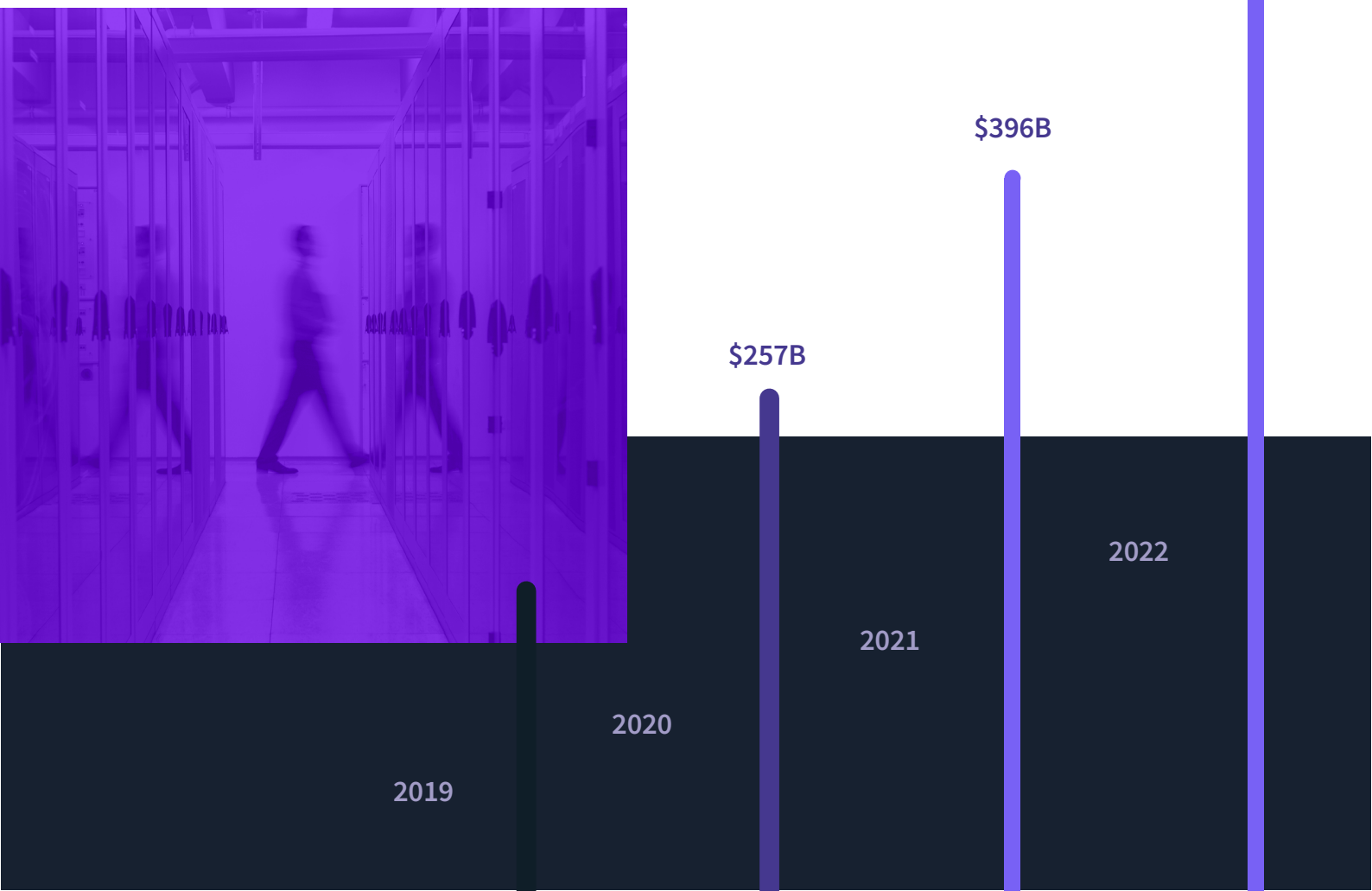
MITIGA

Top 5 New Security Challenges in Cloud Environments

Is your organization ready to handle these challenges?

