CLOUD SECURITY IN THE PANDEMIC-DRIVEN PERIMETERLESS THREAT LANDSCAPE

Since the emergence of the coronavirus pandemic, an unprecedented number of organizations fully migrated to cloud architectures or migrated select applications to the cloud.

And, in the next 12 months, 45% of organizations expect to move an additional 75% of their applications to the cloud. Because cyber criminals are determined to capitalize on cloud computing trends, cloud security threats have recently increased by an astonishing 630%.

> Cloud security threats have recently spiked by 630%.

The complexities involved in securing the cloud environment are immense, and organizations are prone to under-estimating them. More than 90% of companies have a "cloud security readiness gap" between their present cloud usage, planned cloud usage and the maturity of their cloud security infrastructure. This reflects the tendency to downplay the importance of cloud security, almost relegating it to an afterthought.

Close your security gaps now and protect your cloud. Here's how:

1. ZERO TRUST ACCESS PERMISSIONS:

Take a no-nonsense, Zero Trust approach to cloud access management. Ensure that everyone who receives cloud storage access genuinely needs it to fulfill his or her job responsibilities. Conduct regular audits of your access list to ensure that no one maintains unnecessary privileges. When it comes to reducing the risk of human error and insider threats, the use of single sign-on, multi-factor authentication, context-aware policies and anomaly detection can also help.

2. CLOUD DATA ENCRYPTION:

Employ a VPN solution to encrypt cloud data that's in-transit. Use SSL transmission (TLS 1.2) across all interactions with the data. Termination of the SSL transmission should only occur within the cloud service provider's network.

In addition to encrypting data that's in transit, be sure to encrypt data that's at rest. Encrypt disks with AES-256 and be sure to encrypt your encryption keys.

> Research shows that more than 50% of organizations have accidentally exposed at least one cloud storage server.

3. MITIGATE API RELATED RISKS:

APIs that interact with your cloud may have their own baked-in security vulnerabilities. If you're new to cloud computing, limit this potential threat by select a cloud service provider that can provide you with metrics on their attack rates. In addition, ensure that your chosen vendor follows OWASP API security guidelines.

4. CLONE YOUR CONTENT:

To protect your organization from cloud-based data loss, backup your data on a regular basis. Back up your data in multiple locations in case of a multi-system attack. You may also want to consider offloading cloud backup to a reputable cloud backup service that can assist with versioning and meeting stringent HIPPA, Dodd-Frank, Sarbanes Oxley, PCI and/or other data compliance requirements.

> "With proper configurations and security controls, the cloud can offer you cost-effective process improvements, and a premium method for unleashing high-payoff opportunities," says one cloud security expert.

The network perimeter has dissolved, and that change is here to stay. After the coronavirus tappers off, nearly 75% of businesses intend to expand work from home options. To maintain this exciting degree of workplace flexibility, organizations must also maintain a cutting-edge, mature cloud security strategy.

Does your organization have the right infrastructure in place to support workplaces of the future? Learn more about securing your organization's cloud infrastructure right here.