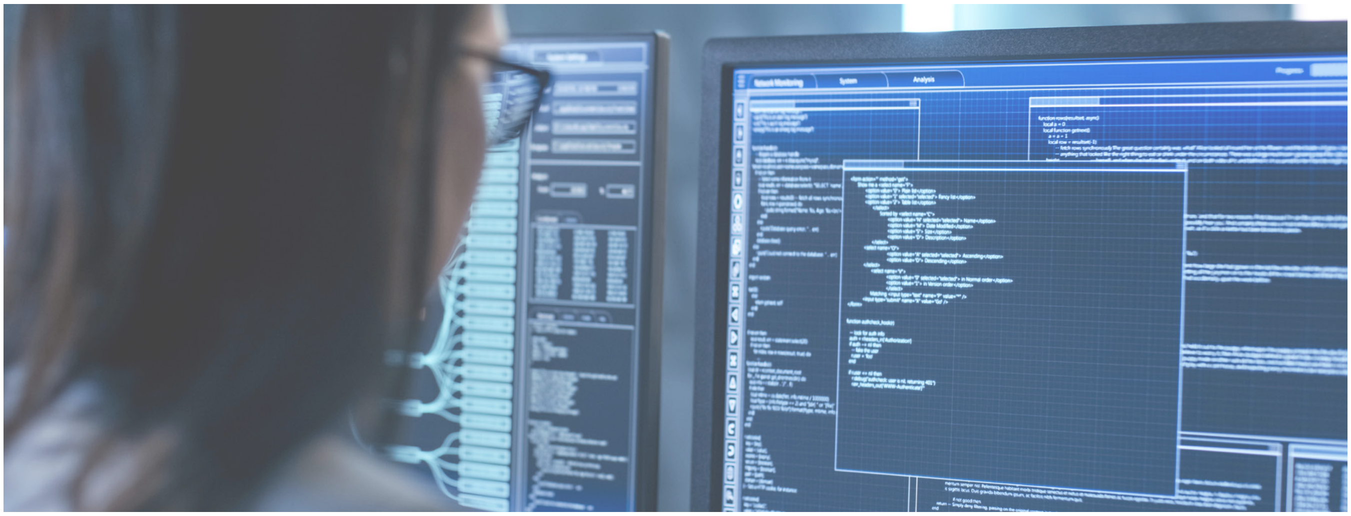
Top 10 Tips for Securing the Cloud

By: Jeff Johnson, Subject Matter Expert



Cloud security: a topic written about thousands of times over the years, but for good reason. According to a recent study released by research firm Comparitech, government agencies have suffered over 440 data breaches since 2014, with 2018 being the worst year on record.

As the data landscape continues to explode—and more and more agencies take advantage of cloud and virtualization-based technologies—challenges with security could very well get worse before they get better. Hackers are getting smarter. Attack surfaces are expanding. Ownership lines are being blurred between agencies and cloud service providers (CSPs). All of these are important factors to consider as agencies make the shift from on premise to the cloud.

Security is also a key topic outlined for successful cloud adoption in the Federal Cloud Computing Strategy, Cloud Smart. The strategy states, "Agencies should take a risk-based approach to securing cloud environments. As recommended by the Report to the President on Federal IT Modernization, agencies should emphasize 'data-level protections and fully leverage modern virtualized technologies.' This requires that agencies place an emphasis on protections at the data layer in addition to the network and physical infrastructure layers, transitioning to a multi-layer defense strategy, otherwise known as defense-in-depth."

However, navigating this new "security frontier" is no easy feat. In an effort to help agencies develop a more robust strategy, I have outlined my top ten tips for securing the cloud.

I encourage you to explore these best practices and closely evaluate how your agency is approaching security in the face of an increasingly complex threat landscape.

1. Build Security in from the Beginning

The security of your data and applications mostly depends on you, regardless of whether they are stored on premise or in the cloud. The National Institute of Standards and Technology (NIST) outlines guidance for organizations to better manage and reduce cybersecurity risk. My first recommendation is that before you do anything in the cloud, you align your strategy with the NIST Cybersecurity Framework following the core functions of identify, protect, detect, respond, and recover. It is also important to note that following these functions should not be done in a serial path, rather concurrently and continuously to ensure your agency is addressing the dynamic nature of risk.

