TAG CYBER

MODERNIZING THE SECURITY INFRASTRUCTURE: MITIGATING ENTERPRISE CLOUD WORKLOAD RISKS IN LEGACY INFRASTRUCTURES

JOHN J. MASSERINI, TAG CYBER

MODERNIZING THE SECURITY INFRASTRUCTURE: MITIGATING ENTERPRISE CLOUD WORKLOAD RISKS IN LEGACY INFRASTRUCTURES

JOHN J. MASSERINI

Cyber security risks associated with using workloads on Amazon Web Services, Google Cloud Platform, Oracle Cloud and Microsoft Azure are distinct and inherently different from legacy enterprise infrastructure risks. Unfortunately, most security teams are ill-equipped to fully understand the risks of these cloud environments and how posture management, vulnerability mitigation, user access and data management are fundamentally different from the typical enterprise paradigm.

In this report, we will review the challenges of leveraging a modern cloud-based workload infrastructure, how it differs from its legacy peer and how the Sonrai platform can highlight these new risks.

INTRODUCTION

Moving to cloud-based, virtual workloads is a primary driver in many of today's enterprises. One **recent study** by the MIT Sloan School of Management reflected how public companies who are aggressively adopting cloud strategies have a 2.3%-6.9% higher annualized revenue growth rate. **Yet another study** has shown that almost half of the enterprise compute work effort is performed within the Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure (Azure), or Oracle cloud environments.

While the benefits of a cloud strategy to enterprises are substantial, the risks which accompany these modernization efforts are often misunderstood or misrepresented

not only within the security teams but across the organization due to shifting paradigms and the related gaps in coverage of the existing security tools. Unlike in legacy infrastructure environments, where security teams could rely on a high degree of visibility from design to implementation as well as some degree of direct control, cloud infrastructure migration, along with the move to DevOps, empowers the development teams to quickly stand-up entire environments, which include workloads, data stores of various type, as well as networks and cloud-based firewalls, with zero reliance on the existing change management processes. Gone are the days of architecture reviews and security evaluations for new applications and requesting firewall changes, DNS updates, or server configuration changes – today DevOps teams can deploy a fully integrated application suite in mere hours, without any assistance/approvals from, and often the knowledge of, the security team.

In this report, we will analyze the stark differences in risks of today's cloud environments in comparison to the legacy environments relied upon by most enterprises over the past 3 decades or more. Throughout the report, we will be highlighting the critical gaps in coverage typically seen by enterprise security teams and ultimately, how the Sonrai platform can facilitate the management of said risks.

ADVANTAGES OF THE NEW MODEL

The advantages of the cloud-based model are numerous. As an example, if we look at AWS, the ability to stand up a 'server' (i.e., workload), allocate a data store to it via an AWS S3 bucket, and assign it to a network with full internet access can now be done by a developer – with zero dependence on any other operations or security teams. Gone are the days of waiting weeks or months to stand up a test environment for developers. Nowadays, a database can be instantiated, tables loaded with data, and cloud-based firewalls opened to the internet – all within a couple of hours. All of this can be done with code, at a scale and speed that is unheard of outside of the cloud.

Today's rapid application deployment models are not only enabling a transformative business climate but are inherently driving significant technology modernization throughout many enterprises. The result is that the DevOps process has turned not only the infrastructure acquisition process but the entire process of building applications and whole environments on its head.

Not only does leveraging cloud solutions benefit the development process, but the ability to leverage virtual infrastructures rather than dealing with lengthy hardware supply-chain delays is forcing internal IT infrastructure teams to re-evaluate the necessity of having on-premises solutions. 'Cloud First' initiatives have not only become a nice-to-have but have evolved into a mandatory requirement to keep the business running.

While not typically a high-risk priority such as a data breach, cost containment is a factor in every enterprise. While many look at cloud solutions with an eye toward cost savings, the tendency of the environment to sprawl should be strongly considered. Oftentimes, temporary files, databases, and code repositories are left on abandoned workloads which, either running or shut down, consume storage and therefore, the fees associated with it. Having the capability to inventory and audit the cloud environment is no longer a nice-to-have, but an unquestionable necessity.

