaaS application space and can, through automation, quickly add value to a customer's cloud compute environment. Additionally, by adding SaaS security to their stack, MSPs can scale their businesses and grow revenue at a time when budget scrutiny will most certainly continue.

On an operational level, providers can use automated threat reports and audits to show numerical proof that they are adding value. In addition, they can help IT strengthen threat defense by remote monitoring, saving staff time for all parties.

As a trusted security partner, MSPs can also educate their customers on general best security practices and preventive measures. The result will be a more secure SaaS environment for the customer and a new means of monetizing SaaS security services for the channel.

Final Thoughts

A final tip for MSPs looking to add SaaS security to their stack to improve their customers' security postures and drive revenue growth is to select a vendor-agnostic provider. The ongoing consolidation in the industry makes this vital to long-term success, and MSPs never know when a solution they're using will be folded into another provider's solution. As such, MSPs should look for vendors that invested in building out their integrations and supporting the SaaS platforms that enable their customers to be secure and productive.

As we move into 2023, there's no doubt that the SaaS market will continue to mature, consolidation will prevail, and security will remain top of mind for businesses of all sizes. MSPs who can build, scale, and monetize their SaaS management and security stack will reap the benefits of this market maturation.