CHANNEL MASTERED
Research | Strategy | Consulting | Content

State of SaaS Security 2024

Sponsored by

SaaS Alerts®

STATE OF SAAS SECURITY 2024

TABLE OF CONTENTS

Introduction

Plenty of today's managed service providers (MSPs) are old enough to remember when software as a service (SaaS) was a novel and somewhat controversial concept. Reliability was an issue in those early days, as were bandwidth constraints. Many businesses worried about the compliance implications of entrusting sensitive data to platforms beyond their direct control.

Enticed by the cloud's scalability and OPEX-based subscription pricing, however, businesses gradually shifted more and more of their workloads to SaaS solutions despite those concerns. Global spending on SaaS offerings will grow 20% in 2024 to just over $247 billion and climb another 19.4% in 2025, according to Gartner, and about two-thirds of business application spending by SMBs this year will go to SaaS vendors, according to Analysys Mason.

SMBs have been especially enthusiastic participants in the SaaS economy. Indeed, the average small business has 217 applications in its software portfolio today and the average medium business has 314, according to SaaS management vendor Productiv.

All of that SaaS adoption has attracted the attention not just of Wall Street but of hackers as well, a fact that's confronted MSPs with serious security challenges that only a new generation of security solutions can address.

Based on research performed by Channel Mastered on behalf of SaaS security vendor SaaS Alerts, this report documents the many ways that widespread use of SaaS applications has impacted MSPs both for better and for worse. Among other key findings, it shows that:

- Cloud vulnerabilities have surpassed ransomware on a long and growing list of cyber threats.
- SaaS security is imposing time-consuming and expensive operational burdens on MSPs.
- SaaS security is generating serious amounts of incremental monthly recurring revenue.

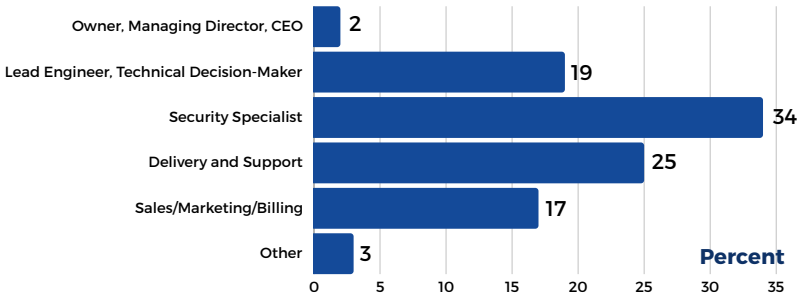
This report shows as well that using appropriate tools equips MSPs to mitigate SaaS security risks and lower SaaS security overhead without sacrificing SaaS security revenue. SaaS Alerts partners in particular, we will see, enjoy a range of important advantages over other MSPs, including:

- Better monthly recurring revenue (MRR) growth
- Better *security* MRR growth
- Fewer security incidents
- More confidence in their ability to safeguard clients

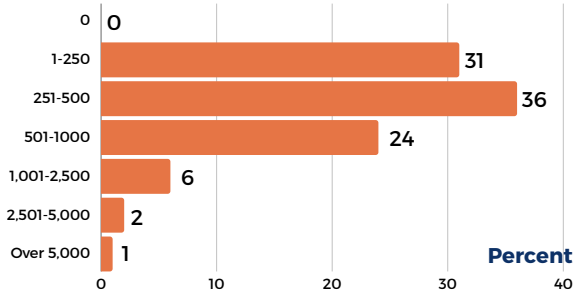
Methodology

The *State of SaaS Security Report* is based on data collected online from 2,804 providers of IT services, including 724 users of SaaS Alerts software, in April and May of 2024.

