Undertaking Security Challenges in Hybrid Cloud Environments
Today, businesses are out to transform their organizations to maximize their full digital potential. After all, digital transformation provides a competitive edge, improved innovation, and new technologies that can drive better business. Cloud technologies by Amazon Web Services (AWS) help power this digital transformation. The cloud provides organizations of varying sizes the ability to process big data as well as provide access to greater storage and processing capabilities, among many others.

Businesses are now turning to hybrid cloud environments to make the most of the cloud’s dependability and dynamicity. A hybrid cloud model, after all, gives organizations the speed and scalability of public and private cloud infrastructures like AWS and the control and reliability of on-premises infrastructure. Hybrid cloud architectures can support Amazon Elastic Compute Cloud (Amazon EC2) workloads, which carry components of various sizes and capabilities ranging from transactional and database to high-performance computing.

In today’s world, organizations need to be able to operate 24/7. To maintain business continuity, critical business data should be backed up — securely — on the cloud, ready to be accessed by users regardless of location. Companies today also need to be able to manage, restore, and recover data, both on-premises and in the cloud.

A 2019 Nutanix survey shows that 85% of its respondents regard the hybrid cloud as the ideal IT operating model. The IDC also predicts that by 2021, over 90% of organizations across the world will be dependent on a combination of cloud computing deployment models that include on-premises, dedicated private clouds, different public clouds, as well as legacy platforms. Hybrid cloud environments provide the flexibility to run applications that need high bandwidth while also supporting workloads that require significantly less on-premises resources, empowering organizations with great elasticity and considerable practicality.

As businesses aim to disrupt their digital capacities and achieve more, an increasing number of organizations are shifting to agile software development to streamline software and application release cycles using DevOps tools and methodologies. Some organizations — those that adhere to the fail-fast philosophy — are prioritizing fast deployments to learn now if a project is a failure or otherwise to minimize business-impacting costs later. For all these to materialize, organizations turn to cloud-enabled and cloud-native applications that are supported by the hybrid cloud architecture, such as Amazon EC2 instances and containers.

With the great need for speed, organizations can follow the AWS Well-Architected Framework to successfully leverage the cloud. Security is one of the pillars of the framework and organizations need to secure their hybrid cloud environments amid cloud migration challenges and an evolving threat landscape. Hybrid cloud environments are now a fundamental business platform. Organizations must maintain the right mindset and deploy the right security tools to fully adhere to the framework and protect their environments.
Cloud Migration Challenges

As companies move to public and private cloud infrastructures like AWS to modernize their existing infrastructures, they need to make sure that they have enough knowledge of the cloud platform that they are moving into so that they can migrate securely, maximize performance, and optimize costs. Moving data and applications to a cloud environment without proper knowledge and preparation could result in decreased app performance or increased business costs. Hybrid cloud environments make the process more challenging, as they deal with varying design principles and security best practices.

The AWS Well-Architected Framework provides organizations an approach for migrating to and building in the cloud successfully and seamlessly. It has five pillars: operational excellence, security, reliability, performance efficiency, and cost optimization. For security, organizations need to understand that it is a shared responsibility. In the shared responsibility model, cloud providers like AWS are responsible for the security of the cloud infrastructure (i.e., hardware, software, and network), while users are responsible for securing the data, workloads, and everything else that they put in the cloud. Configurations, such as setting passwords and appropriate permissions, are the users’ responsibility. This is important to take note of because misconfigurations — whether in file storage buckets or user interfaces — may arise during cloud migration and could cause the exposure of stored personally identifiable information (PII). Misconfigurations, which may stem from customer user oversight or unawareness (such as leaving Amazon Simple Storage Service (Amazon S3) buckets unsecured and unencrypted), could lead to the unintended exposure of customer and mission-critical assets.

When security settings are not properly learned and configured, companies could stand to lose critical data, a hefty sum of money in fines, as well as lose millions of dollars from reputational damage. In recent years, there have been reports of cybercriminals stealing AWS API keys that were left externally accessible by the organization after database migrations. This, and other similar situations, make a strong case for the importance of the shared responsibility mindset when migrating to the cloud.

Furthermore, businesses have to abide by data privacy laws and regulations. For example, the General Data Protection Regulation (GDPR) regulates the collection, use, and movement of the personal data of EU citizens. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) outlines standards and rules for healthcare organizations like hospitals, nursing homes, and private medical practices that deal with sensitive healthcare data. Organizations that run on a hybrid cloud environment need to ensure

3 | Undertaking Security Challenges in Hybrid Cloud Environments
that all of their connected cloud environments — and the sensitive resources that house such — are protected against failing to meet requirements that may lead to data breaches, which can in turn result in costly fines.

The cybersecurity skills shortage — a challenge that affects nearly 50% of organizations with an employee shortage that has reached almost 3 million in 2018 globally — can also play a role in both performance efficiency and security. Because of the cybersecurity skills gap, (specifically, the cloud security skills gap), some organizations do not have security teams with the skills needed to secure a variety of cloud apps and platforms. A Logic Monitor survey found that 58% of organizations consider the lack of cloud experience within their employee roster a big challenge.

