DARKREADING RESEARCH

OCTOBER 2024

The State of Cloud and SaaS Security Report

Commissioned by Qualys

Qualys.

Executive Summary

The rapid adoption of cloud services and containerized applications has progressed unabated, fueled by enterprises looking to drive innovation, enhance agility, and reduce costs. This seismic shift in IT hasn't been without its challenges, however, particularly when it comes to keeping businesses and their digital assets safe from loss, theft, or compromise.

As most organizations discover early on in their cloud and SaaS transformation journeys, traditional defenses geared toward on-premises environments can quickly be overwhelmed by cloud- and SaaS-centric challenges, such as a lack of visibility, unique identity and access management requirements, critical configuration management issues, sophisticated threats, and the need for additional targeted security resources to deal with all of the above.

New research commissioned by Qualys and conducted by Dark Reading shines new light on the various ways information security professionals are coping — or struggling — with the difficulties and nuances of safeguarding cloud and SaaS assets, including measuring, communicating, and eliminating cyber risk in the cloud. The data shows in stark relief the real-world challenges defenders face when it comes to shoehorning traditional security practices and methods — things like managing configs and vulnerabilities, controlling access, and corralling siloed security tools — into the defenses of dynamic multi-cloud and multi-SaaS environments.

The research underscores the importance of a comprehensive, unified, strategic approach to cloud and SaaS security that brings together continuous scanning and vulnerability assessment, automated remediation efforts, AI-powered threat detection and response capabilities, and cross-platform risk prioritization features. In this report, we also share actionable recommendations for improving cloud security posture, addressing common misconceptions, and promoting a focused, holistic approach to cloud and SaaS security in hybrid environments at enterprise scale.

In all, the Qualys State of Cloud and SaaS Security report represents a practical resource for security professionals as they navigate the evolving threat landscape, look to de-risk their organizations, and enhance their cloud and SaaS security posture.

Key Findings

- **Ubiquitous and complex:** Most organizations polled (57%) use two to three cloud service providers, and 58% have at least five corporate-wide SaaS applications deployed. To secure this complex environment, the majority (60%) must manage and reconcile outputs from two or more separate cloud and SaaS security tools — a task they find challenging and suboptimal.

- **Under siege:** More than 1 in 4 respondents (28%) admitted their organizations had been the victim of a cloud- or SaaS-related data breach in the past year; more than one-third of those victims said they'd been hit multiple times in the past 12 months.

- **Attacks are relentless:** Moving data and applications to the cloud and adopting SaaS come with a whole set of risks. Enterprises are worried about threats such as account hijacking, phishing, ransomware and malware, data exfiltration, advanced persistent threats, and distributed denial-of-service attacks.

- **Sleepless nights:** Professional defenders singled out cost (54%), system reliability and performance (36%), and limited cloud-specific security staff skills (27%) as the cloud and SaaS issues that concerned them the most.

- **Config chaos:** One place just about all parties find common ground when assessing cloud and SaaS risk is in the thorny issue of misconfigurations, one of the top concerns for both cloud (24%) and SaaS (33%). The level of concern, however, appears to fall well short of the scope of the actual misconfiguration problem in the wild.

- **Situational blindness:** Few enterprises engage in ongoing or continuous assessment of their cloud and SaaS environments. The rest do security assessments at intervals that range largely from once a quarter (18% for cloud, 11% for SaaS) to once a year (25% cloud, 26% SaaS), and in some cases not at all.

- **Difficulty patching:** Enterprises are also concerned about adversaries exploiting unpatched vulnerabilities in web applications (39%) and cloud environments (23%). Almost 1 in 5 say they have difficulty applying security updates and patches, creating a situation where organizations are exposed to attack as a result of exploitable vulnerabilities.

- **Sluggish response:** Topping the list of IR concerns are a lack of skilled workers (49%), limited visibility into cloud and hosted environments (46%), and the inherent complexity of cloud-centric incidents (46%).

Cloud Adoption: Expanding Systems, Growing Threats

The adoption of cloud services and SaaS applications continues to surge among enterprises, driven by the need for flexibility, scalability, and cost efficiency. This trend is reshaping the IT landscape, presenting both opportunities and challenges for IT departments and the security teams tasked with defending the organization's digital assets.

According to Gartner, worldwide spending on public cloud services at large is expected to grow more than 20% to a whopping $679 billion this year, up from $564 billion in 2023. That growth is driven not only by traditional business needs, but also because of the rapid adoption of emerging tech like automation, IoT "smart" systems, and most notably of late, generative AI.

More than one-third ($244 billion or 36%) of Gartner's estimated total cloud spend is attributed to SaaS. The torrid adoption of hosted business productivity and collaboration apps that began in earnest during the pandemic has now morphed into a drive toward high-powered, AI-enabled SaaS products. That adoption spike shows few signs of subsiding at least for the next five years, analysts note.