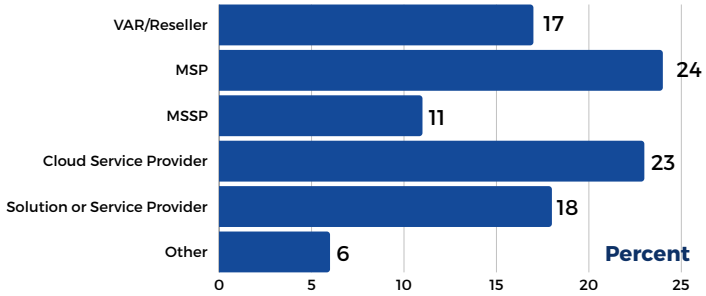
Role



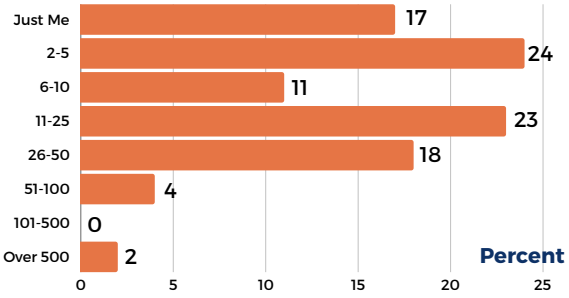
Endpoints Under Management



Primary Business Model



Full-Time Employees



SaaS, SaaS Security, and the Managed Services Business Model

Rising use of SaaS applications by SMBs has affected more than just security for MSPs. It's also disrupted their previously lucrative on-premises revenue streams. 31% of MSPs, in fact, say they've been moderately impacted by the shift to software as a service and 22% have been significantly or extremely impacted. Just 8%, by contrast, say that increased use of SaaS solutions hasn't threatened traditional revenue sources at all. (See Figure 1.)

None of that has prevented MSPs from continuing to see the great success they've enjoyed for years, however. While 4% of those we polled expect monthly recurring revenue to shrink in 2024 and 30% expect it to stay about the same, fully two-thirds anticipate higher MRR this year than last and 26% believe that growth will exceed 10%. (See Figure 2.)

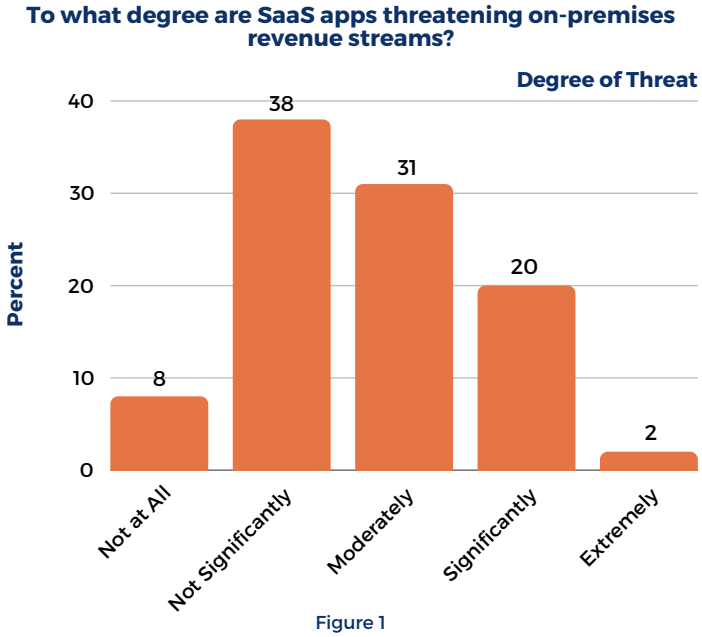


Figure 1

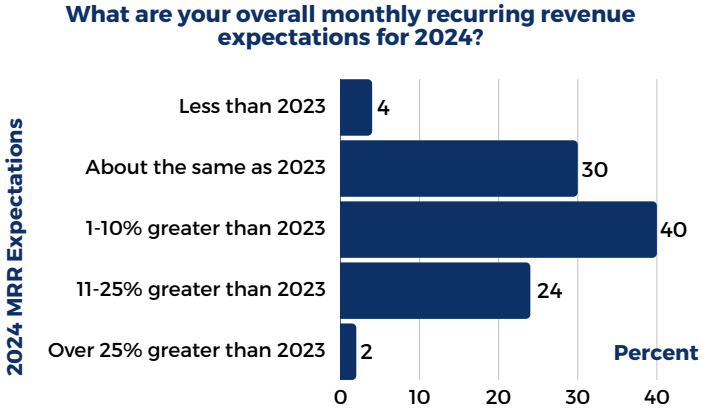


Figure 2

SaaS, SaaS Security, and the Managed Services Business Model Cont.

Projections for security MRR are even better, albeit by small amounts. Though the same 4% of MSPs expect it to decline this year, only 28% believe it will stay the same and 67% believe it will rise. (See Figure 3.)

The absolute dollar amounts behind those percentages are meaningful too. 65% of the MSPs in our research sample, which ranged from small providers to enormous ones, collected at least $50,000 of incremental MRR specifically from offering SaaS security in the prior year, and 44% collected at least $100,000. These are substantial sums given that 65% of survey respondents recorded between $250,000 and $1,000,000 of total MRR in the same time span. (See Figure 4.)

