GoDgtl
by PruTech

2022

THE IMPORTANCE OF CLOUD SECURITY

Table Of Contents

Preventing **data loss, securing access control points,** and setting up **proper notification and alerts** have all become the central focus points within cloud security. Therefore, it is **essential** to work with a cloud provider that offers **best-in-class security** customized for your infrastructure.

Cloud security is imperative for businesses making the transition to the cloud. With security threats constantly evolving and becoming more sophisticated, cloud computing is no less at risk than an on-premise environment. Security breaches make headlines almost every other day, with DDoS being one the most common attacks. Cloud platforms are increasingly becoming targets of such malicious attacks.

As a result, preventing data loss, securing access control points, and setting up proper notification and alerts have all become the central focus points within cloud security. Therefore, it is essential to work with a cloud provider that offers best-in-class security customized for your infrastructure. This paper examines AWS Security solutions and presents the benefits they bring to your organization to secure your cloud infrastructure.

The Need for Cloud Security

An increasing number of organizations are realizing the potential business benefits of moving their systems to the cloud. Cloud computing allows organizations to operate at scale, reduce technology costs and use agile systems that give them the competitive edge. However, it is essential that organizations have complete confidence in their cloud computing security and that all data, systems and applications are protected from data theft, leakage, corruption and deletion.

All cloud models are susceptible to threats. IT departments are naturally cautious about moving mission-critical systems to the cloud, and it is essential that the proper security provisions are in place, whether you are running a native cloud, hybrid, or on-premise environment. Cloud security offers all the functionality of traditional IT security. It allows businesses to harness the many advantages of cloud computing while remaining secure and ensuring that data privacy and compliance requirements are met.

Benefits of Cloud Security Solutions

Cloud security brings several benefits to protect your network infrastructure and ensure the continuity of your business.

Some of the key benefits of cloud security include:

Centralized Security: Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with shadow IT or BYOD. Centrally managing these entities enhances traffic analysis and web filtering, streamlines the monitoring of network events, and results in fewer software and policy updates. Disaster recovery plans can also be implemented and actioned efficiently when managed in one place.

Reduced Costs: One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads. Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.

Reduced Administration: When you choose a reputable cloud services provider or cloud security platform, you can eliminate manual security configurations and receive almost constant security updates. These tasks can have a massive drain on resources–but when you move them to the cloud–all security administration happens in one place and is fully managed on your behalf.

Reliability: Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud, no matter where they are or what device they are using.

Enhancing Security Solutions with AWS Well-Architected Framework Design Principles

You can further enhance your solution set by following basic guidelines outlined in the AWS Security Well-Architected Framework Design Principles. These principles allow you to build robust solutions based on proven methodologies and security strategies.

Here are some of the steps you can take to enhance cloud security:

Implement a strong identity foundation: Implement the principle of least privilege and enforce separation of duties with the appropriate authorization for each interaction with your AWS resources. Centralize identity management and eliminate reliance on long-term static credentials.

Enable traceability: Monitor, alert, and audit actions and changes to your environment in real-time. Integrate log and metric collection with systems to investigate and take action automatically.

Apply security at all layers: Apply a defense in depth approach with multiple security controls. Apply to all layers (for example, edge of the network, VPC, load balancing, every instance and compute service, operating system, application, and code).

Automate security best practices: Automated software-based security mechanisms improve your ability to scale more rapidly, securely, and cost-effectively. Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates.

Protect data in transit and at rest: Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.

Keep people away from data: Use mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of mishandling or modification and human error when handling sensitive data.

Prepare for security events: Prepare for an incident by having incident management and investigation policy and processes that align with your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

Benefits of AWS Security Tools

While there are many options for cloud security, AWS stands out for a variety of reasons. AWS tools have availability in 44 different zones and more than 16 geographical locations. As such, you can access servers from any country of your choice. Another valuable benefit is their disaster recovery system. Perhaps one of the most valuable reasons, however, is that AWS as a cloud service regularly offers enhanced security to protect data and check for security vulnerabilities.

Let's take a further look into some of the details of AWS security policies and features and why it's a great solution.

SCALE SECURELY WITH SUPERIOR VISIBILITY AND CONTROL

With AWS, you control where your data is stored, who can access it, and what resources your organization is consuming at any given moment. Fine-grain identity and access control combined with continuous monitoring for near real-time security information ensure that the right resources have the right access at all times, wherever your information is stored.

Furthermore, with security automation and activity monitoring services, you can detect suspicious security events, like configuration changes, across your ecosystem and can reduce the risk as you scale. It is also possible to integrate these services with your existing solutions to support existing workflows, streamline your operations, and simplify compliance reporting.

AUTOMATE AND REDUCE RISK WITH DEEPLY INTEGRATED SERVICES

Automating security tasks on AWS enables you to be more secure by reducing human configuration errors and giving your team more time to focus on other work critical to your business. You can select from a wide variety of deeply integrated solutions that can be combined to automate tasks in novel ways. As a result, your security team can work closely with developer and operations teams to create and deploy code faster and more securely.

For example, by employing technologies like machine learning, AWS enables you to automatically and continuously discover, classify, and protect sensitive data in AWS with just a few clicks in the AWS console. You can also automate infrastructure and application security checks to continually enforce your security and compliance controls and help ensure confidentiality, integrity, and availability at all times.