Consequently, cloud ubiquity — and complexity — is evident throughout our research. The majority of infosec professionals we polled (57%) say they work in organizations supporting two to three separate cloud service providers. Similarly, 58% of those polled have at least five corporate-wide SaaS applications deployed; **33% have 10 or more.**

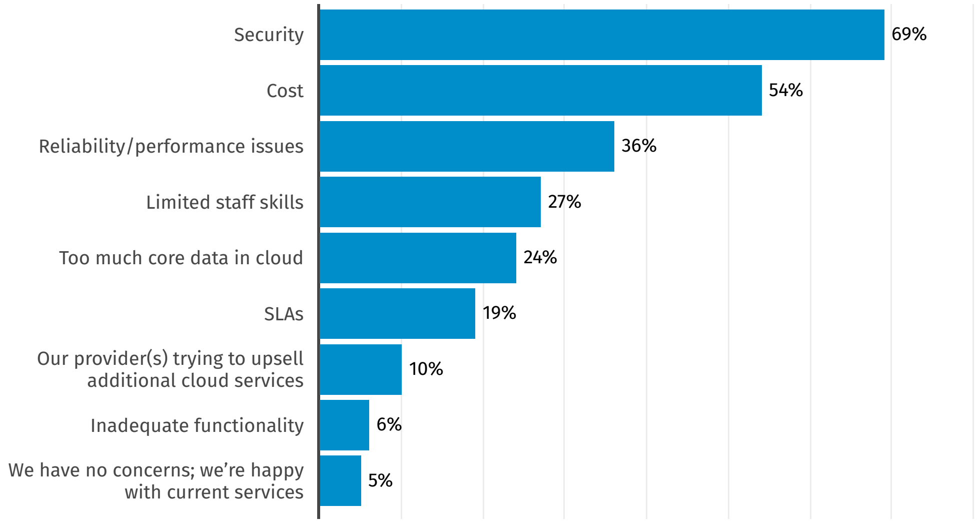
In defense of these systems, the typical security organization claims specific cloud security methodologies for data protection (55%), threat detection and response (51%), and identity and access management (51%). The commitments trail off, however, when it comes to security posture management for cloud and SaaS, where only about 1 in 3 has a specific security approach. Applications development, as we'll explore further later in this report, is even further down the priority list, with just 26% claiming formal app containerization and Kubernetes security efforts.

The ramifications for managing multi-platform and hybrid systems complexity are well established. As capable as they are at driving productivity, efficiency and innovation, multi-cloud and hybrid cloud environments come with their fair share of cyber risk. Defenders in such environments need to be keenly aware of issues like:

Figure 1

CONCERNS ABOUT CLOUD SERVICES

Looking ahead, what are your biggest concerns about your company's use of cloud services?



Note: Maximum of three responses allowed
Data: Dark Reading survey of 101 cybersecurity and IT professionals involved in securing cloud environments, March 2024

- **Increased attack surface:** With more assets in the cloud, the attack surface expands, providing a proliferation of entry points for malicious actors and potential threats.

- **Management complexity:** Keeping tabs on security across multiple cloud platforms and on-premises systems ramps up the complications — and the headaches. Each platform can have different security controls and requirements, making unified management challenging at best.

- **Misconfigurations:** Cloud misconfigurations are a common issue and can lead to significant vulnerabilities. The difficulty of keeping configurations in check across diverse environments heightens the risk of errors, compromise, data loss, and more.

- **Identity and Access Management (IAM):** Ensuring proper IAM across multiple environments is crucial. Just like botched configs, unauthorized access is a quick path to systems compromises and data breaches.

- **Advanced threats:** The presence of advanced malware, ransomware, and other cyber threats in cloud environments requires its own unique blend of sophisticated detection and response capabilities, something that on-prem focused security teams can struggle with.

Given this cautionary roster, when considering their cloud and SaaS app exposure, "security" writ large is the top concern (69%) among the security professionals we surveyed (Figure 1). Little surprise there. How that concern manifests, however, reveals the specific infosec pain points these defenders are coping with as they try to address the morass of cloud and SaaS issues.

Respondents singled out cost (54%), system reliability and performance (36%), and limited cloud-specific security staff skills (27%) as the cloud and SaaS issues that concerned them the most. A smaller but still significant 1 in 4 (24%) felt their organizations risked putting too much critical data in off-premises cloud and hosted environments.

It seems like many companies are underfunded, understaffed, and staring down a litany of known risks inherent to this new world order of multi-cloud and hybrid environments. Security leaders aren't denying the problems, but they aren't coping with them very effectively either (as we'll see throughout the report). They need help. They need AI-enhanced, automation-driven force multipliers that can bring cloud- and SaaS-specific scanning, assessment, and controls management together with their existing security infrastructure. And, with systems expanding and corresponding threats exploding, they need it now.