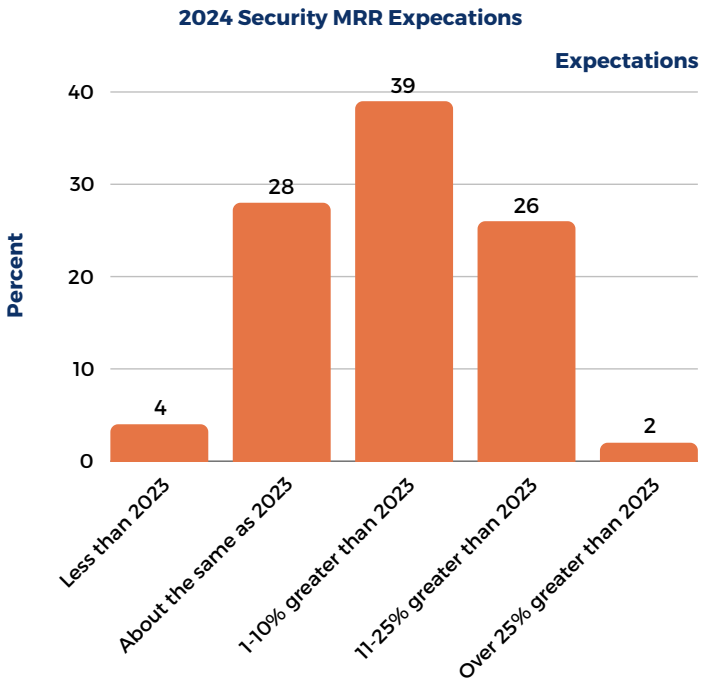


Figure 3

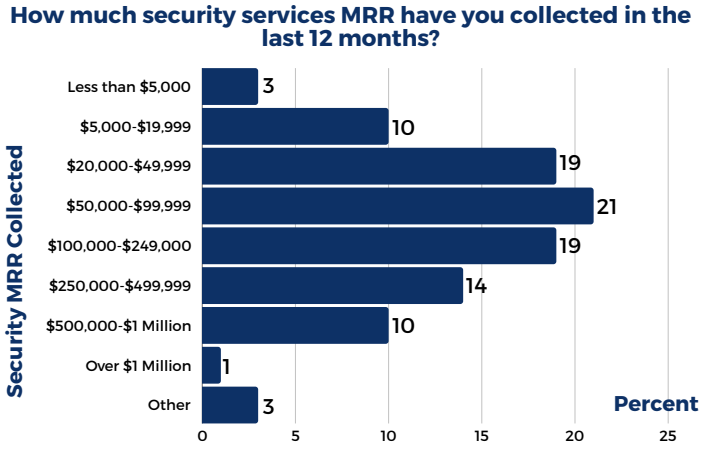


Figure 4

SaaS Security's Operational Impact

Though SaaS security has been a source of fresh income for managed service providers, it's also been a source of added operational expenses. Fully 45% of MSPs currently devote at least five hours a week on average to SaaS security monitoring and management, and 20% dedicate at least 10 hours weekly. (See Figure 5.)

One particular component of SaaS security management—policy configuration management and reporting—is proving to be especially time-consuming. Some 40% of MSPs we surveyed are dedicating five or more hours a week to that task, and 12% are dedicating at least 10 hours. (See Figure 6.)

Numbers like that add up quickly. Median total pay for a managed services technician (which excludes costs included in "fully burdened" labor calculations) is $67,577 at present, according to employment site Glassdoor. That comes out to roughly $32.50 an hour. An MSP spending eight hours a week on SaaS security monitoring and management, therefore, is paying $260 for that work 52 times a year, which amounts to $13,520 annually. This means an MSP receiving $70,000 a year of incremental MRR from SaaS security is losing just under a fifth of it to administrative overhead.

Additional data from our survey confirms that SaaS security monitoring and management is expensive for MSPs. 61% of them say it accounts for more than 20% of their overall labor spending, and 23% say it accounts for over 30%. (See Figure 7.)

On average, how many hours a week do you or your techs spend on SaaS security monitoring and management?