In addition, you can also utilize information management and security tools to automate in a hybrid environment and easily integrate AWS as a seamless and secure extension of your on-premises and legacy environments.

BUILD WITH THE HIGHEST STANDARDS FOR PRIVACY AND DATA SECURITY

AWS is vigilant about privacy. Customers care deeply about data security, and they have a world-class team of security experts monitoring the systems 24×7 to protect your content. With AWS, you can build on the most secure global infrastructure, knowing you always own your data, including the ability to encrypt it, move it, and manage retention.

All data flowing across the AWS global network that interconnects data centers and regions is automatically encrypted at the physical layer before it leaves the secured facilities. There are also additional encryption layers in all VPC cross-region peering traffic and customer or service-to-service TLS connections.

AWS also provides tools that allow you to easily encrypt your data in transit and at rest to help ensure only authorized access using keys managed by AWS Key Management System (KMS) or through your own encryption keys with CloudHSM using FIPS 140-2 Level 3 validated HSMs.

With these tools, you also get the control and visibility to ensure your compliance with regional and local data privacy laws and regulations. In addition, the global infrastructure design further allows you to retain complete control over the regions in which your data is physically located, helping you meet data residency requirements.

INHERIT THE MOST COMPREHENSIVE SECURITY AND COMPLIANCE CONTROLS

To aid your compliance efforts, AWS regularly achieves third-party validation for thousands of global compliance requirements to help you meet security and compliance standards for finance, retail, healthcare, government, and beyond. As a result, you inherit the latest security controls operated by AWS, strengthening your own compliance and certification programs. In addition, you also receive access to tools that can help reduce your cost and time to run your own specific security assurance requirements.

Moreover, AWS supports more security standards and compliance certifications than any other offering. The list includes PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171. This broad support helps satisfy compliance requirements for virtually every regulatory agency around the globe.

STRATEGIC SECURITY

AWS is designed to help you build secure, high-performing, resilient, and efficient infrastructure for your applications. These security services and solutions are focused on delivering the following key strategic benefits critical to helping you implement your organization's optimal security posture:

- **Prevent:** Define user permissions and identities, infrastructure protection and data protection measures for a smooth and planned AWS adoption strategy.
- **Detect:** Gain visibility into your organization's security posture with logging and monitoring services. Ingest this information into a scalable platform for event management, testing, and auditing.
- **Respond:** Automated incident response and recovery to help shift the primary focus of security teams from response to analyzing the root cause.
- **Remediate:** Leverage event-driven automation to quickly remediate and secure your AWS environment in near real-time.

Why Choose AWS for Cloud Security

As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations. Security in the cloud is much like security in your on-premises data centers—only without the costs of maintaining facilities and hardware.

Here are some of the convincing reasons to adopt AWS for cloud security.

*AWS Cloud allows you to scale and innovate while maintaining a secure environment and **paying only for the services you use.** This means that you can have the security you need **at a lower cost than in an on-premises environment.***

The AWS Cloud enables a shared responsibility model. While AWS manages the security of the cloud, you are responsible for security in the cloud. This means that you retain control of the security you choose to implement to protect your own content, platform, applications, systems, and networks no differently than you would in an on-site data center.

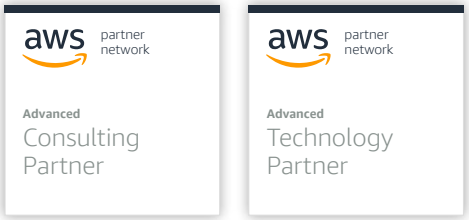
AWS provides security-specific tools and features across network security, configuration management, access control, and data encryption. AWS environments are continuously audited, with certifications from accreditation bodies across geographies and verticals. You can take advantage of automated tools for asset inventory and privileged access reporting.

AWS provides you with guidance and expertise through online resources, personnel, and partners. AWS provides you with advisories for current issues, plus you can work with AWS when you encounter security issues. You get access to hundreds of tools and features to help you to meet your security objectives.

As an AWS customer, you inherit all the best practices of AWS policies, architecture, and operational processes built to satisfy the requirements of our most security-sensitive customers.

How GoDgtl Collaborates with AWS

GoDgtl brings a team of experienced cloud experts who work directly with AWS to bring value and real solutions for your cloud projects. With direct access to AWS resources and in house cloud consulting talent, GoDgtl is ready to guide you through your cloud (security) journey regardless of where you are on that path. Whether it's more knowledge-based information on cloud topics such as security, or governance and compliance or basic cloud migration aspects or even if an assessment is needed, GoDgtl can provide a roadmap for your path to project completion and success.



Sources

https://www.tripwire.com/state-of-security/security-data-protection/cloud/cloud-compliance-best-practices-a-quick-overview/

https://aws.amazon.com/blogs/security/how-to-think-about-cloud-security-governance/?secd_comp2

https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/security.html

https://aws.amazon.com/security/

GoDgtl
by PruTech

*Our mission is to **help client organizations like yours access the latest resources and make their DX goals a reality.** Connect with our teams at Go-Dgtl to embrace new ideas and key enablers. **We promise to make your digital acceleration journey a success.***

ENABLE | TRANSFORM | ACHIEVE | ANALYZE | ADAPT

OUR LOCATIONS // Charlotte | Bangalore | Hyderabad | Mexico City | New Jersey (Iselin) | New York | Washington DC

CONTACT US // info@go-dgtl.com | (646) 536-7777 | go-dgtl.com