WHITE PAPER

7 WAYS TO SECURE YOUR CLOUD SOFTWARE QUICKLY

One of the biggest deterrents preventing companies from migrating to the cloud is fear that their data won't be secure. Read how business managers and IT staff can gain a better understanding of security on cloud applications.

Drew Koenig
Security Solutions Architect
September 2019

Magenic® // Fast Forward

Intro

Nothing is more important than the security of your digital assets. In the past, the best bet for organizations was to lock up data in servers and data centers and manage the assets directly, but today's cloud technology can do all of this more economically and quickly.

Using cloud-based resources is a trend that is growing in popularity. A **survey by the Cloud Native Computing Foundation** shows that the use of serverless technology among respondents went up 22 percent between 2017 and 2018.

As with most technology though, it won't help unless you know how to deploy it effectively. For many this is where things get tricky. Using a cloud architecture might be challenging for some organizations because they are accustomed to having direct access to their servers, but cloud servers are accessible only via the internet.

These seven tips will help companies transition some of the assets to the cloud more easily. By following them, your cloud learning curve won't be as steep and you should experience a significant upside.

Shared Resources Is the Cloud's Strength

Conventional wisdom in the past suggested that the best way to protect a company's assets was by separating mission-critical applications and data into separate segments on a network. Today, companies can place business essential information in the cloud in a way that is more secure than maintaining the information on premises but making this shift shouldn't be the end of the company's decision-making. In fact, the dynamics of who shares what in the cloud — between the cloud server vendor and the client — is an important distinction.

The traditional shared-security model assigns the security of the cloud to the vendor, and the security of what's in the cloud to the client. If not careful, that line can become blurred, leaving clients responsible for applications running in the cloud environment. A solid proactive resource plan should be shared that will mitigate any potential confusion. It is important not to make assumptions about who owns security in a cloud environment. Proactively working with a cloud provider to agree on security responsibilities will prevent disruptions and duplicated effort in the event there is an attack on a company's assets.

It's About More Than Technology. It's a Cultural Shift

In order for security to work in the cloud, a cultural shift to embrace an Agile mentality must happen inside an organization. Cloud services can improve security across an application or platform in several ways. The cloud service can provide a "single pane of glass" when it comes to security reviews. Most major cloud providers have security tools that can give one an easy-to-view report that aggregates all of a company's cloud assets that allow teams to identify issues and then review and remediate across multiple systems. Cloud services also make it more difficult for Shadow IT behaviors that create new services or server instances without a security team being alerted. Lastly, a company has the ability restore full systems in minutes.

But remember, it's not just about the system. It's about the ability to communicate the philosophy of the system in an organization so that everyone is equally bought in, from the executive suite to the IT team to the support staff.

Employ a "Shift-Left" Mentality

The days are over when an application is built to completion then reviewed in full by the security team. In order for security teams to be effective there must be a "shift-left" mentality. Using serverless technology, virtual workloads can be created or modified in minutes. As such, cloud computing teams operate in a highly dynamic environment with workloads constantly changing. Rather than waiting until the end, security teams need to be involved at the start, working with the architects and developers during the development process. In order for security teams to keep up with the increased development and workload schedules, security reviews need to be automated earlier and more frequently.

When done properly, shifting security "left" to the early stages of an application's design and development will increase a company's release frequency. There will be less time spent reviewing and remediating at the end of a build because the security controls and processes will be active throughout the lifecycle of the application's development, rather than when a product or feature is ready for release. This will reduce the number of risks and issues before final testing and release to production.

Prepare Against Ransomware by Isolating Your Data

The safest preparation against ransomware is to have your data isolated off-line, typically in a tape vault. To protect data from malicious or unintentional damage or loss from the cloud provider, a data backup solution must be considered for any application. In the cloud there are many options for backup solutions, from using the cloud services built in backup offering to sending the data to a company's own data center's backup solution. In order to ensure the integrity of a data backup, there must be separation from the backup process and storage to avoid any trickle-down impacts.

Encrypting Data

Data encryption in transit is a mandatory requirement in today's applications. There is no reason not to encrypt all data in transit, especially those moving in, out, and throughout a company's cloud service. Depending on the sensitivity of a company's data, encrypting data at rest, either in the databases or in stand-alone storage, is crucial. This is especially true when a company is using cloud services across multiple regions.

Embrace Role-Based Protections

Cloud services shared across multiple departments or divisions requires specific permissions to be put in place to enforce layered authorization. The most efficient way to do this is through role-based protections. Roles allow a central point for granting user, account, and service authorizations. Once put in place, roles and permissions rarely need to be modified. It is best practice to never assign authorization to a single individual or service directly. People and servers come and go frequently. Roles do not.

Work with a Partner

In order to leverage the cloud for its efficiency, scalability, and flexibility – and do so while keeping your digital assets secure – you need a partner that can show you how to get there with speed. Magenic has been achieving positive results for its clients through innovative digital solutions for more than two decades. Our delivery excellence and successful implementations have been led by top consultants in cloud technology. Reach out to learn more about our **Cloud Readiness Assessment** and how it can provide your organization a secure roadmap to the cloud.

About Magenic

Magenic is the digital technology consulting company built for speed. We have the right digital strategies, the right process, and the right people to get our clients digital products to market faster.

Visit us at **magenic.com** or call us at **877.277.1044** to learn more or to engage Magenic today.

Magenic® // Fast Forward