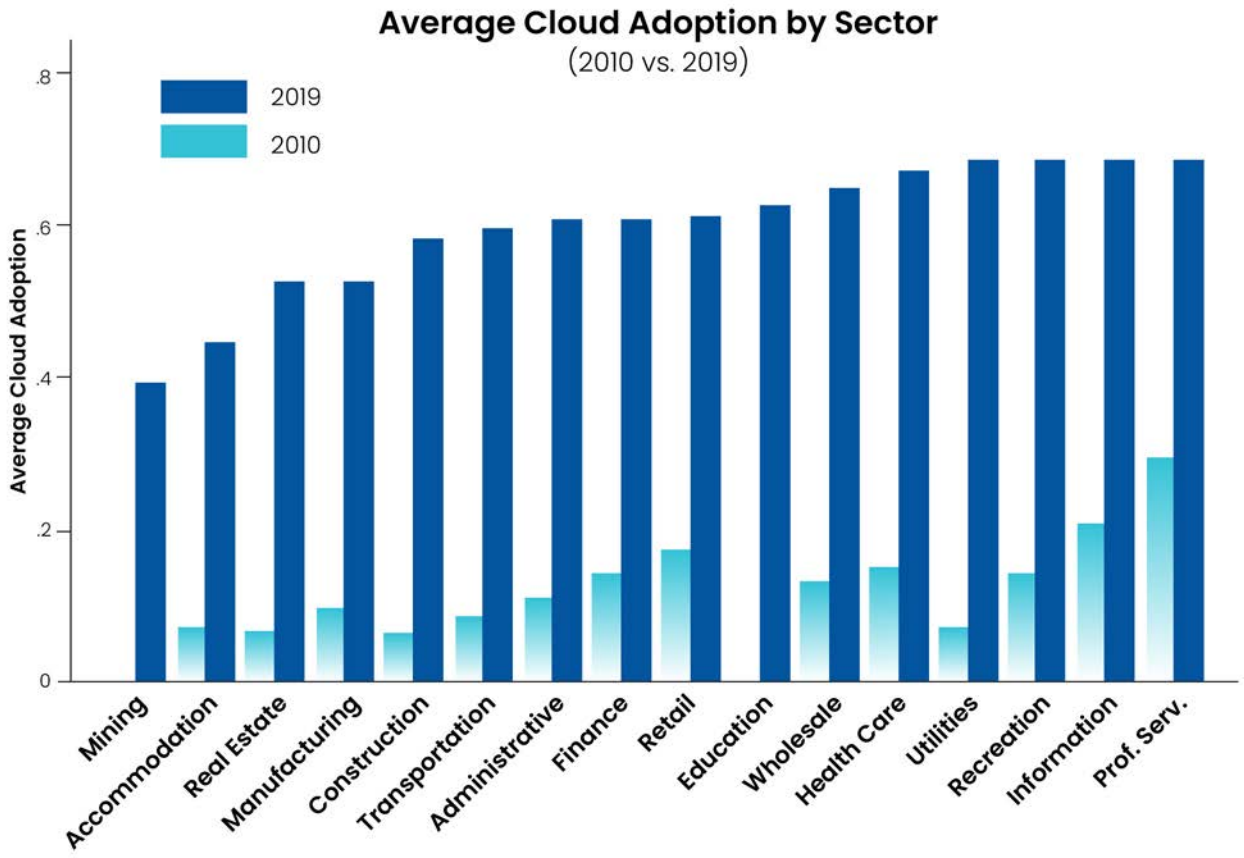

Figure 1: Cloud adoption 2010-2019 @Wang Jin

CHALLENGES OF CLOUD-BASED INFRASTRUCTURE MODELS

While most security executives have accepted the existence of the cloud within their organizations, most fail to understand the substantial difference in risk posture within this new model. In the previous example, while the developer was able to deploy their application stack quickly and easily, neither the security nor the infrastructure operations teams were alerted to the existence of the environment, much less given an opportunity to review the posture or the deployment settings of not only the workloads but of the entire environment.

Unfortunately, there are two fundamental root causes of this lack of visibility. The first is the inherent reliance on legacy process management to identify when changes occur within the infrastructure. Consider the average enterprise: when a business wants to offer a new application or service, they go through a rigorous process of architecture design & engineering, and hardware procurement, deployment, testing, and then operationalization. Each step along the way documents the environment changes, identifies those who are responsible, and ensures all ITSM change management efforts have been completed. From IP address assignment to firewall or DNS changes, the infrastructure operations teams 'own' the process and can ensure that new devices meet the documented requirements, have the appropriate controls, and do not disrupt the stability of the environment. This 'catch-all' legacy hardware and application deployment process is tried and true – and fails miserably when cloud technologies are introduced to the environment.