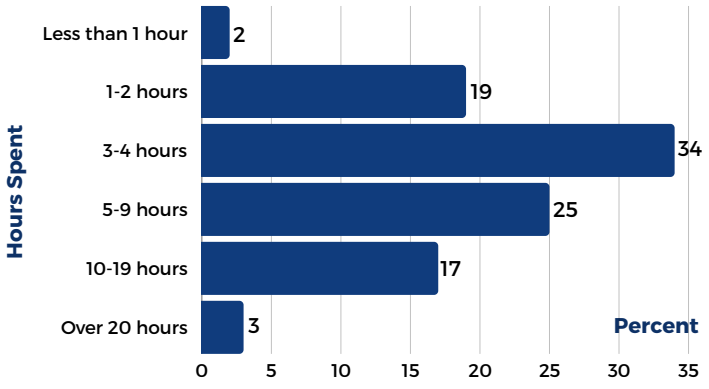


Figure 5

On average, how many hours a week do you or your techs spend on security policy configuration management and reporting?

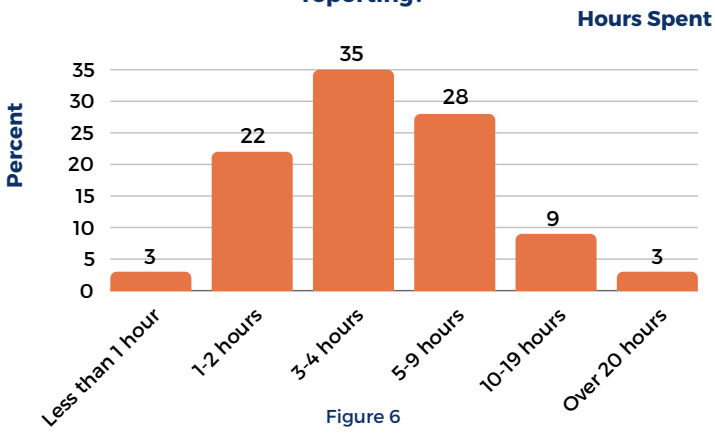


Figure 6

On average, what percentage of your overall labor spending is consumed by SaaS monitoring and management?

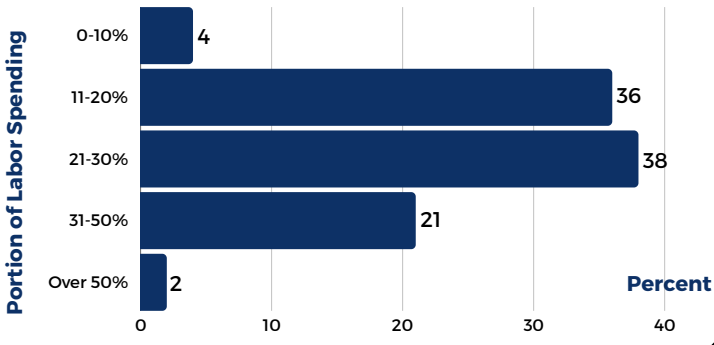


Figure 7

The SaaS Threat Landscape

Though SaaS has become the dominant way SMBs run applications, solutions designed chiefly or exclusively to protect SaaS applications remain surprisingly rare. Threats aimed at SaaS solutions, by contrast, are anything but unusual. Cloud vulnerabilities are in fact the third largest security threat end users face at present and comfortably ahead of ransomware, according to MSPs in our study. Only phishing and business email compromise attacks scored as bigger dangers, and since both of those threats involve SaaS email applications, they arguably are cloud vulnerabilities too. (See Figure 8.)

Specific cloud vulnerabilities MSPs worry about include poor access management (cited by 54% of survey participants), misconfigurations (cited by 44%), and lack of multifactor authentication (cited by 43%). It's worth noting that the *2024 SaaS Application Security Insights* report from SaaS Alerts showed that MFA is disabled or inactive for a staggering 65% of end-user accounts managed by SaaS Alerts' partners. (See Figure 9.)