2. Don't Overlook People, Processes, and Technology

The basic principles of security don't change from on premise to the cloud. In fact, many of the processes you employ today can extend directly to your cloud deployment. However, before you do anything, it is important for you to analyze the people, processes, and technology that you currently have available. Due to the nature of government acquisitions, agencies oftentimes have four different tools performing the same function, yet they are missing the one tool that performs an integral task.

Carrying out a gap analysis on your people, processes, and technology will allow you to maximize the investments you do have through optimization and education, as well as mitigate tool gaps and saturation prior to migrating to the cloud.

3. Ensure You Know Who Owns the Data

When it comes to the cloud, clearly identifying who owns the data is of paramount importance. A clear distinction must be made between the CSP's right to store and process the data and the ownership that is retained by the agency. Read the fine print and ensure you have binding and enforceable terms and conditions with the CSP you choose. You should also ensure you have effective service level agreements (SLAs) around data access.

4. Choose the Correct Tenancy for Your Mission Objectives

When you leverage the public cloud, you are extending your own environment to infrastructure that you do not own or maintain. This can provide a certain level of discomfort to federal agencies who have typically had 100% control. Before making a decision on tenancy, understand your mission objectives. Can you accept multi-tenant tenancy? Or does the nature of your data and applications require dedicated tenancy. Do you need to worry about citizenship and security classification? Factors such as these should all be closely considered before making a decision on which CSP and cloud model will best meet your agency's needs.

5. Develop a Cloud Maturity Model

When developing your agency's Cloud Maturity Model, I highly encourage you to embrace proven tools, techniques, and methodologies that are readily available from groups such as the Cloud Security Alliance (CSA) and Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG). These documents provide a standardized assessment and authorization process for CSPs to gain a provisional authorization so that they can properly serve federal customers.

6. Don't Underestimate the Importance of Configuration/ Change Management

If you aren't controlling the changes that are being made to your environment, how can you address issues if something were to go wrong? The importance of having proper controls for configuration/change management cannot be understated. NIST Special Publication 800-53 offers recommended security controls for federal information systems and organizations. I highly encourage you to align your policies with this set of controls.

7. Conduct Threat Modeling… Continuously

Cloud security should never be a "check the box once" activity. You must continuously monitor your environment to protect your data. There are many tools available in the market to help you accomplish this task, covering data loss protection (DLP), disaster recovery, encryption, masking, tokenization, access control, and more. The bottom line is, attackers get smarter every day, and you must stay ever vigilant to safeguard your infrastructure.

8. Protect All Endpoints

In a hybrid model, you have both on premise and cloud environments, which means that your attack surface expands. You have your own environment, your connection to the cloud(s), and your residence within the cloud(s) – all of which must be an area of focus for security. There are many robust tools available from vendors such as Symantec, Trend Micro, McAfee and Sophos that can help ensure you are protected from all possible angles.

9. Understand Your Role in the "In/Of" the Cloud Model

When it comes to the cloud, there is a shared responsibility between an agency and a CSP. CSPs provide storage, compute, network, and security, but it is up to the end user to properly configure and manage these resources. A cloud broker (like Cloud Lake Technology) can act as a trusted advisor and integrator to help agencies better understand their role in this new "in/of the cloud model."

10. Leverage the Tools the CSP Gives You

Today, CSPs offer robust tools for managing the security of your cloud environment. AWS, for example, offers Amazon CloudWatch, a tool that allows you to detect anomalous behavior in your environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly. Tools such as this make it much easier for you to get near real-time information into your cloud security status and establish a position of safety. I would offer that you take advantage of these built-in tools, as well as explore additional services that allow you to dive a few levels deeper into the data.

There are many more best practices I could cover, but I believe what is outlined above are some of the most important activities you can do prior to implementing cloud services at your agency. How would you rate your agency's cloud security posture today?

Cloud Lake Technology is a trusted cloud advisor for the federal government. Whether you are looking for end-to-end services, or support for only a piece of the transition, our cloud experts stand ready to support you. Learn more at www.cloudlakellc.com.