Corralling Risk in the Complex World of Cloud and SaaS

As cloud and SaaS adoption rises, so too does risk. The dynamic nature of most hosted environments, coupled with their broad attack surfaces, make them attractive targets for malicious actors.

In fact, more than a quarter of the respondents in our survey (28%) admitted their organizations had been the victim of a cloud- or SaaS-related cybersecurity incident in the past year; of those data breach victims, nearly 4 in 10 (36%) said they'd been hit multiple times in the past 12 months.

Because of such clear and present danger, today's infosec professionals in cloud-centric or hybrid environments expend much blood and treasure staring down threats like:

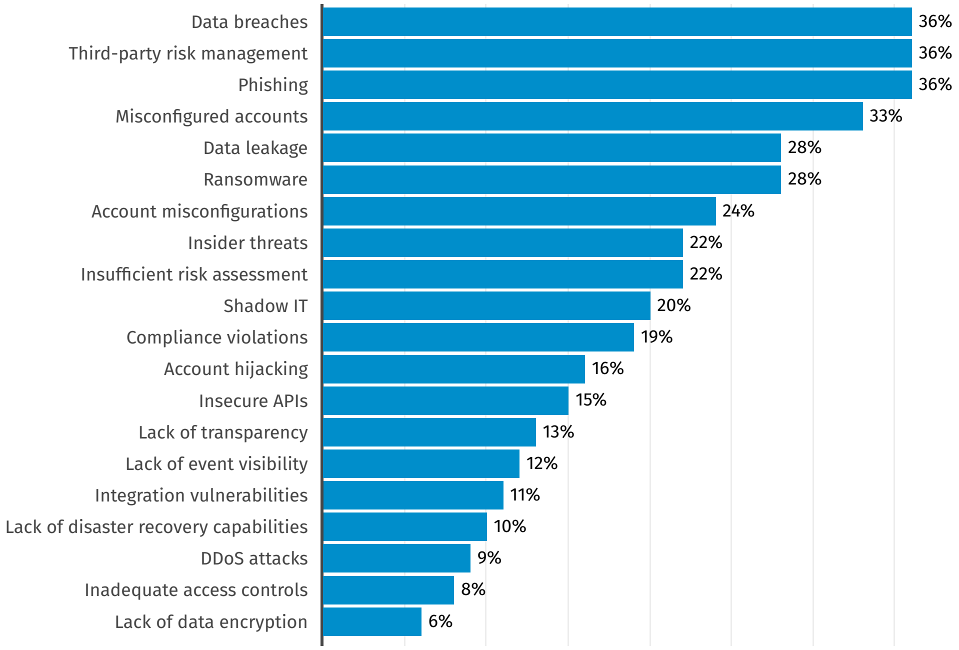
- **Phishing and Social Engineering** (36% saw this as a top SaaS risk): Attackers use deceptive emails, messages, and websites to trick users into revealing sensitive information or downloading malicious software. In SaaS environments, where users often interact with various platforms and services, the risk of falling for phishing attacks is heightened (Figure 2).

- **Ransomware** (28% saw this as a top SaaS risk): Among defenders' biggest fears for their ability to shut down systems and generate whopping financial losses, these now commonplace attacks involve encrypting an organization's data and demanding a ransom for its release. In cloud and SaaS environments, ransomware can spread rapidly, if proper access controls and backups are not in place.

Figure 2

SECURITY RISKS TO SAAS IMPLEMENTATION

In your opinion, which of the following pose the biggest security risk to your organization's SaaS implementations today?

