MITIGA

Top Security Challenges of Cloud Environments

Preparing Your Enterprise to Respond to Today's Cyber Risks

Over the past decade, cloud adoption has skyrocketed.

The global pandemic accelerated the shift. Today, enterprises continue to migrate to cloud-based offerings, supporting their operations and innovation. They're shifting towards application infrastructure services, system infrastructure services, and growing their SaaS adoption. McKinsey has projected that the cloud could generate $3 trillion in value by 2030[1].

However, as the opportunities of cloud continue to expand, so do the risks. Navigating the challenges of cloud environments has become fundamental to managing business risk and maximizing business advantage.

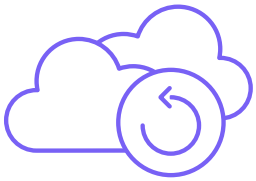
[1]Projecting the Global Value of Cloud, McKinsey Digital, November 28, 2022

Keeping up with ever-changing cloud complexity

01

Today's cloud provider marketplace is incredibly diverse: global cloud service providers (CSPs) operate side by side with start-ups supplying a vast array of niche SaaS applications, and many more providers in between. To gain the full benefits from these solutions, organizations must allow them to access and use data from other cloud and on-premises systems. In this type of environment, it's vital to have a clear view of what's available across the cloud marketplace and the related opportunities and risks. As the market expands, however, it becomes more difficult to develop a comprehensive view of the ecosystem. This lack of visibility adds to the challenges of trying to manage which applications or users have access to what, and why.

In addition, cloud solutions of all types – from global CSPs to SaaS start-ups – are on a cycle of constant change and innovation. New vulnerabilities are frequently disclosed, resulting in patches and other remediation updates. A constant stream of new features makes it more difficult for organizations to stay on top of changes or know where to focus security attention. While conducting incident investigations, we've seen cloud services evolve (for example, adding new features or changing configuration screens) during the course of a single project, changing the scope and focus of our project as well. Few organizations have the bandwidth or knowledge needed to adequately investigate an issue with a service that changes so rapidly.



Cloud solutions of all types – from global CSPs to SaaS start-ups – are on a cycle of constant change and innovation. Modern incident response needs to keep pace.

The Cloud enables faster business growth, but without IT oversight

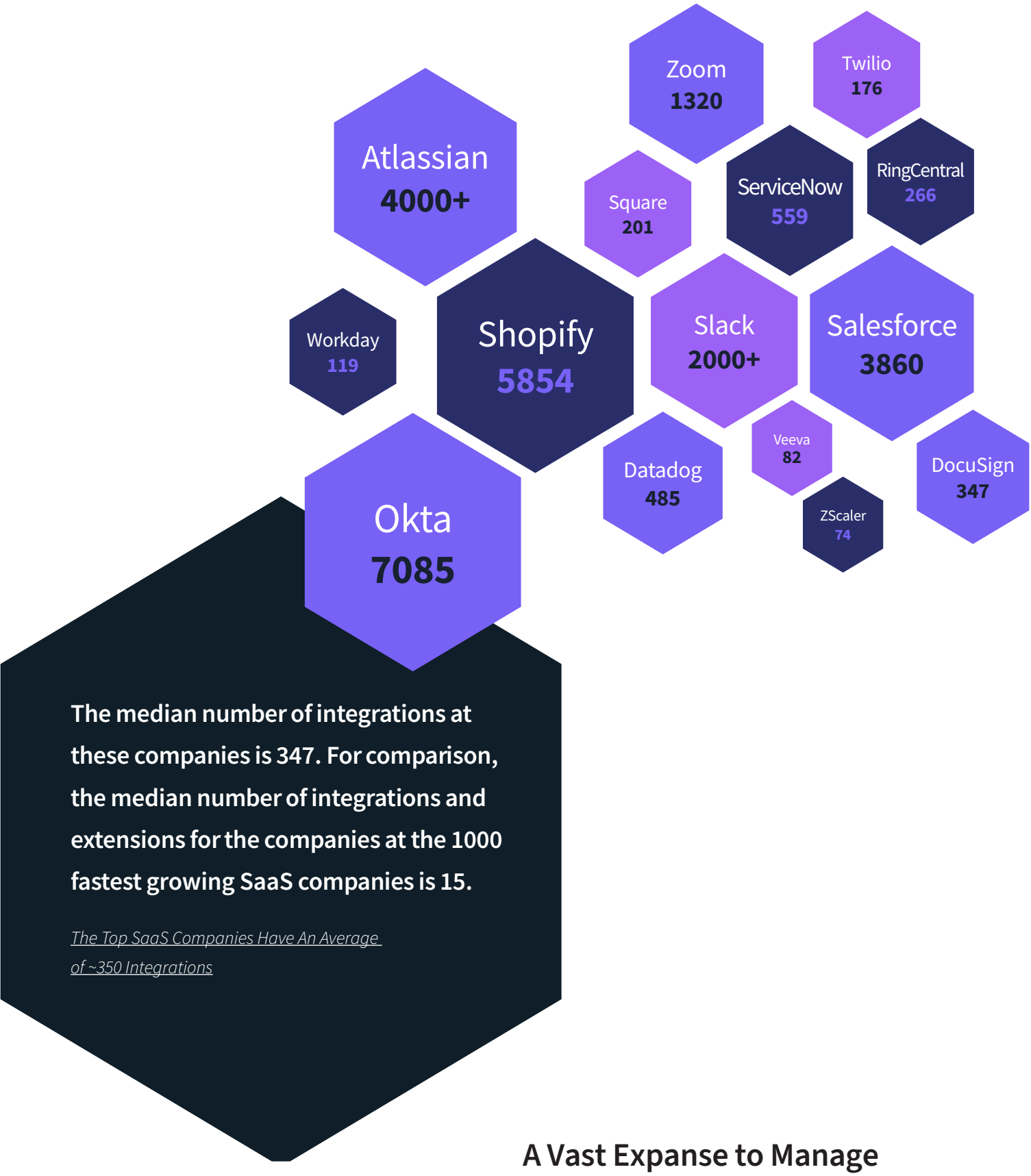
Moving to the cloud provides ready access to enterprise-grade technology for stakeholders across the business. It's also simple enough that teams can take action unilaterally, helping their organizations innovate and scale more rapidly than ever.