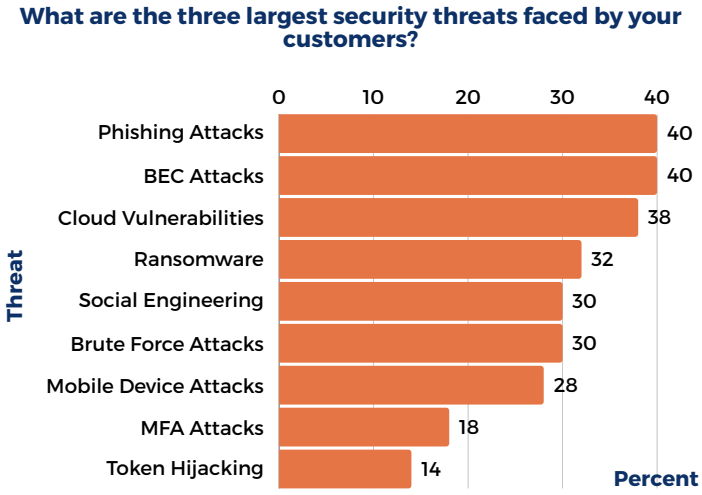


Figure 8

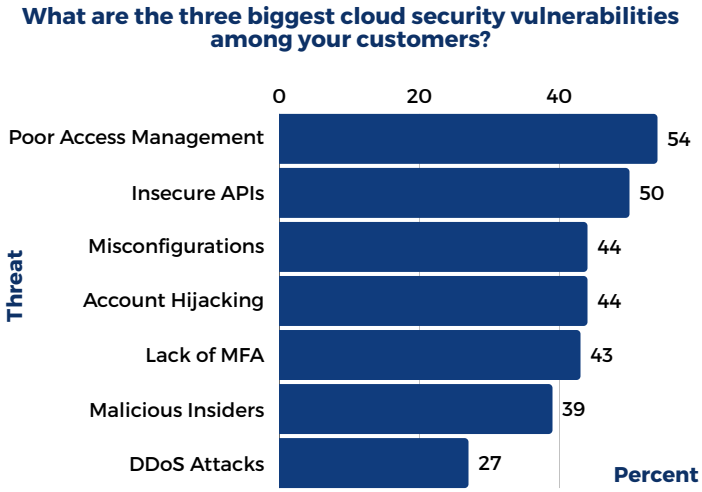


Figure 9

The SaaS Threat Landscape Cont.

Cumulatively, cloud vulnerabilities saddle MSPs with a range of difficult security challenges. Some, like too much log data and too many false positives, are familiar, but today's number one challenge—centralized, correlated visibility across multiple applications from different vendors—is specific to SaaS. A Microsoft 365 login in Beijing by a user already running Salesforce in Chicago is a sure sign of trouble that an MSP will miss if they can't see all of a customer's SaaS activity in one place. (See Figure 10.)

Given this long list of challenges, it's no surprise that SaaS-related incidents have become disturbingly commonplace. Close to half (49%) of the MSPs in our survey say that more than five of their customers have experienced a SaaS compromise in the last year and 22% say that over 10 accounts have had a compromise. (See Figure 11.)

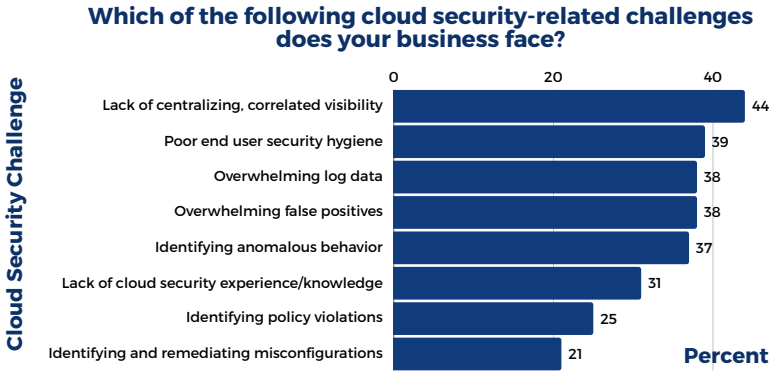


Figure 10

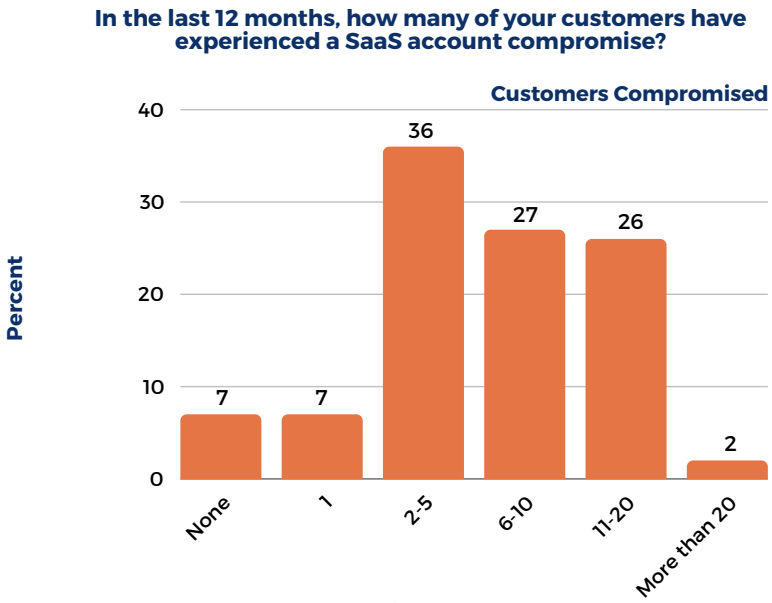


Figure 11

SaaS Alerts Partners Enjoy Significant Advantages

As noted before, only a handful of solutions on the market today focus on SaaS security, and SaaS security systems with table stakes functionality for MSPs like multi-tenancy and PSA integrations are even harder to find. SaaS Alerts is one of those exceedingly rare solutions, and data in this report illustrates the advantages for MSPs of having a pure-play SaaS security solution in their stack. More specifically, *SaaS Alerts users are keeping customers safer, growing faster, and sleeping better at night than other managed service providers*.