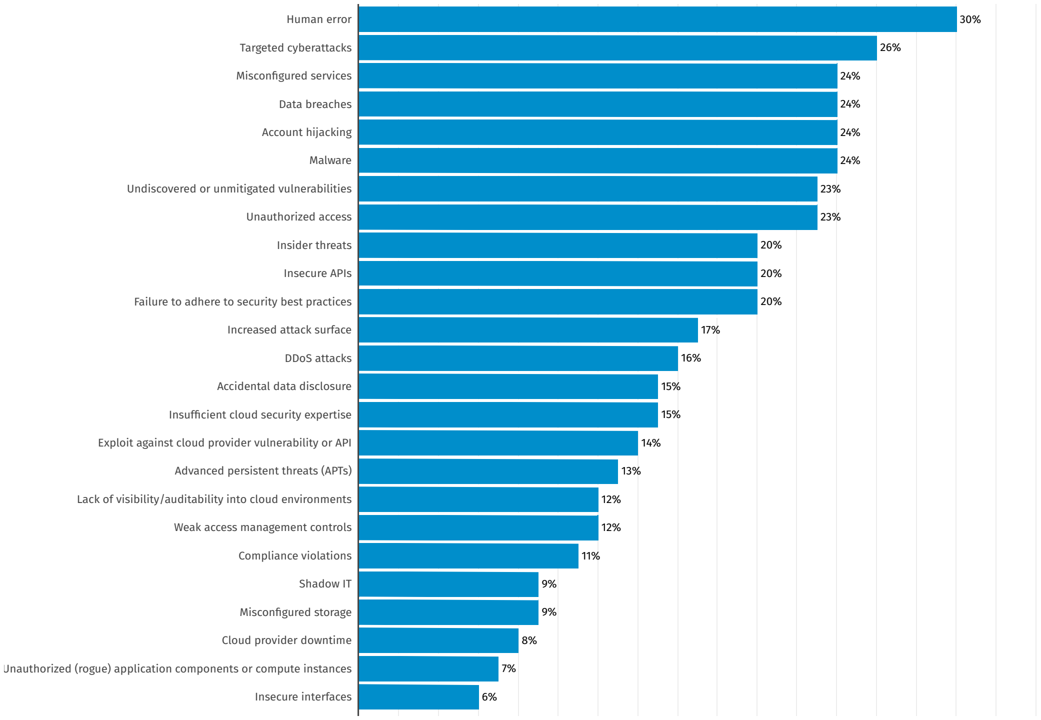


Note: Maximum of five responses allowed
Data: Dark Reading survey of 101 cybersecurity and IT professionals involved in securing cloud environments, March 2024

Figure 3

SECURITY RISKS TO CLOUD ENVIRONMENTS

Which of the following pose the biggest security risk to your organization's cloud environments today?



Note: Maximum of five responses allowed
Data: Dark Reading survey of 101 cybersecurity and IT professionals involved in securing cloud environments, March 2024

- **Targeted cyberattacks** (26% said targeted attacks were a key cloud risk, 13% picked APTs specifically): Prolonged and targeted cyberattacks — sometimes used synonymously with advanced persistent threats — or APTs — where an intruder gains access to a network and remains undetected for an extended period. These attacks are often orchestrated by well-funded and skilled adversaries, aiming to steal data or disrupt operations. Cloud and SaaS environments, with their extensive data and services, are attractive targets for APTs (Figure 3).

- **Malware** (24% saw this as a top cloud risk): Viruses, worms, trojans, and their ilk continue to be a significant threat to cloud and SaaS environments. Such malicious programs infiltrate systems through phishing attacks, compromised downloads, and other vectors. Once inside, malware can steal data, disrupt operations, and spread to other systems.

- **Account hijacking** (24% saw this as a top cloud risk): Unauthorized access to user accounts, often through compromised credentials or phishing attacks, can give attackers access to sensitive data and critical systems.

- **Data leakage** (23% said this was a top cloud risk): Thanks to the large volume of data being stored and processed, cloud and SaaS environments are particularly vulnerable to threats of unauthorized access to sensitive data. Misconfigurations, inadequate access controls, and vulnerabilities in applications can all lead to these kinds of data breaches.

- **Insider threats** (22% picked this as a top SaaS risk): Malicious or negligent actions by employees, contractors, or other trusted individuals can be particularly challenging to detect and mitigate. In cloud and SaaS environments, where access to data and systems is often widespread, insider threats can lead to data theft, sabotage, and other harmful activities.

- **API vulnerabilities** (14% said this was a key cloud concern): APIs (Application Programming Interfaces) are essential for integrating various cloud services and SaaS applications. However, they can also introduce vulnerabilities that could allow attackers to bypass authentication, access sensitive data, and manipulate services.

- **Rogue applications/instances** (7% felt this was a top cloud risk): The best example of rogue instances is the dreaded cryptojacking, the unauthorized use of an organization's computing resources to mine cryptocurrency. In cloud environments, where on-demand resources are flexible and scalable, crypto-mining can quickly consume copious amounts of computing power, leading to degraded performance and increased costs.

Clearly security practitioners in our research see risk assessment and defense of cloud and SaaS assets as related — but different — challenges. Their top cloud security risk concerns include issues like human error (30%), targeted cyberattacks (26%), and, to a lesser degree malware and account management controls. For SaaS assets, security pros mainly worry about data breaches, third-party risk management, and phishing (36% each).

The story gets a little more nuanced when we look at SaaS issues through the lens of organization size. Smaller organizations (under 500 employees) say phishing is the top SaaS concern, while corralling third-party risk tops the list for large companies. This demonstrates how organizations evolve from a smaller, less mature security posture where basics like user awareness training are lacking, to more mature environments where the problems shift to complexity, sprawl, and management of connected systems both inside and outside of the organization.

