Devolutions

4 Key Cloud Security Challenges in 2021 & How to Deal With Them

A SURVEY BY THE CLOUD SECURITY ALLIANCE REVEALED THAT 41% OF ORGANIZATIONS HAVE NOW SHIFTED TO CLOUD SERVICES

While drawing conclusions is difficult — and in many cases unwise — given how uncertain things have been over the last 18 months, one significant fact is indisputable: more organizations are rising to the cloud.

A survey by the Cloud Security Alliance revealed that 41% of organizations have now shifted to cloud services, which is up from 25% before the pandemic. What's more, 21% of organizations expect to move 80-100% of their workload to the cloud at some point in 2021.

Naturally, this re-focus is impacting budgets, too. A survey by Gartner found that almost all respondents plan to maintain or increase their spending on cloud computing within the next 12 months. Douglas Murray, CEO of the cloud security vendor Valtix, explains: "In 2020, spending on public cloud infrastructure exceeded on-prem for the first time. It is clear the cloud has won and is now achieving escape velocity. I don't see a slowing anywhere on the horizon."

Security in the Cloud Is Improving

A 2019 survey of around 400,000 IT professionals by cybersecurity company Coalfire found the two biggest barriers of cloud adoption were related to security; specifically: data loss and leakage (64%) and data privacy/confidentiality (62%). These findings align with separate research by the Cloud Security Alliance, in which 73% of organizations said security concerns were holding back cloud projects.

However, while there are some key security challenges that need to be identified and addressed (and which are explored further in this article), the fact remains that cloud security is significantly stronger and more trustworthy now than it was in the past. There are several reasons for this, including:

- Cloud service providers continuously monitor security and conduct penetration and vulnerability testing. This is a level of scrutiny that many organizations — especially SMBs — cannot provide. Commented Vivek Kundra, former EVP at Salesforce and current COO at Sprinklr: "Cloud computing is often far more secure than traditional computing because companies like Google and Amazon can attract and retain cybersecurity personnel of a higher quality than many governmental agencies."
- Unlike on-prem systems that primarily rely on firewalls, cloud systems deploy multiple layers of security, including AI and machine learning, to automatically get smarter.
- Data in the cloud can be wiped remotely in the event of theft or breach, and most cloud services have built-in security features, such as role-based authentication and the capacity to shut down any part of a system if a threat is detected.
- Storing data in the cloud can help reduce the frequency and severity of insider threats. Research by the Ponemon Institute found that between 2018 and 2020 the average global cost of insider threats rose by 31% to $11.45 million, and the frequency of incidents spiked by 47%.
- Cloud systems store data in multiple locations, which protects information from hardware failure and corruption. Recovery times are 4x faster for SMBs that use cloud services versus those that don't.

The Biggest Cloud Security Challenges Ahead

Security in the cloud has the potential to be significantly more robust than when using conventional on-prem solutions. However, there are some challenges that need to be identified and addressed to help ensure that the experience is safe and profitable instead of risky and costly. Here are four of the biggest cloud security challenges in 2021 and how to address them:

1. Preventing Data Breaches

Unsurprisingly, preventing data breaches is — and likely always will be — the number one cloud security challenge. To address this concern, Donald Faatz, a Security Solutions Engineer at Carnegie Mellon Institute's Software Engineering Institute (SEI), advises organizations to adopt an integrated approach that includes all of the following aspects:

- Conduct due diligence across the lifecycle of deployed applications and systems, including planning, development and deployment, operations, and decommissioning.
- Identify and authenticate users, assign user rights, and enforce access control policies for resources.
- Enable access to critical data in the event of errors and failures.
- Prevent data that was supposed to be deleted from being accidentally disclosed.
- Monitor and defend systems and applications created via cloud-provided services.
- Collaborate with cloud service providers to investigate and respond to potential security incidents, and in a manner that is compliant with privacy regulations.

2. Complying with Regulations

There is a misperception among some organizations that when they shift workloads to the cloud, they delegate all responsibility for compliance to providers. However, this is not the case. Organizations are still obligated to ensure that data and applications are secure in a manner that aligns with prevailing regulations (e.g. GDPR, PCI-DSS, CCPA, etc.).