For starters, SaaS Alerts partners experience fewer account compromises than their peers. 58% of them report fewer than six compromises over the last 12 months versus 48% of everyone else. (See Figure 12.)

When accounts are breached, SaaS Alerts' users auto-remediate the issue at significantly higher rates too. Fully 76% of them, in fact, say their SaaS security tool remediates compromises to prevent data loss and other malicious activity automatically, versus 67% of everyone else. (See Figure 13.)

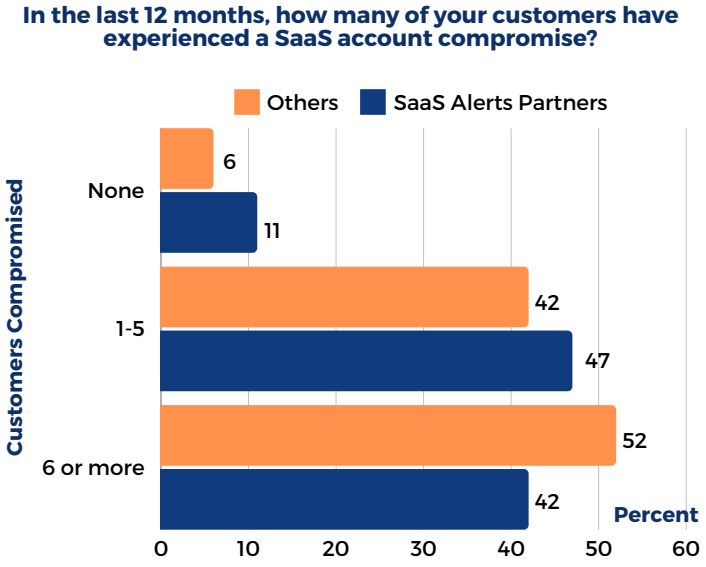


Figure 12

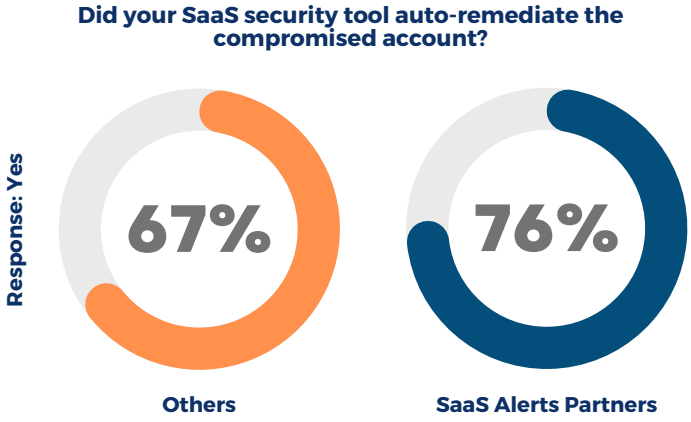


Figure 13

SaaS Alerts Partners Enjoy Significant Advantages Cont.

Predictably, in light of numbers like that, SaaS Alerts users have more confidence about security than others, and by remarkably consistent percentages. Some 67% of them rate their confidence in the ability of their SaaS security solution to protect customers between 7 and 10 on a 1-10 scale, for example, versus 53% of other survey respondents. (See Figure 14.)

By a nearly identical margin (66% to 52%), SaaS Alerts' users have higher confidence in the effectiveness of their entire security stack too. (See Figure 15.)

As one would expect, given the trust they have in their tools, SaaS Alerts partners have more trust in themselves as well. Two-thirds of them, in fact, score their confidence about safeguarding customers from threats generally and cloud application threats specifically 7 or higher, versus half of users on other platforms. Significantly far fewer SaaS Alerts partners than others rate their confidence just 1-3 too. (See Figure 16.)