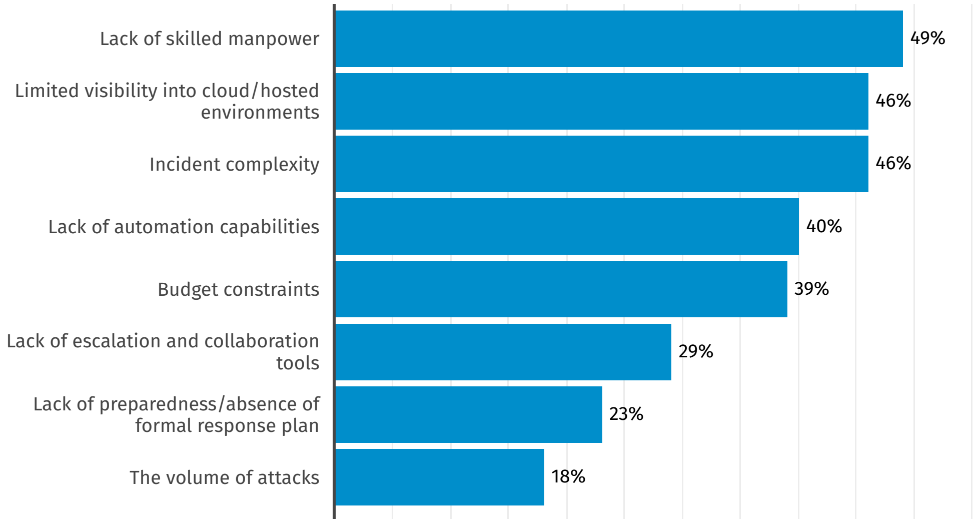
Misconfigurations Get Short Shrift

Where just about all parties find common ground when assessing Cloud and SaaS risk, however, is in the thorny issue of misconfigurations, a top five worry on both cloud (24%) and SaaS (33%) lists for organizations of all sizes. That level of concern doesn't match the scope of the misconfiguration problem in the real world, however. According

Figure 4

CHALLENGES WITH CLOUD SECURITY INCIDENTS

What are the biggest challenges your organization faces when responding to security incidents that involve cloud or hosted assets?



Note: Multiple responses allowed
Data: Dark Reading survey of 101 cybersecurity and IT professionals involved in securing cloud environments, March 2024

to the 2023 Qualys TotalCloud Security Insights report based on anonymized telemetry pulled from the Qualys TruRisk Platform, nearly two-thirds of monitored production systems across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) fail basic Center for Internet Security (CIS) configuration benchmarks.

Poorly configured cloud services and configuration errors on SaaS accounts are at the heart of many recent high-profile attacks, hence the heightened concern.

Botched configurations can include unrestricted outbound access, disabled logging, missing alerts, exposed access keys, overly permissive account credentials, poor network segmentation, open storage buckets and improperly de-commissioned assets.

Infamously in 2019, it was a web application firewall misconfiguration that allowed an attacker to compromise a major bank's AWS cloud infrastructure exposing sensitive data from S3 buckets on 100 million customers over several months. The breach cost the company $150 million in recovery costs, $80 million in fines, and an untold amount in reputational damage.

When Things Go Wrong in the Cloud

Faced with a crisis like the banking incident, most of those surveyed (52%) said they would share the immediate response duties with the cloud or SaaS provider. But that doesn't mean they feel good about their DFIR capabilities overall.

Most said they feel poorly positioned to respond to cloud- and SaaS-related incidents. Topping the list of IR concerns are a lack of skilled security workers (49%), limited visibility into cloud and hosted environments (46%), and the inherent complexity of cloud-centric incidents (46%) (Figure 4). Equally important, 4 in 10 cite a lack of automation capabilities as their biggest cloud IR challenge.

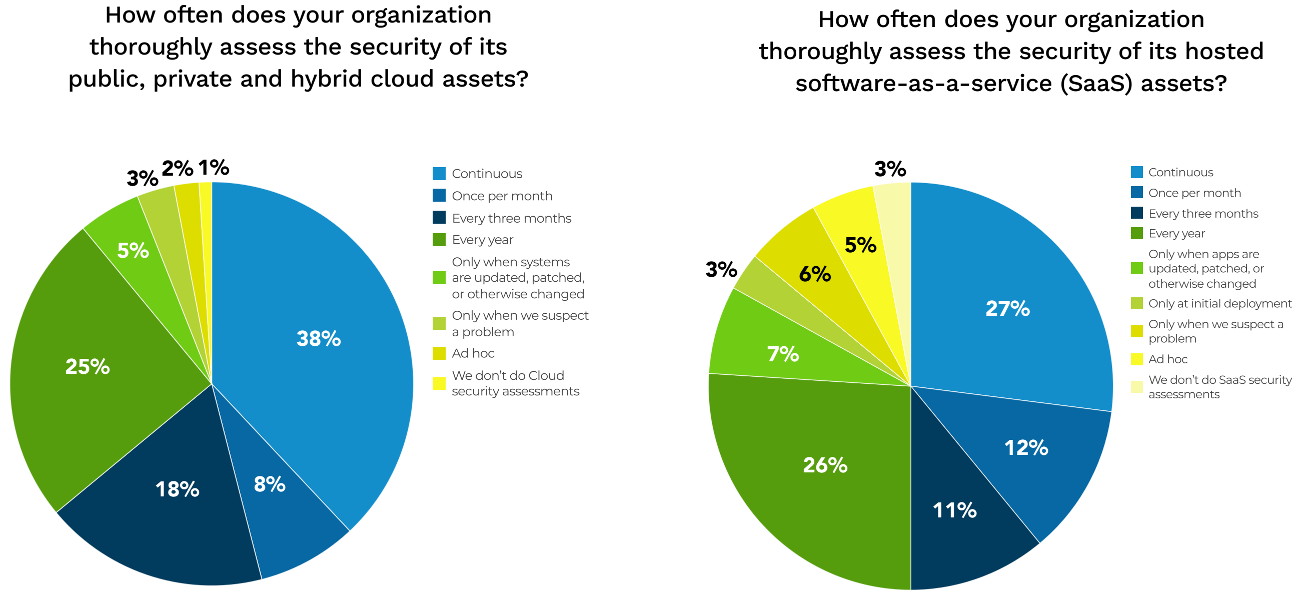
That automation piece is important. Particularly in response to cloud-centric incidents, automation can be the force multiplier that helps defenders overcome not only a lack of human and budgetary resources but also the challenges of systems complexity as well.

