SPONSORED CONTENT

DEFENSESYSTEMS

SECURITY IN THE COMMERCIAL CLOUD: BETTER THAN EVER

As security compliance certifications have improved, agencies are more comfortable moving workloads to the cloud.

During the past few years, defense agencies have increasingly begun to rely on commercial cloud infrastructures to store unclassified data. Part of the reason for this heightened comfort level are the stringent certifications and requirements for cloud providers DoD and the federal government in general have put in place, such as FedRAMP and the Department of Defense Cloud Computing Security Requirements Guide (SRG).

Defense agencies are more comfortable using cloud providers that have achieved these high level certifications, especially when they have a successful track record managing the most business critical data of millions of customers. In fact, with the right processes and controls, there's no reason why defense data can't be just as secure in a commercial cloud environment.

According to a 2016 Gartner report, "The automation and programmatic infrastructure of leading IaaS providers enables enterprises to significantly improve the security protection of public cloud workloads to the extent that, if best practices are followed, they can be more secure than those in traditional data centers."*

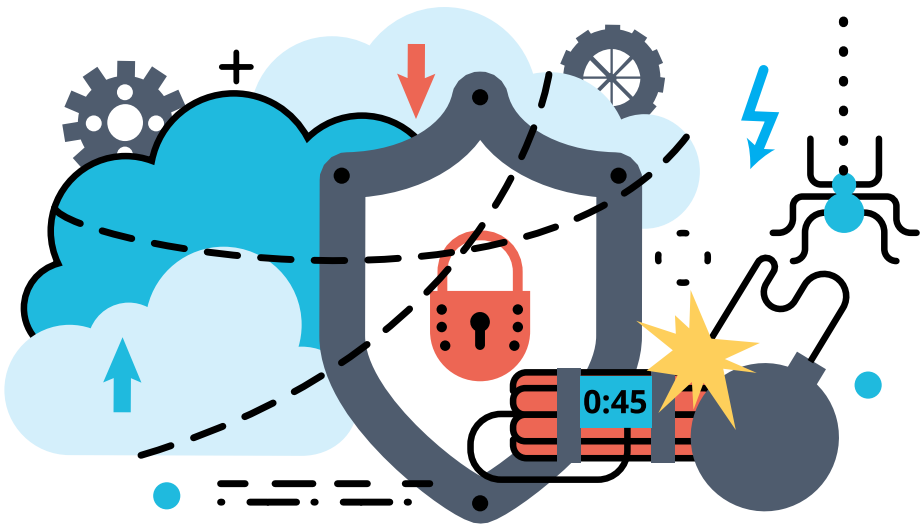
Despite this overwhelming evidence, some are still hesitant to trust the commercial cloud with sensitive information. For example, some believe multi-tenancy—the idea that more than one organization or user share physical compute, storage or networking resources—is inherently risky.

Nearly 10 to 15 years ago, there was reason to be concerned about whether you could really have strong logical isolation in virtualized layers. Today, you can have strong isolation and multi-tenancy in the compute layer by using a hardened hypervisor purpose built for the cloud, micro-segmentation through Software Defined Networking (SDN), logical isolation of storage and encryption for data at rest.

Other important features, such as strong authentication, encryption key management services, improved infrastructure visibility and data analytics have convinced many defense agencies it's time to gain the benefits of the commercial cloud. Amazon Web Services (AWS), for example, is connected to the NIPRNet and other unclassified DoD networks. This lets defense agencies store, process and analyze data in ways they have not previously been able to do because of limited compute power and storage resources in their own premise data centers. The DoD can now use cloud resources to analyze the terabytes of data it collects each day in near real time to find attackers and remediate security issues.

Many defense agencies are following suit. The Air Force's Space and Missile Center in Los Angeles, for example, turned to the commercial cloud to create test environments for the software that controls GPS satellites. "Where we needed help the most was creating test environments where we could test the software in a reliable and predictable fashion," said Lt. General Samuel Greaves at AWS re:Invent 2016.

Without moving testing to the commercial cloud, which helps developers field enough test environments to get results, the ground software capability was in danger of being terminated, says Greaves. "We were taking weeks to months to reconfigure between one test environment and another. The cloud capability helped us essentially buy a lot of schedule back, reduce cost and deliver capability as promised."



