ICE
TRUSTED IT PARTNER

ICE'S ULTIMATE GUIDE TO

CLOUD SECURITY

ENHANCING CLOUD SECURITY: UNVEILING THE 6 PILLARS OF RESILIENCE

Cloud providers such as Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP) offer various security features and services for cloud-native environments. However, for comprehensive protection against breaches, data leaks, and targeted attacks, enterprise-grade cloud workload protection requires additional third-party solutions. To implement industry best practices effectively, an integrated cloud-native/third-party security stack is essential. It provides centralized visibility and policy-based granular control, enabling organizations to safeguard their cloud environments seamlessly.

#1 Identity & Authorization Management

IAM and authentication controls that are granular and policy-based in complicated environments

To simplify the process of updating IAM definitions in response to evolving business requirements, it is recommended to work with groups and roles rather than managing individual IAM access. Assign groups or positions the minimum access privileges necessary to perform their duties and increase the layers of authentication as access privileges grow. Additionally, maintaining proper IAM hygiene is crucial, including implementing authorization time-outs, enforcing strong password rules, and applying other relevant security measures.

#2 Zero Trust Environment

Zero-trust cloud network security measures used to micro-segments and logically isolated networks

Deploy business-critical apps and services in logically isolated areas of your cloud provider's network, like Virtual Private Clouds (AWS and Google) or vNET (Azure). Utilize subnets and fine-tuned security settings at subnet gateways to micro-segregate your workloads. For hybrid systems, consider dedicated WAN lines. Customize access to virtual devices, networks, gateways, and public IP addresses using static user-defined routing settings. This approach ensures improved performance, security, and personalized control over your cloud infrastructure.

#3 Threat Intelligence

Threat intelligence that quickly identifies and eliminates both known and unidentified threats

By providing rich context to the diverse streams of cloud-native logs, these vendors contribute to faster incident response times. Additionally, they offer tools that aid in visualizing and querying the threat landscape, empowering organizations to better understand and mitigate risks.

Utilizing AI-based anomaly detection algorithms, unknown threats are identified and undergo a thorough forensics analysis to determine their risk profile. Real-time notifications promptly alert users to intrusions and policy breaches, expediting the time to remediation. In certain cases, these alerts even trigger automated remediation operations. Third-party cloud security vendors cleverly integrate aggregated log data with internal data from asset and configuration management systems, vulnerability scanners, and more. They also leverage external data from public threat intelligence feeds and geolocation databases.

#4 Virtual Server Protection

Enforcing virtual server protection procedures and regulations, including software upgrades and change management

Cloud security suppliers provide robust Cloud Security Posture Management. They ensure consistent application of governance and compliance rules, along with templates, when provisioning virtual servers. Moreover, they actively audit configuration deviations and automate remediation when possible.

#5 Next-Gen Web App Firewall

Utilizing a next-generation web application firewall to protect all applications, but especially cloud-native distributed applications

This solution enables meticulous inspection and precise control of traffic to and from web application servers. It automatically updates WAF rules based on changes in traffic behavior and is deployed near microservices hosting workloads.

#6 Advanced Data Protection

Designed to maintain end-to-end encryption for shared content if all participants have Advanced Data Protection enabled

Enhanced data security is achieved through various measures including robust file sharing, encrypted communications, comprehensive compliance risk management, and meticulous resource hygiene for data storage. This encompasses identifying incorrectly set up buckets and eliminating orphan resources.

6 KEY CLOUD SECURITY CHALLENGES: NAVIGATING THE ADVANCED FRONTIER

The security landscape of the public cloud presents a distinct reality, as it lacks defined boundaries. Embracing modern cloud strategies, such as distributed serverless architectures, automated Continuous Integration and Continuous Deployment (CI/CD) techniques, and ephemeral assets like containers and Functions as a Service, further compounds the challenge in securing valuable resources.

Modern cloud-oriented enterprises face various sophisticated cloud-native security issues and risk levels. Let's explore a few of these challenges in depth.

Cloud Compliance and Governance

Major cloud service providers comply with well-known accreditation schemes like PCI 3.2, NIST 800-53, HIPAA, and GDPR. While customers are responsible for ensuring their data procedures and activities are compliant, the dynamic cloud environment and limited visibility make compliance audits challenging. However, using tools that enable continuous compliance checks and provide real-time notifications about misconfigurations can streamline the process.

Granular Privilege and Key Management

Cloud user roles are often configured with excessive permissions, granting unnecessary and unintended powers. A common example is giving unskilled or unnecessary users the ability to manipulate and modify databases, risking data security. Inadequate key and privilege configurations further exacerbate security vulnerabilities at the application level.

Complex Environments

Nowadays, enterprises prefer hybrid and multi-cloud environments. To ensure consistent security management across these environments, it is crucial to employ techniques and solutions that seamlessly operate across private cloud providers, public cloud providers, and on-prem deployments. This includes branch office edge protection for geographically dispersed organizations.

Ever-Changing Workloads

Cloud resources are swiftly allocated and decommissioned, operating at a rapid pace and scale. Due to the continuously evolving and transient workloads, conventional security systems struggle to effectively enforce protective policies within this adaptable and dynamic environment.

Increased Attack Surface

In today's digital landscape, hackers have found a new playground in the public cloud environment. With weakly secured cloud ingress ports as their gateway, they exploit vulnerabilities to access and tamper with valuable workloads and data. From malware and account takeover to zero-day vulnerabilities, we are witnessing an alarming rise in these detrimental threats.

Lack of Visibility and Tracking

Within the Infrastructure-as-a-Service (IaaS) model, cloud providers have complete control over the infrastructure layer, concealing it from their clients. As we move into the PaaS and SaaS cloud models, the already limited visibility and control are further amplified. Consequently, cloud users often face challenges in visualizing their cloud environments and efficiently identifying and measuring their cloud assets.

CONCERNED ABOUT YOUR CLOUD INFRASTRUCTURE'S SECURITY?

OR

HAVE ANY CLOUD PROJECTS ON THE HORIZON?

ICE Consulting is a managed IT, Cybersecurity, Cloud, and Compliance provider. We have AWS, Azure, and GCP certified architects, engineers, programmers, and security specialists who can help design, build, maintain, and most importantly secure any type of cloud environment.

CONTACT US TODAY FOR A FREE CLOUD CONSULTATION!

ICE
TRUSTED IT PARTNER

☎ 888-423-4801
✉ info@iceconsulting.com