Tactical View: The Blocking and Tackling of Cloud Defense

Earlier, we noted that today's practitioners desperately need help to untangle the cloud and SaaS

Figure 5

FREQUENCY OF ASSESSING CLOUD SECURITY



How often does your organization thoroughly assess the security of its public, private and hybrid cloud assets?

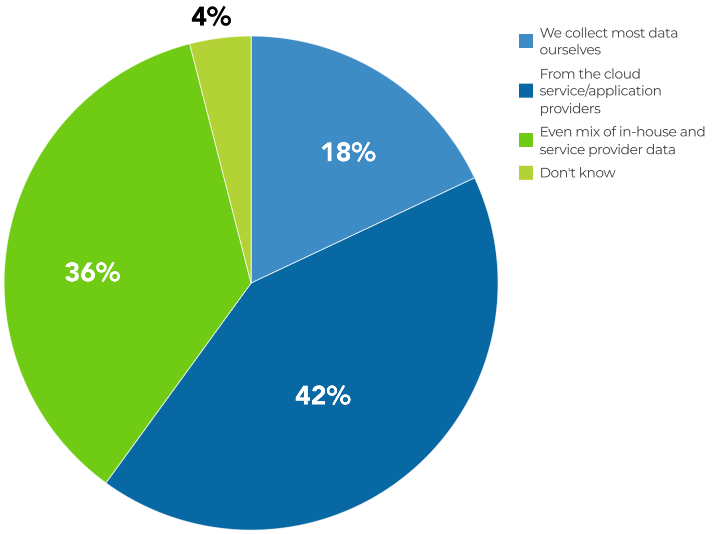
How often does your organization thoroughly assess the security of its hosted software-as-a-service (SaaS) assets?

Data: Dark Reading survey of 101 cybersecurity and IT professionals involved in securing cloud environments, March 2024

Figure 6

EVALUATING SECURITY OF DATA IN THE CLOUD

Where does your organization get the telemetry it needs to evaluate the security of its data residing in the cloud?



Data: Dark Reading survey of 101 cybersecurity and IT professionals involved in securing cloud environments, March 2024

security snarl. How much help do infosec teams really need? Quite a bit, the data suggests.
It starts with visibility. Or lack thereof.

The cadence for assessing the security of cloud assets and SaaS implementations is woefully inadequate, the research reveals. Only a scant minority of respondents engage in ongoing or continuous assessment of their cloud and SaaS environments. The rest do security assessments at intervals that range largely from once a quarter (18% for cloud, 11% for SaaS) to once a year(25% cloud, 26% for SaaS), and in some cases, not at all (Figure 5).

It is critical for diligent scanning to be an integral part of effective vulnerability management, particularly in the cloud where threats are continuously evolving, even as cloud and SaaS features and functions change rapidly. This sporadic approach to assessments leaves long gaps during which vulnerabilities can go undetected and unaddressed, affording attackers ample opportunity to exploit weaknesses.

It bears stressing: The dynamic nature of cloud and SaaS environments means new vulnerabilities emerge all the time, due to constant updates, configuration changes, and evolving threat landscapes. Quarterly or annual assessments will never be enough to keep pace with such changes.

Without continuous monitoring and comprehensive, unified, AI-enhanced, and real-time detection to expose active exploits and malware, enterprises risk damaging — and mostly preventable — data breaches, unauthorized access, and other cyber-chaos. To maintain robust security, enterprises must adopt continuous security assessment practices that can provide real-time insights and enable swift response to emerging threats.

And to get a complete picture of one's cloud risk, not only does scanning need to be ongoing, it also needs to be multifaceted. That means a combination of API-based, agent-based, network-based scanning, and snapshotting , in order to cover all of the potential weak spots across the environment.