While an accurate device inventory has always been a challenge for most technology departments, the introduction of the cloud, with the ability to spin up workloads at a moment's notice, make an already problematic issue substantially more onerous. While most public cloud providers offer tools to manage inventory, all too often the function is neglected due to the lack of most companies assigning an individual to own cloud usage. Because of this, Asset inventory is virtually non-existent when it comes to most enterprise cloud environments, even though they have the ability to do it to an extent far greater than ever before.

The other major issue most security teams are facing is the inability of most legacy security tools to identify the risk and security issues around cloud workloads and applications. From configuration management, vulnerability scanning, or supplying security logs to the SEIM/SOC, cloud environments are often overlooked by the security teams mainly because of their inability to see what is running within the environments. Additionally, even when legacy security tools are deployed, their lack of conceptualizing the entire cloud environment leaves them woefully inadequate when it comes to identifying cloud-based risks.

TECHNICAL AND DATA MANAGEMENT RISKS OF CLOUD ENVIRONMENTS

Fundamentally, cloud risk management breaks down into two distinct risk profiles, Technical Security and Data Management. The technical security risks of most concern are three of the same issues you would find in a typical infrastructure; misconfigurations, vulnerabilities, and access controls/excessive permissions. As for Data Management risks, the lack of controls over data stores and the information stored in them is of critical importance within cloud environments. Not only of concern is the sensitivity of data stored, but also how it's stored, who or what has access to it - and what permissions have been provided - as well as what they are doing with the data.

TECHNICAL SECURITY RISKS

In a similar vein to their legacy counterparts, cloud environments are vulnerable to the same types of technology-centric risks that security teams have been dealing with for decades. Unfortunately, due to the inherent trust relationships which exist in most cloud environments, risks that would have historically been limited in scope to specific devices or networks now impact the entire platform. While such trust relationships enhance the speed by which deployment can occur, it also greatly increases the possibility that an otherwise innocuous user or vulnerability could be leveraged to subvert the entire cloud environment. Trust relationships within the modern cloud environment are truly their Achilles Heel.

ACCESS CONTROLS

One of the most critical issues facing cloud environments is the lack of controls around user and machine access management. Having common, shared passwords across users and systems is a frequent deployment method to ensure everyone who needs access can get it. In general, the DevOps process consists of a write-build-test-deploy cycle called a 'sprint' which generally lasts around a couple of weeks. To ensure everyone on the DevOps team, from the developer to the testers, to the business partner, has access to the applications as needed, common, easily shared non-person cloud identities, such as AWS Roles, Azure Service Principles, etc., are used. Unfortunately, such access rights tend to migrate into production as the application does, providing access that was intended for testing now with full permissions to often sensitive production data.

This same issue exists when you evaluate the trust relationships in workload-to-workload (machine-to-machine) connections and communications. If we were lucky and the developer decided to configure SSH connectivity or something as basic as FTP accounts to move flat files from host to host, SSH keys and accounts with weak passwords or excessive privileges tend to follow the system all the way to production. As previously highlighted, the lack of ability to track and report on these users and privileged keys leaves the enterprise highly vulnerable to both external and internal attacks.

POSTURE AND VULNERABILITY MANAGEMENT

Much in the same way as access control issues mirror that of the legacy enterprise, so do risks associated with posture and vulnerability management. If a developer decides to deploy a LAMP (Linux-Apache-MySQL-PHP) stack, they will likely choose the image that gives them the greatest number of development and application options, rather than the one that is pre-hardened. Many of these workload images are designed for ease of deployment and take few security controls into consideration, resulting in a highly vulnerable system that is now being exposed to the public. As we've highlighted previously, the lack of visibility into the workloads, or even that the workloads exist, leaves the security teams behind the proverbial 8-ball when it comes to trying to manage risks in the cloud. This has never been more apparent than after the recent Log4j and Log2Shell vulnerabilities, where without an accurate workload inventory, determining the risk to the enterprise would be nearly impossible.