In the past decade, cloud adoption has steadily increased; Gartner expected worldwide public cloud services to grow 6.3% in 2020 to $257.9 billion.

We actually saw a far faster rate of growth, and Gartner now expects spending on public cloud services to reach $396 billion in 2021 and then grow another 21.7% in 2022. The ongoing global pandemic pushed more businesses to migrate to cloud-based offerings, such as application infrastructure services, system infrastructure services, and software as a service. While the cloud helps modernize environments and improves remote work models, the evolving cloud landscape also gives rise to new challenges. To adapt quickly to new considerations in the changing cloud landscape, organizations need to address these five new security challenges in cloud environments.

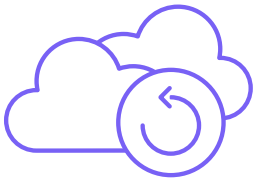


Keeping up with ever-changing cloud complexity

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.

Cloud enables faster business growth, but without IT oversight

Moving to the cloud enables faster business growth by providing businesses of all sizes with access to enterprise-grade technology. This helps them to overcome many challenges and scale quickly to meet the needs of a growing customer base. While the cloud enables this growth, it also leads to decentralized adoption of cloud resources. This essentially creates a new type of Shadow IT that IT and security teams have little control over.

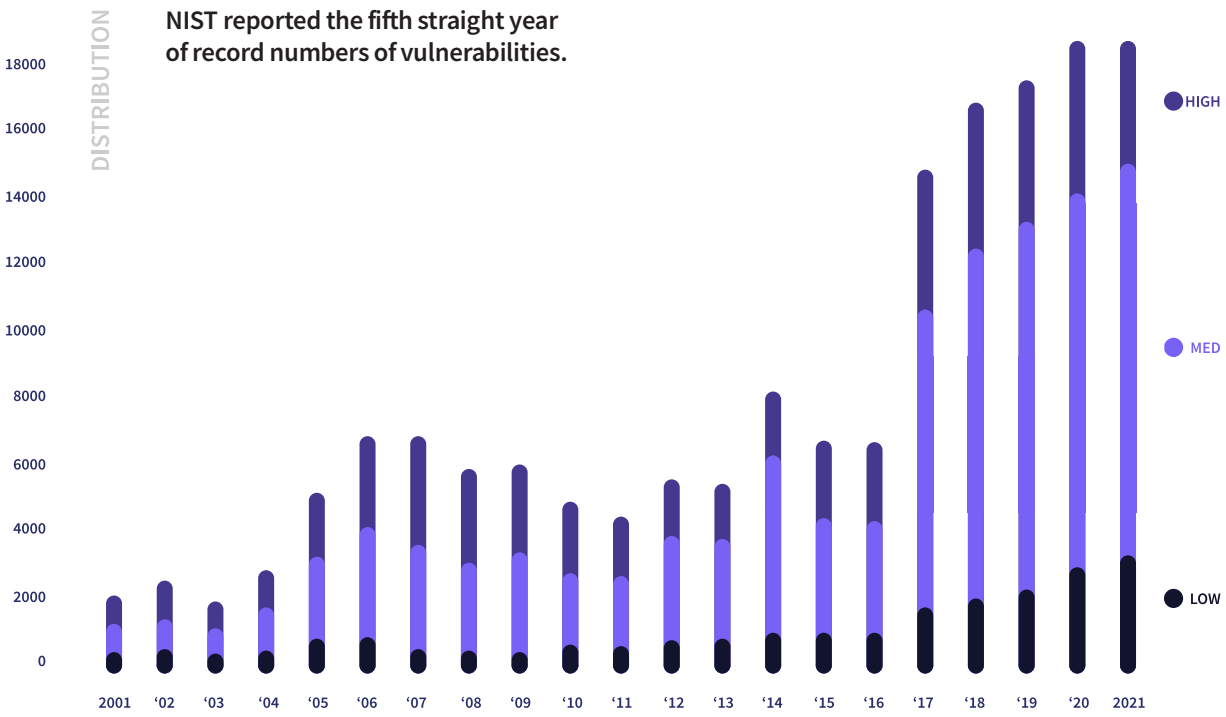
> **Cloud technology allows startups and midsize companies to access big tech capabilities — compute power, algorithms, programming tools, and architectures — and partner in an ecosystem with larger firms.**
>
> *- Harvard Business Review:* *What CEOs Need to Know About the Cloud in 2021*

