CYBALT

Why Cloud Security Is Crucial?

Cybalt Inc. Suite #510, 2701,
North Dallas Parkway, Plano, TX

discover@cybalt.com

Why Cloud Security Is Crucial?

The benefits of reduced costs and complexity, flexible scalability, and lower per-unit cost organizations migrating their applications and data to the cloud. A number of studies suggest that the cloud platforms provide enterprises with a more secure outlet for storing applications and data. But organizations can't leverage the benefits of cloud computing without ensuring the security of its applications and data. They need robust security solutions that meet the frequency and speed of cloud deployment. Also, organizations must focus on the latest security tools and implement advanced security protocols to eliminate the disastrous impact of targeted security attacks.

There are several key reasons why traditional security strategies no longer suffice for an Organization for meeting cloud security challenges.

- The rise of hybrid cloud and multi-cloud architectures has increased even further the amount of complexity required to secure cloud workloads.
- Cloud container environments are highly dynamic. Because containers spin up and down constantly, there is often no consistent baseline that organizations can use to determine what constitutes a normal operating state.
- Misconfigurations of cloud security settings are a leading cause of cloud data breaches.
- A number of major data breaches have been caused by hacked, exposed, or broken APIs. In essence, it becomes imperative for companies to have an understanding of the security features that characterize the design and presentation of these interfaces.
- Traditional data centre security models are not suitable for the cloud. Administrators must learn new strategies and skills specific to cloud security.
- Zero-day exploits target vulnerabilities in popular software and operating systems that the cloud vendor hasn't patched.

Cloud Security best practices for the Organization

Cloud security is constantly evolving, but a handful of best practices have remained constant for ensuring the security of cloud environments. Organizations that have existing cloud solutions in place or are looking to implement them should consider these tips and tools to ensure that sensitive applications and data don't fall into the wrong hands.

- Implementing Zero Trust in an enterprise network establishes where boundaries can be placed and enforces access controls to shield sensitive applications, such as those within on-premises data centres, from unauthorized access and lateral movement.
- Discovers cloud resources across multiple cloud accounts and cloud service provider (CSP), and maintains an audit trail of changes to each discovered asset throughout its entire lifecycle. This enables the foundational visibility and awareness necessary for any successful cloud security program.

- Posture Management visualize and assess security posture, detect misconfigurations, model and actively enforce gold standard policies, in context and with enriched intelligence. Protect against attacks and insider threats, cloud security intelligence for cloud intrusion detection, and comply with regulatory requirements and best practices all from one unified platform.
- Monitors compliance posture across cloud environments and supports a vast library of compliance frameworks, providing real-time compliance monitoring and the ability to immediately generate audit-ready reports.
- Security correlates user actions across environments and uses machine learning to establish behaviour profiles. This is also known as user and entity behaviour analytics (UEBA). It monitors for sensitive activities, such as root user activity, security group changes and IAM (Identity and Access Management) configuration updates that may be signs of compromised credentials or malicious insider threats.
- Directly integrated with SOAR offerings, are based on rich, contextual data from various sources within cloud-native environments. Coupled with granular forensic capabilities and analysed with machine learning algorithms, these help expedite security incident investigations.
- Monitors all activities and runtime production environments across containers, images, hosts and functions, and stack-ranks vulnerabilities and risks across the entire cloud-native infrastructure.