Data Sources and Cross-Platform Reconciliation

Security teams trying to evaluate the security of data residing in the cloud and hosted assets need access to telemetry, but there is a divergence in opinion on who provides that information. While 42% of those surveyed are wholly reliant on the CSP or SaaS providers for telemetry, 18% say they collect the bulk of the necessary security data on their own (Figure 6). Thirty six percent share the responsibility with the providers.

To secure the systems that comprise their complex multi-cloud, multi-SaaS environments, the majority (60%) continue to rely on two or more different tools to safeguard cloud and SaaS assets. Unified risk assessment and prioritization across all hybrid/multi-cloud digital assets is treated in much the same way. Forty percent of those polled use a separate tool to reconcile cross-platform risk, while 29% say they forego risk reconciliation altogether and continue to treat on-premises, cloud, and SaaS environments as discrete security silos.

The increasing complexity of modern IT environments necessitates a unified approach to security management. Treating on-premises, cloud, and SaaS environments as discrete silos or using separate tools to reconcile risk can lead to significant security gaps, inefficiencies, and higher costs. By adopting a unified security strategy, enterprises can achieve comprehensive visibility, consistent policy application, streamlined incident response, and cost savings, ultimately enhancing their overall security posture and resilience against cyber threats.

Web Apps and DevOps: The Other Cloud Conundrum

Cloud and SaaS security isn't just about other people's systems and apps. Most enterprises today — and even many smaller organizations — are busy churning out their own cloud assets in the form of bespoke, in-house web applications.

And where web apps go, cloud security complications are sure to follow.

Industry analysts generally put the share of production web apps with critical, undiscovered, or unpatched security flaws at between 80% and 90%. The most common blunders are broken access controls, encryption errors, misconfigurations, the use of vulnerable, outdated open-source components, cross-site scripting flaws, SQL injection flaws, logging and monitoring failures, and the list goes on.

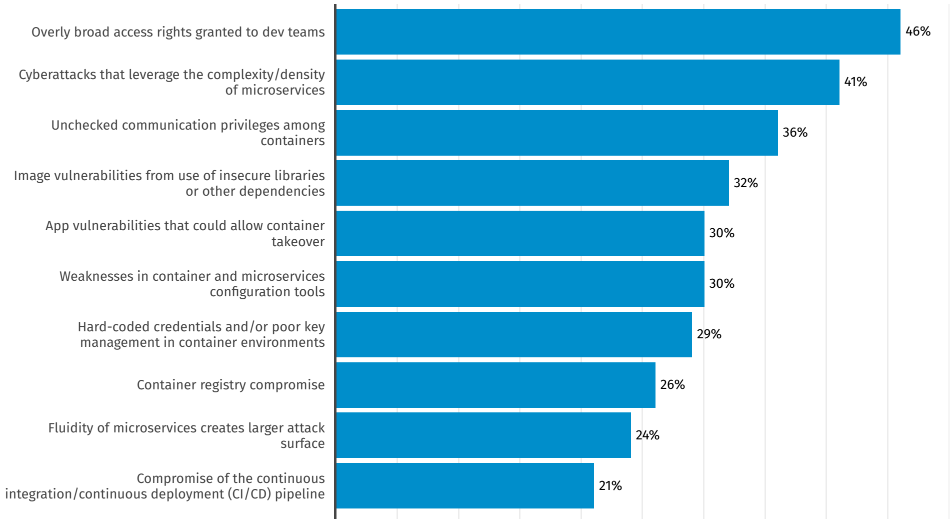
Most respondents we surveyed (68%) work in organizations where in-house applications development relies on the use of app containers and microservices, a specific discipline within cloud security that demands its own unique set of security controls and methods.

With that framework, security professionals say they're most concerned with the granting overly broad access rights to dev teams (46%), the difficulty of defending against attacks targeting the complexity of application microservices (41%), the proliferation of communication and authentication privileges among app containers (36%), and the spreading

Figure 7

APP SEC CONCERNS REGARDING CONTAINERIZATION

What are your top application security concerns in a containerization and/or microservices AppDev environment?



Base: 68 respondents who use containers and microservices frequently, infrequently, or plan to start using this year
Note: Multiple responses allowed
Data: Dark Reading survey of 101 cybersecurity and IT professionals involved in securing cloud environments, March 2024

of vulnerabilities through corrupt images, libraries, and other dependencies (32%) (Figure 7).

Earlier, we noted that exploits targeting APIs was a cloud/SaaS risk concern for around 15% of respondents. That's a worry that carries over to DevOps, where single page and low- code/no-code applications today increasingly rely on APIs over traditional web pages, making app traffic much more difficult to monitor and secure, and rendering many aspects of SAST and DAST testing obsolete. The rise of APIs presents both opportunities and challenges in today's hyperconnected digital world. APIs are integral to digital transformation initiatives across industries. The latest data indicates that over 83% of web traffic now comprises API traffic, highlighting their critical role in modern web applications using microservices, cloud, and hybrid environments. However, this also underscores the vulnerabilities that accompany their widespread adoption. This rapid increase in API usage expands the attack surface, making effective API security solutions more crucial than ever.