The growth this creates for enterprises is a tremendous advantage, but it also has a dark side. Decentralized adoption of cloud resources becomes a new type of Shadow IT, as business units spin up environments that IT and security teams have little control over.

For the most part, internal teams are unaware of the impacts of their actions. They aren't trying to cause problems. They're simply leveraging the power and functionality of SaaS and IaaS services, and they're eager to implement them as quickly as possible.

The challenge occurs because teams' objectives are focused on things like innovation and maximizing operational efficiency; security isn’t always a primary consideration. As a result, they may bypass the team responsible for reviewing, approving, and securing cloud resources.

It's this type of fast, uncontrolled expansion that is impossible for IT teams to manage effectively and, over time, puts an organization’s security posture at risk. In the cloud era, building awareness of cloud security issues and the role they play in operations is vital for all business users.



The median number of integrations at these companies is 347. For comparison, the median number of integrations and extensions for the companies at the 1000 fastest growing SaaS companies is 15.

The Top SaaS Companies Have An Average of ~350 Integrations

A Vast Expanse to Manage

Number of integrations and extensions at the 15 largest SaaS Companies

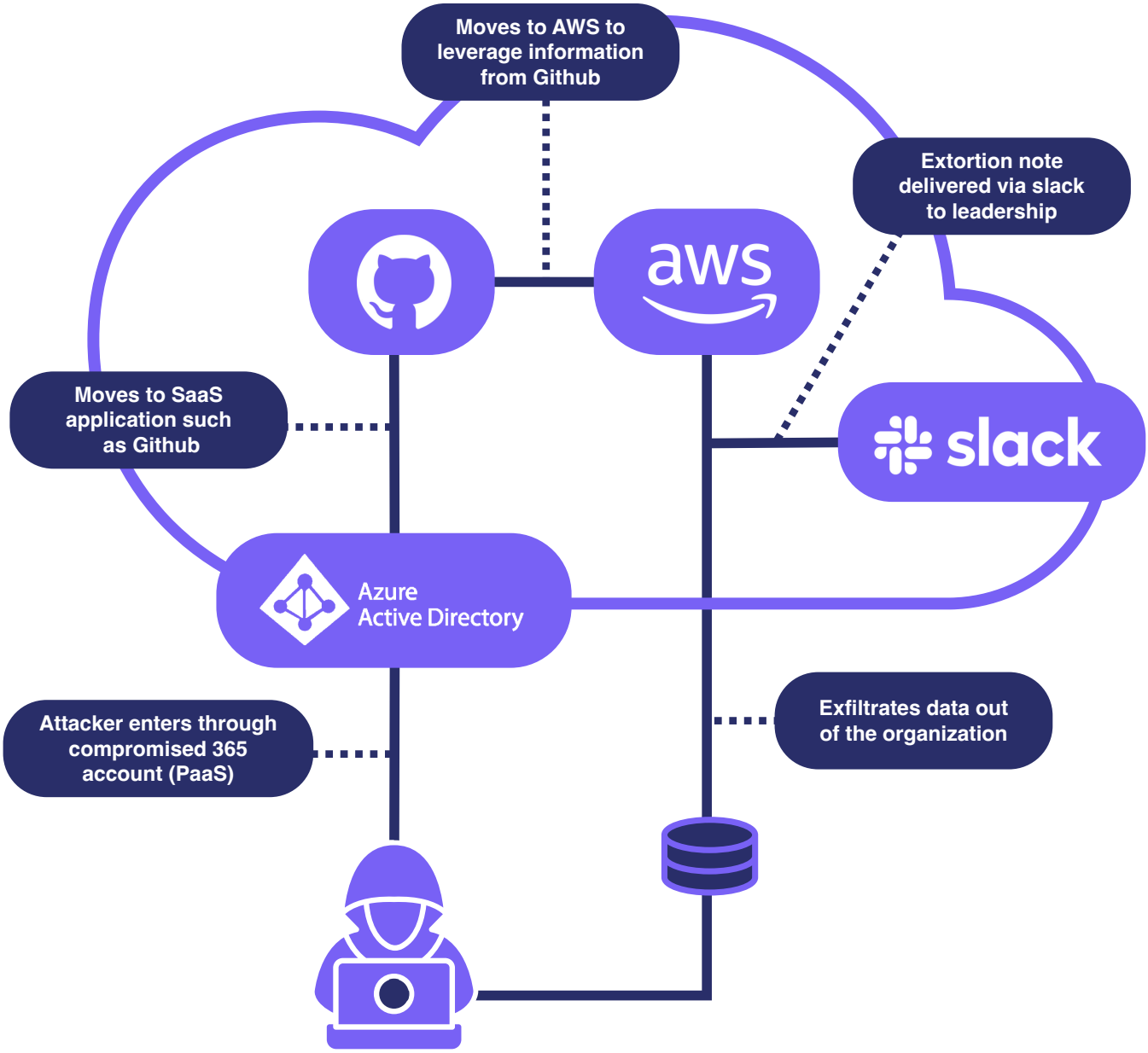
Overcoming Cloud Skills Gaps and Governance Issues

The pace at which cloud technology continues to develop makes it nearly impossible for an organization's technical team to continue expanding their skill sets to keep pace with new needs, and hiring new staff to fill the need is an uphill battle given the ongoing cyber talent gap. There aren't enough people available who are skilled at managing and securing cloud resources.