Today, internal customers across an organization are increasingly aware of the power and functionality of SaaS and IaaS services and are eager to implement them as quickly as possible. Security isn't always a primary consideration for these business users, and they may bypass the team responsible for reviewing and approving those resources. This type of uncontrolled expansion is impossible for IT teams to manage effectively and puts the organization's overall security posture at risk.

As the IT security community strives to keep pace with cloud advances, increasingly pervasive usage of cloud within organizations results in new and larger risks. With the potential attack surface for cloud expanding steadily, researchers are using advanced capabilities and resources to find ways to exploit vulnerabilities. Security researchers, criminal organizations, and nation state actors alike are investing time and energy into investigating these risks. As a result, we expect the next several years to see rapid innovation, resulting in new and different types of cloud-native attacks. Very few organizations today are prepared for the attacks ahead.

CVSS Severity Distribution Over Time

This visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of ***LOW, MEDIUM*** and ***HIGH*** is based upon the CVSS Base score. For more information on how this data was constructed please **see the NVD CVSS page.**



- ZDNet: With 18,378 vulnerabilities reported in 2021, NIST records fifth straight year of record numbers

Rising skills and governance challenges

The pace at which cloud technology has developed – and continues to develop – makes it nearly impossible for an organization's technical team and their skills to keep pace with its needs. This lack of knowledge is compounded in the cloud security domain by strong demand for hard-to-acquire cyber expertise. Also, many on-premises security skills aren't directly translatable to cloud environments, increasing the need for staff education and training. Quite simply, there aren't enough people available who are skilled at managing and securing cloud resources.

The transition to cloud native environments and applications goes hand in hand with the new models for building and deploying applications, such as DevOps, which fundamentally changes many of the roles and teams in the IT and engineering groups.

To go along with these new environments and development models, we need to adopt new structures and add new security roles.

Many organizations transitioned to cloud without understanding how the new cloud operating model impacts how they assess, manage, and control security risks. 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 many cases, this structure is simply not suitable for a cloud-based environment and may actually be counterproductive in terms of addressing security risks in the cloud. Major changes are needed – 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*