How to protect systems while shifting to the cloud

Organizations need to take the time to learn their cloud environments — including its security features and settings — as well as learn how to modify credentials and permissions. Aside from regularly auditing their cloud assets for misconfigurations, organizations should have integrated protection with advanced, consolidated, and adaptive security solutions that provide real-time protection as well as continuous compliance.
Evolutionary Threats

Cyberthreats continue to not only rise but also transform into more insidious variants. Organizations face a constant barrage of threats that can affect their bottom lines: the estimated losses that financial institutions can potentially incur yearly is anywhere between US$100 – 300 billion. And as businesses turn to the cloud to improve their infrastructure and processes, cybercriminals are quick to follow suit, crafting threats that compromise cloud platforms and applications.

Attackers are always trying to find ways to compromise organizations, so users should recognize the importance of correctly configuring services and making sure that all cloud-hosted software and applications are updated to the latest versions.

Customer user misconfigurations could become avenues for threats. For example, cryptocurrency-mining malware, which provides threat actors with new, illicit ways to turn a profit, has been found targeting the cloud infrastructure by compromising exposed containers, injecting malicious Docker images, or stealing leaked API keys. Last year, attackers infected more than 2,000 exposed Docker hosts with Monero-mining cryptocurrency malware. Meanwhile, according to our security predictions for 2020, vulnerabilities in container components will be one of the top security concerns for DevOps teams this year. Organizations must ensure that containers deployed on-premises or in the cloud are secured, and strong access controls should be in place to prevent unauthorized access.

How to combat evolutionary threats that affect the hybrid cloud environment

Because cybercriminals are adapting as organizations move to the cloud, organizations need to have security solutions that provide agile protection for the whole hybrid cloud infrastructure. Businesses can benefit from solutions that proactively defend against network threats and vulnerabilities with intrusion prevention and virtual patching. Applications and software in the cloud environment need to be protected against code vulnerabilities, data exfiltration, and vulnerability exploits. Cybersecurity solutions should be able to automatically lock down systems and provide real-time alerts for unexpected changes in interconnected environments with automated integrity monitoring and log inspection.
Expansive Attack Surface

With hybrid environments, the attack surface becomes more expansive because organizations that want to be able to build and deploy products as quickly as possible will need to interconnect applications, software, services, platforms, and networks. And all these would require holistic protection — especially as code injection attacks against cloud platforms and services via third-party libraries are becoming prominent.

Last year, Trend Micro researchers discovered an attack wherein cybercriminals took advantage of an API misconfiguration in Docker Engine-Community, an open-source DevOps tool. The misconfiguration allowed the threat actors to infect containers with a variant of the AESDDoS botnet.

It is critical to secure containers — which are also essential to DevOps — across different zones in the development pipeline, including in the image development stage and at the source code and registry levels.

Cybercriminals are also targeting other parts of the software supply chain, such as service providers. This is what happened to SmarterASP.net, a service provider for the web application framework ASP.NET, when threat actors infected it with ransomware. And as organizations adopt serverless computing for further efficiency, it will expectedly introduce an attack surface for misconfiguration and vulnerable codes.

How to secure a wide attack surface

Various applications, software, and platforms are now linked to allow businesses to host and run workloads simultaneously and quickly. Unfortunately, these interwoven technologies pose visibility challenges. An organization’s internal and outsourced security teams need a full view of the environment to identify security issues and remediate them as quickly as possible.
Trend Micro's All-in-One Cloud Security Platform

Migrating to the cloud and adopting DevOps can be challenging — but essential — for organizations, and it can be done with security and compliance in mind. Organizations will benefit from solutions that allow them to thrive in their hybrid cloud environments and enjoy agile and scalable software delivery cycles while keeping security and compliance at the forefront.

Trend Micro's Hybrid Cloud Security solution provides powerful, streamlined, and automated security within your organization's DevOps pipeline and delivers multiple XGen™ threat defense techniques for protecting runtime physical, virtual, and cloud workloads.

The Trend Micro™ Cloud One™ platform provides organizations a single-pane-of-glass look at their hybrid cloud environments and real-time security with the following automated and flexible services:

- **Workload Security** can automatically protect legacy systems with virtual patching and cloud workloads like Amazon EC2 from evolving threats through machine learning technology.
- **Application Security** is an embedded security framework that proactively detects threats and protects applications and APIs on their containers, serverless, as well as other cloud computing platforms.
- **Container Security** detects threats, vulnerabilities, and exposed sensitive data such as API keys and passwords, within container images.
- **File Storage Security** protects cloud file/object storage services like Amazon S3 that are on cloud-native application architectures via malware scanning and integrating into custom workflows.
- **Network Security** defends virtual private clouds by blocking attacks, threats, and detecting infiltrations.
The Cloud One platform also includes Cloud One - Conformity, which strengthens organizations’ cloud security posture by running automated compliance checks to ensure that they adhere to regulations and industry standards — such as PCI, GDPR, HIPAA, and NIST. Cloud One - Conformity also has a Knowledge Base, a continually growing library that contains checks that run against AWS accounts and provides step-by-step remediation rules to rectify any failures. It helps organizations adhere to the AWS Well-Architected Framework.

For organizations looking for runtime workload and container security or container image security as software, Deep Security™ and Deep Security Smart Check solutions can scan container images during predeployment and at runtime. With Deep Security’s automated deployment, extensive REST API integration, and exceptional security capabilities, organizations that adopt DevOps can churn out application release cycles quickly and flexibly while keeping their environments safe from ever-evolving threats. Deep Security also provides a financially elastic way to enhance the security of Amazon EC2 instances, as well as a streamlined approach to secure workloads across multiple environments through AWS Marketplace’s simple procurement and billing system.
TREND MICRO™ RESEARCH
Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com