However, securing APIs for the modern application development world comes with its own set of challenges. Discovering all APIs across various environments — hybrid, multicloud, and others — remains a significant challenge due to the complexity and diversity of modern IT architectures. Forrester's 2024 predictions highlight the difficulty of managing API security without comprehensive visibility into the API inventory, given that an average enterprise has over 300 APIs.

Looking Ahead

The rising complexity of managing multi-cloud and multi-SaaS environments clearly requires a unified security approach that covers all parts of the IT ecosystem wherever they reside, be it on-premises, in the cloud, or delivered via a third-party host as a service. Such a comprehensive strategy is now critical to safeguarding modern businesses. To enhance security posture, organizations should consider:

Implementing continuous monitoring and assessment: Enterprises should move away from periodic assessments and adopt continuous security monitoring to identify and mitigate threats in real time. Continuous assessment helps in promptly detecting vulnerabilities that emerge due to constant updates and configuration changes in cloud and SaaS environments.

Adopting a unified security platform: Using a single, integrated security platform to manage all aspects of security across on-premises, cloud, and SaaS environments is crucial. A unified platform provides comprehensive visibility, streamlined security operations, and consistent policy enforcement, hence reducing the risk of security gaps and inefficiencies wherever they occur.

Enhancing identity and access management (IAM): Proper IAM practices are essential for securing access to sensitive data and systems, especially in cloud and hosted systems. Enterprises need robust IAM solutions that include multi-factor authentication, least privilege access, and regular access reviews to prevent unauthorized access and minimize insider threats.

Leveraging automation for security processes: Automating security processes such as vulnerability scanning, patch management, configuration and change management, and incident response significantly improves operational efficiency and reduces risk of human error. Automation especially empowers under-resourced security teams — that means most of them — to quickly address threats and maintain a mature, proactive security posture.

Investing in advanced threat detection and response capabilities: To combat sophisticated threats such as advanced persistent threats (APTs), ransomware, and next-gen malware, enterprises should invest in AI-powered threat detection and response solutions. These advanced capabilities enable organizations to detect and respond to threats swiftly, minimizing potential damage.

Wrapping Up

The adoption of cloud services and SaaS applications presents both opportunities and challenges for enterprises. As highlighted throughout this research, while the complexity of managing multi-cloud and hybrid environments necessitates a comprehensive and unified security strategy, most organizations today still struggle with the basic requirements of cloud and SaaS defense.

Organizations need to move away from periodic assessments, siloed management, and labor-intensive threat detection and response if they've any hope of effectively corralling cloud-centric risk. To that end, implementing a unified, tightly integrated, cloud-aware security platform offers the best path toward the kind of visibility and streamlined security operations leading to fewer security gaps, improved policy enforcement and enhanced security maturity.

About Qualys

Qualys, Inc is a leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings.

The Qualys Enterprise TruRisk Platform leverages a single agent to continuously deliver critical security intelligence while enabling enterprises to automate the full spectrum of vulnerability detection, compliance, and protection for IT systems, workloads and web applications across on premises, endpoints, servers, public and private clouds, containers, and mobile devices. Founded in 1999 as one of the first SaaS security companies, Qualys has strategic partnerships and seamlessly integrates its vulnerability management capabilities into security offerings from cloud service providers, including Amazon Web Services, the Google Cloud Platform and Microsoft Azure, along with a number of leading managed service providers and global consulting organizations. For more information, please visit http://www.qualys.com.

Methodology & Firmographics

Qualys commissioned Informa Tech's Dark Reading to research the current state of cloud and SaaS security posture and risk mitigation acumen at small, midsize and enterprise business organizations. The survey queried 101 cybersecurity and IT professionals familiar with their organization's cloud environments, SaaS applications, and the efforts to secure them.

The survey was conducted online in March 2024. Respondents were recruited via emailed invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database. Informa Tech was responsible for all survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing U.S. privacy laws.

Thirty-one percent of the respondents are from organizations with fewer than 100 full-time employees. Another 31% represent businesses with between 100 and 999; 27% have between 1,000 and 9,999 employees, and 11% have 10,000 or more workers.
The survey queried respondents with job titles that include IT executive titles such as chief information officer (CIO), chief information security officer (CISO), chief privacy officer, other security executive (CSO, VP Security), head of information security or cybersecurity, senior IT management, applications and DevSecOps management, corporate management, cybersecurity staff, and network administration.

Respondents' organizations represent more than 20 vertical industries including technology, government, business services, banking and financial services, healthcare, education, and manufacturing.