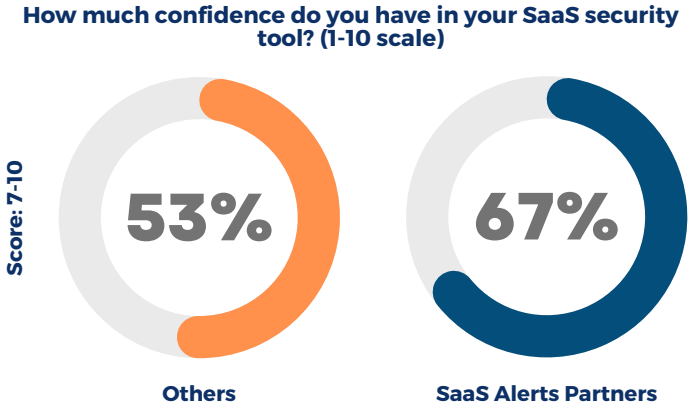


Figure 14

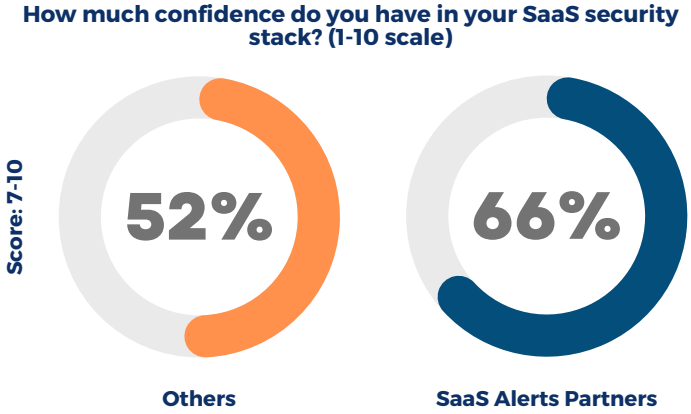


Figure 15

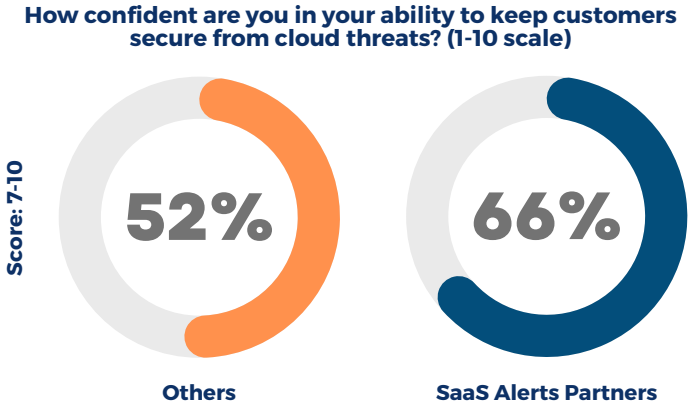


Figure 16

SaaS Alerts Partners Enjoy Significant Advantages Cont.

Unsurprisingly, given that they have better tools and more security-related confidence, SaaS Alerts partners are outgrowing others. Three-fourths of them expect to increase MRR in 2024 and 73% expect to increase security MRR. By comparison, 64% of MSPs who don't use SaaS Alerts anticipate higher MRR this year and 66% predict higher security MRR. (See Figures 17 and 18.)