Compounding this challenge is an education gap. Many on-premises security skills aren't directly translatable to cloud environments, and there is an increasing need for security staff education and training that many enterprises aren't yet offering. As a result, acquiring cloud-specific cyber expertise can become a trial by fire as teams learn by battling and recovering from cloud attacks in real time. Most enterprises would agree that it's not the learning environment they favor. New professional development programs are needed.

Additionally, many organizations transitioned to the cloud without understanding how the new operating model would impact the ways they assess, manage, and control security risks. At Mitiga, we've worked on several cloud security projects with CISOs whose teams are still set up under a traditional IT security or information security governance model. In the majority of cases, this structure is simply not suitable for a cloud-based environment, and it may actually be counterproductive to addressing cloud security risks. Fundamental changes are needed to support transformation, including a new organizational chart for the information security function.

> **75% of IT decision-makers [are] struggling with existing skills gaps, particularly in cybersecurity and cloud related fields.**
>
> - *HelpNetSecurity: The latest trends in online cybersecurity learning and training*



A Sample Cloud-based Attack

Managing third-party risk via SaaS marketplaces and integrations

SaaS vendors tend to specialize in specific business processes, tasks, or capabilities, and then deliver them by providing the full stack of services from infrastructure to application management. There's a lot of diversity among SaaS vendors, ranging in size and capability from Salesforce.com and Microsoft 365 to small start-up providers. Increasingly, SaaS providers of all sizes provide capabilities that offer interconnected building blocks for whatever applications an organization is building. Sharing data between them, these SaaS components are now forming a new, interconnected mesh of corporate IT, bringing with it significant implications for security.

