7 Steps to Better, Stronger Cloud Security

Security is a shared responsibility between the organization and the cloud provider Storage upkeep, infrastructure and networking are some of the cloud provider's responsibility, whereas applications, access management, and network traffic protection is more on the organization's end. On day one post move, the cloud provides best in class security features and tools that continue to get better over time.

What is cloud security?

Cloud security is the protection of data, applications, and infrastructures involved in cloud computing. It is about preventing access. Cloud environments, whether public, private or hybrid, use the same security strategies as on-premise IT architecture. Your assets may be more secure in the cloud because cloud providers have superior security measures and their employees are security experts.

However, leveraging a cloud maintained by someone else doesn't mean you can, or should, sit back and relax. While AWS, Microsoft Azure, and Google Cloud have extensive security cloud experience, they are responsible for protecting the overall cloud infrastructure, but organizations need to recognize they have responsibilities too.

Check out our latest webinar, Security & Your GIS Cloud

Shine a Light: Establish Visibility

Organizations grow, shrink, split and merge. So do projects, people and locations. In the same fashion, you naturally acquire, adopt, and sunset tools that must be integrated or exported, in most instances, in and out of legacy systems. These integrations require building new relationships, processes and documentation. Growing complexity can make it difficult to maintain a big picture view. Security today relies on clear visibility into how everything works (or doesn't work) together - your network, systems, storage and applications.

Based on the 2019 Cloud Security Report sponsored by (ISC)2, the International Information System Security Certification Consortium, one of the top 2 greatest operational day-to-day headaches trying to protect cloud workloads is the lack of visibility into infrastructure security (33%). You can't secure your cloud environment, no matter what it looks like, without having it fully mapped and establishing real-time visibility.

Continued Education: Train Employees

"The only thing worse than training your employees and having them leave is not training them and having them stay." - Henry Ford

The majority of data security issues involve human error - misconfiguration, poor access control, or even a simple mistake. With employee negligence and mistakes as one of the biggest security issues, proper training is important.

Organizations prioritize the following cloud security skills as most critical in importance:

- knowledge of cloud specific security tools (47%)
- incident response skills (43%)
- knowledge of network behaviors (43%)

Ensure your staff have the skills they need to properly configure the tools they're using. Arm your employees with good security hygiene and set very clear policies about who is responsible and what the procedure is in the event of a potential incident. It's impossible to completely prevent errors, but the right response can make a world of difference.

Let's Talk About S-E-C-U-R-I-T-Y and Early.

Part of the problem for anyone trying to secure the cloud is that they're typically retrofitting security into a system that wasn't designed with it in mind; the old square peg in a round hole scenario. Often those responsible for security struggle to convince under-pressure teams to change their processes. Barriers between departments can lead to resistance.

One way to solve for this trend, is to shift towards DevSecOps, a practice that allows for security to be designed in from the start. This might be ambitious, but including security as early as possible in any discussion is valid, whether it's about a new tool, software in development, or a change to your cloud architecture.

Continuously Be Consistent

Being able to visualize your cloud and map precisely where your data is at any given moment is just the foundation, you also need to be continually vigilant. Data should be encrypted all the time, access should be tightly controlled, traffic should be monitored, and vulnerabilities need to be identified and remediated as swiftly as possible.

Continuously monitoring your network and feeding in fresh information about potential threats on an ongoing basis is vital. The faster you find issues the better your chances of mitigating them.

Use Trusted Software

What is in the cloud matters. You want a reliable, mature source of software that has the mechanics in place to provide and install updates timely, appropriately and efficiently.

Understand Your Audience

If you understand how people will interact with your data, application, or portal, you can better ensure safe usage and collaboration. Establishing user profiles and the roles and responsibilities for each profile will help determine permissions, access and expected user behavior. These profiles act as a baseline and send red flags if and when anomalies surface beyond the profile baselines. Only a system that understands the user's behavior can mark a user as trusted and warn a user from performing activities that might present a risk.

Choose the right people

Both hire and partner with qualified, trustworthy people who understand the complexities of cloud security. A public cloud's infrastructure, as with Azure or AWS, may be more secure than an organization's private cloud because the public cloud provider has a better informed and equipped security team in place. Partnering with a Cloud Service Provider who will guide your organization through these 7 steps will lead you on a path to stronger security.

For the third year in a row, training and certifying IT staff (51%) ranks as the primary tactic organizations deploy to assure that their evolving security needs are met. 45% rely on their cloud provider's native security tools, and 30% partner with a managed services provider to fill gaps in capabilities.

'Tis the Season! Check out our holiday checklist to get ready for a 2020 cloud migration!

In Conclusion

Security isn't something compromised when moving to the cloud. Security comes with the cloud. There will always be threats, whether in the cloud or on the ground. It is your organization's responsibility to stay on top of best practices to ensure you evolve to keep up with the latest. Need help? Let us be the ones to stay up at night, so you can sleep better knowing your assets are protected. Contact Us Today

There's no doubt that widespread adoption of the cloud has enabled collaboration on a much greater scale, driving innovation and creativity. Distributed workforces can work harmoniously, IT departments can offload expensive hardware and maintenance costs, and organizations can benefit from the latest developments in software tools