The most practical solution to this challenge is for organizations to verify that providers meet relevant regulatory standards. For example, Devolutions has achieved SOC 2 accreditation and ISO/IEC 27001 certification. We are also compliant with PCI-DSS, we implement enterprise-grade security model and encryption to safeguard data at rest and in transit, and we abide by a rigorous set of secure software development practices. To learn more, please visit this page: https://devolutions.net/legal/security.

3. Lack of In-House Expertise

According to the Cloud Adoption Practices & Priorities survey by the Cloud Security Alliance, 34% of organizations are not deploying (or not fully deploying) workloads to the cloud because they lack in-house IT expertise. And the problem is only going to get worse in the years ahead. As reported by Forbes: "Advanced cloud and security skills are in higher demand than ever before; however, there is a significant lack of qualified, skilled professionals to support this movement towards innovation."

While some organizations can outspend their competition to recruit the talent they need, this is not an effective or feasible option for many firms — especially SMBs. In these cases, working with a Managed Service Provider (MSP) can be an affordable, strategic, and effective way to close the skills gap. Click here for advice on how to choose the right MSP.

4. Cloud Migration Issues

Three of the most common — and costly — security-related cloud migration challenges that organizations face are migrating too quickly, misconfigurations, and API vulnerabilities.

Understandably, there can often be a great deal of eagerness — particularly among executives — to "get everything to the cloud ASAP!" However, organizations are strongly advised to take a slow-and-steady approach, carefully prioritizing what data and which apps should be part of the migration. As pointed out by cybersecurity firm Check Point: "Trying to accomplish everything at once is a major mistake. The migration process should be broken down into stages to reduce the risk of critical errors that could corrupt data and/or lead to vulnerabilities."

To mitigate the risk of misconfigurations, organizations should utilize comprehensive logging and reporting to rapidly detect and respond to issues. Other strategies include configuring appropriate access restrictions and permission during migration vs. doing this once post-migration as the network is built out. It is also extremely important to audit all resources, assets, and settings prior to migration. In 2018, a breach at FedEx exposed over 150,000 documents, which included sensitive material such as passports and driver's licenses. It was later discovered that the storage bucket that triggered the breach was exposed before FedEx purchased the originating company. In other words, FedEx inherited this vulnerability, and the risk remained unaddressed for several years before it was exploited.

Insecure APIs are the cause of many high-profile data breaches, such as those that have occurred in recent years at Venmo (mass scraping of 200 million records), Facebook (affected 6.8 million users and 1,500 apps), USPS (mass scraping of 60 million records), Federation of Industries of the State of São Paulo (exposing data points for 130,000 companies), and JustDial (exposing data points for 100 million users). It is critical for organizations to ensure that cloud providers have highly secure APIs that are constantly being updated and patched. What's more, this must extend beyond main or flagship solutions and pertain to companion tools and add-ons as well. For example, at Devolutions we recently increased the security of the API integrating Remote Desktop Manager with Devolutions Web Login. Click here to learn more about this upgrade.

From the Desk of Our CSO Martin Lemay

While all of the items here are important, in my view the number one priority for most organizations is to have access to qualified and experienced cloud professionals. With the right expertise, these organizations are much more likely to:

- *Prevent breaches*
- *Be prepared to comply with regulations and standards*
- *Perform migrations with minimal risks*

In addition, some cloud hosting providers only offer virtual machine deployments, which are basically systems exposed on the Internet without much security in mind. Working with cloud security experts — which is not the same as working with traditional IT experts — is crucial. Compared to traditional IT experts, cloud security experts have advanced tools and are better equipped and trained to understand and tackle security. They also provide strategic guidance and ultimately help businesses generate a better ROI on operation costs while reducing risks.

The Bottom Line

More organizations are elevating to the cloud. Research predicts that the global cloud computing market will grow at a CAGR through 2023, at which time it will reach an estimated value of $623 billion. And while there are significant rewards and advantages, there are also risks. Effectively identifying and addressing the security challenges described above will go a long way towards making the future successful — and safe.