When an organization creates this new mesh of cloud and SaaS systems, the SaaS applications within it must access (and potentially hold) sensitive enterprise data as part of their core function. They also integrate into other environments, such as internal on-premises and legacy IT systems, as well as core cloud capabilities. Smaller SaaS providers also request access to central enterprise data, because that's how they deliver the best outcomes and user experiences. So, while the organization's core infrastructure may be secure, that core has many interconnections and access points managed by other SaaS applications.

This new interconnected mesh of SaaS applications accessing and sharing sensitive corporate data opens up further risks: lateral attacks. It's a term that dates back to on-prem legacy environments, when an attacker might gain access to one asset – such as a user's personal computer – and use that as an entry-point to move laterally into other assets across the organization. Today, the interconnectivity of multiple SaaS services recreates the risk of lateral movement in a modern form since an attacker can hack into one solution and then use interconnections to progress into other cloud environments.

The risks of lateral movement increase as SaaS services offer new marketplaces where third-party innovators can provide add-on capabilities. While the resulting functionality may be very useful in business terms, the risk is that organizations may be trading this enhanced functionality for downgraded security. The innovators developing these tools may be tiny companies with less mature levels of security. However, since their products integrate into a SaaS application, which in turn connects to the organization's core IT and data, they can provide an access point for attackers to move laterally into the corporate cloud infrastructure.

Such attacks made via marketplace apps are not yet the majority of attacks we see but are already accountable for some major breaches. They have already increased in both frequency and complexity at an alarming rate. In the years ahead, the trajectory of most enterprises transformers ensures that these kinds of attacks will continue to increase dramatically.

05

Ensuring timely access to forensic data

Incident response (IR) needs to change because attacks are changing. As cloud and SaaS adoption escalates, the focus for threat actors is moving from on-premises systems to the cloud. And within the cloud, they are shifting the focus of their attacks from cloud infrastructure to SaaS. To respond effectively and stay secure, organizations have no choice but to change how they think about IR.

A big part of IR is understanding what happened – a task made more complex by attackers' efforts to hide their tracks. Establishing the facts requires an investigation based on forensic data. With purely on-premises systems, all the forensics data is available on the organization's own hardware. When an incident occurs is in the cloud, however, organizations are at the mercy of what the cloud vendors can offer.

The logs externalized to users are only a subset of the overall information, and much of the forensic data may be inaccessible, or accessible only with limitations.

A key factor here is how long the vendor chooses to retain forensic data. With most cloud vendors this typically falls somewhere between 30 and 180 days. Yet industry statistics show that the average time it takes to identify a breach is 207 days, with another 70 days for containment. It's not a good match.

In fact, an organization is likely to discover that they have been breached long after all the forensic data is gone, making a thorough and rapid investigation more challenging—and sometimes impossible. Cloud requires organizations think about incident readiness and response in very different ways. In other words, the best response to your next cloud or SaaS breach starts before the breach occurs.

> **The average time taken to identify and contain a data breach is 277 days.**

Source: Cost of Data Breach Report 2022, IBM

Preparing your enterprise to meet today's cloud security challenges

As cloud and SaaS breaches continue to rise, it demands a strategic approach and a realistic assessment of your current strengths and gaps—from your tech stack to your resource allocation. Ultimately, a proactive approach that keeps today's cloud challenges top of mind is the winning one for modern enterprises.

If you would like to assess your organization's level of readiness and get on a path to growing your cloud capabilities, **talk with us.** We have expert teams dedicated to helping elevate your enterprise's cloud readiness, support cloud and SaaS incident response, and grow your cloud resilience.

Mitiga provides next-gen cloud and SaaS incident response solutions to simplify and dramatically accelerate investigation and recovery.

For more information, visit www.mitiga.io or email us at info@mitiga.io

US +1 (888) 598-4654 | **UK** +44 (20) 3974 1616 | **IL** + 972-3-978-6654 | **SG** +65-3138-3094

MITIGA