ArtRoseStudio/Shutterstock.com

COMFORT WITH THE CLOUD

The tide is clearly changing. Many believe the commercial cloud can actually be more secure than private cloud or data centers. Not only are security patches automatically applied to systems as soon as they are available, but equipment and software are constantly being improved upon and updated.

Security compliance certifications provide confidence to defense agencies

that they can build secure systems on top of a cloud environment. To verify security and compliance is being managed as promised to help agencies meet security control requirements, cloud providers should undergo testing by third-party auditors. Important certifications include:

• ***FedRAMP High baseline:*** This includes more than 400 security controls for non-classified systems certifying the cloud environment is able to host highly sensitive workloads. FedRAMP High assesses cloud environments using NIST SP 800-53 security controls. Achieving FedRAMP High allows FISMA High systems to be deployed in the cloud environment.

• ***DoD Cloud Computing Security Requirements Guide (SRG):*** Achieving this certification means a commercial cloud provider has a provisional authority to host DoD data. There are four levels of certification, each more restrictive than the last. Impact level 4, for example, lets DoD agencies use the cloud for production workloads with export-controlled data, privacy information and protected health information, along with other controlled unclassified information.

With certifications checked and confirmed, the next step is determining whether a potential commercial cloud provider has the most advanced security features. That includes full visibility and control capabilities, as well as state-of-the-art identity & access management features.

Visibility and control of an agency's infrastructure and data are critical to ensure strong security in the cloud. Knowing how many servers exist, who has access to those servers, who can touch specific data sets and where encryption keys are stored is a constant challenge. These tasks are easier to achieve in the cloud, especially in an API-driven environment that uses Software Defined Networking to logically isolate private networks.

With one command or audit report, you can get a sense in real time of how all your infrastructure is configured across all cloud resources. This lets you move fast while still ensuring your cloud resources comply with agency standards and best practices. You can see who has configured the cloud service APIs, including who, what, and from where calls were made. AWS CloudTrail provides deep visibility into API calls through log files you can ingest and analyze for anomalies.

Using the AWS Identity and Access Management (IAM) service, agencies can implement fine-grained access controls to manage and monitor privileged user access at a granular level. For example, you might allow only certain users to have access to specific AWS service APIs and resources and deny access to other resources. IAM also lets you add specific conditions to privileged access, such as time of day, originating IP address, whether they are using SSL/TLS, or whether they have authenticated with a multi-factor authentication device to control use of AWS.

All cloud computing activity should be logged and fed to log analytics services, which expedites incident response and troubleshooting. With proper logging and activity monitoring, IT managers can even review the agency's cloud resource history, including how they have been configured over a period of months or even years.

Encryption techniques are another critical factor. While all cloud providers that have earned security certifications will have excellent encryption options, there are differences when it comes to encryption features and key management options. For example, the ability for agencies to control encryption keys gives them the power to put data into any environment, as long as they ensure those encryption keys are secure and isolated.

Today, there is no reason you can't be as secure if not more secure operating in a commercial cloud environment. Check out the cloud provider's ability to comply with applicable security compliance regulations or audit standards completely. If they meet all of the criteria, commercial cloud services can be a great way to securely support the mission of the warfighters.

CERTIFICATIONS ONLY GO SO FAR

While commercial cloud environments have become more secure, it's important to leave nothing to chance. Here are some best practices to ensure your commercial cloud environment is fully secure.*

- Use the cloud provider's native security capabilities in conjunction with DevSecOps practices and tools to automate security controls throughout the application lifecycle
- Encrypt all data at rest in IaaS
- Control and monitor administrative access tightly
- Log everything, and monitor logs for indications of malicious intent
- Scan workloads for vulnerabilities before release into production and while in production
- Integrate application security testing and other vulnerability scanning capabilities into the deployment cycle, including scanning containers if they are used

FOR MORE INFORMATION, PLEASE VISIT:
AWS.AMAZON.COM/GOVERNMENT-EDUCATION/

amazon web services | intel

Gartner, How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center, 24 June 2016