Third-party risk via SaaS marketplaces and integrations

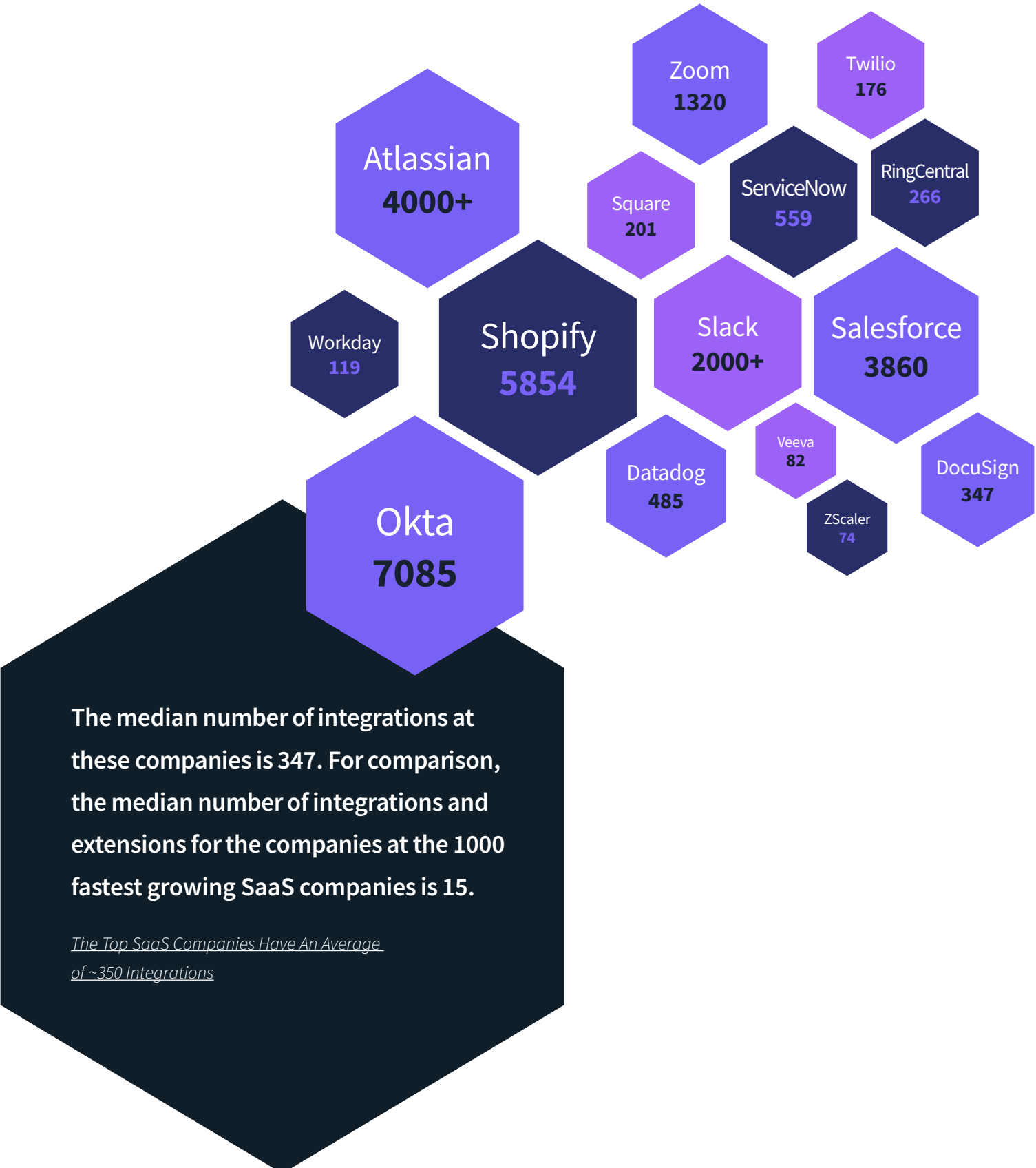
SaaS vendors tend to specialize in specific business processes, tasks, or capabilities, and then deliver them by providing the full stack of services from infrastructure to application management. There's a lot of diversity among SaaS vendors, ranging in size and capability from Salesforce.com and Microsoft 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. And in the next two or three years, we believe these attacks are going to increase dramatically.

Number of Integrations & Extensions at the 15 Largest SaaS Companies



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

Timely access to the right data

05

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 taken to discover a breach after it has occurred is 212 days.

So, in many cases, an organization might discover that there was a breach after all the forensic data is gone, making a thorough and rapid investigation much more challenging. The new realities that come with a shift to the cloud require fundamental changes in how organizations think about incident readiness and response.

> **The average time taken to discover a breach after it has occurred is 212 days.**
>
> *- IBM: Cost of a Data Breach Report 2021*

Are you ready for the new cloud security challenges?

Cloud adoption isn't slowing down, nor is the innovation that both drives and fuels the shift to cloud. Considering these security cloud challenges is an important step in making sure your organization is ready if — or when — an incident occurs in your cloud environment.

Mitiga's technology and services lower the impact of cyber breaches and optimize readiness for cloud and hybrid incidents and accelerate both response and recovery times when incidents occur. Importantly, Mitiga's readiness prioritization also increases resiliency for future incidents. Mitiga's shared-responsibility model is unique. Unlike others, who charge additional fees for incident response and recovery, Mitiga subscribers face no add-on fees.

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