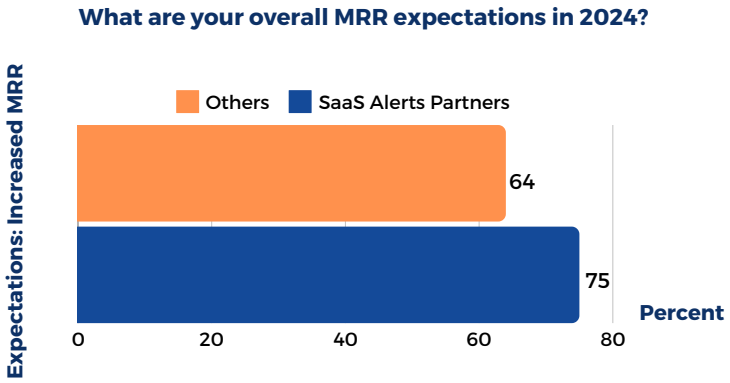


Figure 17

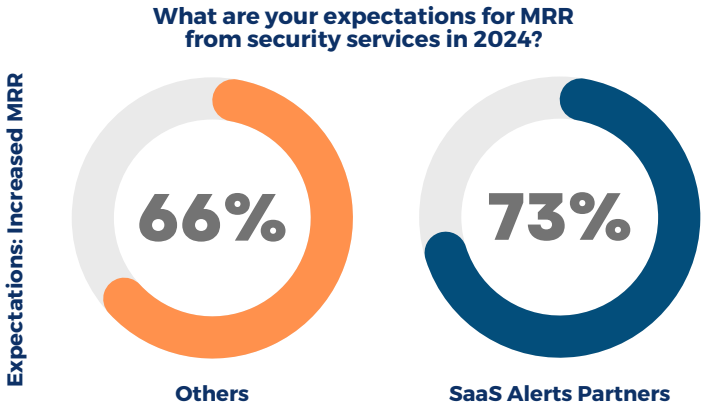


Figure 18

Conclusion

For anyone who supports the technology needs of small and midsize businesses, software as a service is no longer tomorrow's technology. It's today's mainstream application delivery model.

It's also, as this report makes clear, both a major security opportunity and a costly operational headache. On the plus side:

- More than two-thirds of MSPs expect their security-related monthly recurring revenue to increase in 2024.
- Almost two-thirds of MSPs collected at least $50,000 of incremental MRR from offering SaaS security in the prior year.

On the less helpful side:

- 38% of MSPs call cloud vulnerabilities one of the top security threats their clients face.
- Ransomware and phishing attacks, cited by 40% of MSPs each, were the only two dangers to rank higher than cloud security threats, and a mere 32% named ransomware as a top-three threat.
- 45% of MSPs currently spend at least five hours a week on SaaS security monitoring and management, and 20% dedicate at least 10 hours.
- That amounts to an estimated $13,520 a year for an MSP devoting eight hours a week to this task.

MSPs armed with tools designed specifically to address SaaS security challenges are better positioned than others to mitigate those burdens, however. More specifically, our data shows that SaaS Alerts partners:

- Have significantly fewer account compromises than other MSPs.
- Are significantly more likely to anticipate higher MRR this year.
- Are significantly more confident about their security toolset and ability to keep clients secure.

By extension, this report suggests, MSPs *without* a true SaaS security solution like SaaS Alerts in their stack are doing their customers and themselves a costly disservice.

A Message from Jim Lippie

CEO | SAAS ALERTS

At SaaS Alerts, we recognize a significant shift in cybersecurity—from a device-centric, on-premise focus to one that prioritizes user behavior and account security. We developed SaaS Alerts to help MSPs not only navigate this transition but thrive, by enhancing both their cybersecurity capabilities and profitability. Our goal is to enable MSPs to protect customers against evolving threats while driving consistent MRR growth.

This report provides clear third-party validation: MSPs using SaaS Alerts are markedly more effective at securing cloud environments than those who aren't. Our partners experience greater confidence in their security stacks and services, along with higher MRR. They expect their revenue from security services to continue growing in the years ahead.

If you're not yet using SaaS Alerts, we'd welcome the opportunity to show you how our platform can help you achieve these same results. We're ready to connect whenever you are.

Jim Lippie
CEO
SaaS Alerts

This report provides clear third-party validation: MSPs using SaaS Alerts are markedly more effective at securing cloud environments than those who aren't.

Jim Lippie
CEO
SaaS Alerts

The 2024 *State of SaaS Security Report* was prepared for SaaS Alerts by Channel Mastered, and written by Rich Freeman.

About Rich Freeman

Rich Freeman is Channel Mastered's chief content officer and channel analyst. One of the tech industry's most experienced, respected authorities on the SMB channel, Rich writes Channelholic (www.channelholic.news), a blog that delivers an insider's take on managed services, cloud computing, cybersecurity, and more. He's also both founding editor and former executive editor of The ChannelPro Network.

About Channel Mastered

Our team of multi-award-winning MSP experts help vendors build successful channel programs that drive growth and revenue with services ranging from research and analysis of the latest channel trends to channel assessment and optimization to partner recruitment and enablement. See www.channelmastered.com for more details.

About SaaS Alerts

SaaS Alerts is a cybersecurity platform for managed service providers to detect and automate the remediation of SaaS security threats. The platform provides unified, continuous monitoring of core business SaaS applications to protect against data theft and malicious actors, including Microsoft 365, Google Workspace, Salesforce, Slack, Dropbox, Okta and Duo.

SaaS Alerts uses machine learning pattern detection to identify breaches, create instant alerts, and lock affected accounts, providing MSPs with valuable time to respond before further damage can occur. It also enables users to terminate dangerous end-user file sharing activities and automate essential security tasks, enhancing efficiency and overall client security.

Learn more at www.saasalerts.com.