SPONSORED CONTENT

CIO FROM IDG

Achieving Always-on Security in the Cloud Era

Navigating cloud security with a new approach to secure your business.

CIO 5M READ TIME

IDG COMMUNICATIONS, INC.

The technology and operational challenges posed by the global COVID-19 pandemic have been substantial, and IT organizations have heroically met them. Within days, IT organizations provided remote access at-scale to ensure seamless work, and then had to ensure the remote infrastructure was as stable and safe as possible.

The challenge is not over, however; 55% of organizations say that, post-pandemic, most employees will continue working from home at least one day a week, according to the PwC 2020 U.S. Remote Work Survey.

IT must revisit many of the workarounds they implemented initially to provide remote access quickly; now, they face replacing them with a permanent, more robust, and secure remote infrastructure. As a result, organizations that were already moving applications, data, and infrastructure to the cloud have accelerated their efforts.

Cloud migration provides many benefits. These include ubiquitous access, easy and unlimited scalability, and a sharp reduction in capital expenditures. It also can introduce risks, however—most notably, human error.

Cloud providers operate on a shared responsibility model; while they are responsible to secure their infrastructure, customers must secure access to their instances and buckets, as well as the data inside each tenancy and compartment. So, if an employee inadvertently misconfigures an instance, data could be vulnerable to risks from malicious attacks.

Additionally, as organizations move apps and data to the cloud, the scope of potential threats expands. In a public cloud, IT must worry about who else is sharing space there and whether there may be malicious insiders.

Growing risks of cyberattacks

Meanwhile, the risk of a cyberattack continues to grow. The first quarter of 2020 was the worst ever for compromised records, increasing by 273% over the same period in 2018, according to the Risk Based Security 2020 Q1 Report Data Breach QuickView Report.

Additionally, 80% of organizations were unable to prevent intruders from accessing critical data over the prior 12 months, according to a 2019 survey from CrowdStrike.

Traditional security responses, however, often do not translate well to the cloud. Established data center security policies have not been designed to work within an autoscaling environment. Additionally, traditional perimeter-based security measures typically require information about IP addresses, payloads, and ports—all of which are typically opaque in a cloud environment.

Remote workers introduce new risks, too. Employees' home networks may not be secure, for instance, and because they're working outside the corporate firewall, many of the security systems IT has in place may no longer apply.

This era requires a new approach to security.

Prioritizing cybersecurity across the business

First, remote employees must be able to connect securely to the resources they need, ideally through a virtual private network (VPN). This encrypts communications, protecting them from compromise.

Next, foundational security measures must take high priority and:

- Ensure all instances and buckets are properly configured; a mistake can allow malicious actors access.
- Encrypt data, both in transit and at rest, to protect communications and sensitive information stored in the cloud should a breach occur.
- Set up systems and procedures to proactively monitor for threats.
- Use automation to remediate identified risks such as misconfigurations and apply security patch updates to preempt security concerns.

Many organizations are considering adopting a zero-trust approach, in which all internal communications are treated as untrusted until the users, devices, or software attempting to connect are identified and authorized. This strategy effectively creates a micro-perimeter around each digital asset so that only identified devices and users with appropriate permissions can connect. This helps IT to prevent the lateral movement of threats across the environment.

Oracle Cloud and Database Security Solutions

IT can strengthen its security posture and reduce risk with Oracle Cloud, where security-first design principles center on

providing built-in security controls. Oracle isolates network virtualization in Oracle Cloud Infrastructure and provides strict separation of duties in Oracle Database.

Customers can automate security to reduce complexity, prevent human error, and lower costs with automated patching for Autonomous Database and threat mitigation for Oracle Cloud Infrastructure. Furthermore, Oracle database security solutions can reduce the risk of data breach and simplify compliance through encryption, key management, data masking, privileged user access controls, activity monitoring, and auditing capabilities.

The COVID-19 pandemic has transformed the IT landscape, pushing more employees to work from home while accelerating the transition to multiple clouds to solve problems. Although the new challenges for IT security are daunting, they are not insurmountable.

A new approach to security is required—one that no longer assumes employees, applications, and data reside within the corporate firewall. The use of cloud technologies and remote workforces are only going to grow, and IT security must adapt.