Unlike in a legacy environment, however, vulnerabilities and configuration issues on workloads can result in a significant risk of breach across the entire cloud environment. Time and time again, vulnerabilities have been used to exploit misconfigured workloads, resulting in the attacker gaining access to a specific workload. While significant, due to the frequent misconfiguration of identities and roles within the cloud environments, the attacker now potentially has elevated access to every other workload within the environment.

DATA MANAGEMENT

While generally, the focus of most risk analysis tends to be on vulnerabilities and threat actors, the way data is managed throughout a cloud environment can substantially mitigate those threats, or conversely, elevate the risk if not managed correctly. Due to the nature of the DevOps lifecycle, the various data stores within cloud environments tend to replicate quickly, leaving outdated databases or file extracts lying around unprotected. A solid cloud data management program is essential to mitigating data breach risks of any cloud deployment.

When developing a data management program for most cloud deployments, the security teams must consider four key elements:

- Where within the cloud is the data stored? (Location)
- What type of data is stored in the cloud environment? (Classification)
- Who /what has access to that data? (Entitlements)
- What are they doing with it? (Usage)

Due to the fundamentally different ways in which most cloud environments are managed, understanding the inherent risk associated with cloud data storage should be the foundation of any cloud strategy.

Production Data Management
Protected data, be it customer information, health care or financial records, or any type of intellectual property, must be managed especially tightly within cloud environments. Due to the lack of segmentation, the hard, air-gapped network boundaries that most infrastructure teams rely on disappear within cloud environments.

Since the major appeal of adopting DevOps is the rapid time-to-market for new business applications, understanding how production data is used and managed is key. Much like the applications themselves, data models change frequently throughout the early DevOps sprints so models which had little protected data in the early stages will often end up with a collection of elements that elevate the entire cloud data store to a protected level.

As more enterprises adopt a DevOps model, managing production data and appropriately mitigating these new types of risks will be critical. This gap was a root cause identified in one of the most noteworthy breaches of the last several years. As the after-action report from the Department of Justice noted, the **Capital One breach** in July 2019 was due to a vulnerable workload, which had access to cloud data stores of customer data, that was exposed to the internet.

Test Data Management
Within any typical development shop, regardless of the methodology used, the need for accurate, current test data is critical in ensuring the applications are functionally tested adequately. As such, duplicating, moving, and backing up databases is a common occurrence in development environments. Unlike in legacy infrastructures, cloud-centric development teams have the capability of making countless copies of data stores, datasets, full databases, or flat files, full of the customer data

SONRAI PLATFORM OVERVIEW

Sonrai offers a total public cloud security solution for Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Oracle Cloud. Sonrai Dig identifies and monitors all relationships between workloads, identities, and data stores that exist within your various cloud platforms to provide security teams a continuous view of all risks, unusual activity and automated remediations.

Through a single user account, Sonrai can analyze host, datastore, and user activity to provide a complete picture of what's happening across your clouds. Additionally, Sonrai applies analytics to the workload activity logs to provide deep insight into data access activities and user permissions across the entire environment, uncovering risky relationships between workloads and identities.

By leveraging the Sonrai Governance Engine, security teams can automate risk remediation workflows such as patching, posture validation, or user access/privilege management to ensure the platforms stay secure in real-time. By being able to identify protected information within the various datastores, Sonrai can determine the true risk to your data across the entire platform, not just based on the risk of a single workload.

ACTION PLAN

Surprisingly, the 'not in my backyard' opinion of many security leaders is indicative of the cloud security problem, and unfortunately, far too many have ignored the rapid expansion of such platforms within their environments. While most cloud platforms offer adequate security controls, more often than not, developers choose ease and speed over security since many are left to make their own decisions.

The DevOps model, and cloud solutions in general, continue to be adopted at an ever-increasing pace. As business leaders recognize the increased revenue growth associated with cloud strategies, the Information Security teams must find ways to adapt and, more importantly, participate in this rapid deployment approach. Ongoing reliance on legacy security approaches and tools will only hasten the increase in cloud-centric risks that already exist in most organizations.

Security executives must recognize the risks of such cloud initiatives are in many ways different from what they are accustomed to. They can no longer presume that their legacy vulnerability scanners, configuration managers, and identity management solutions can provide a holistic view into the highly volatile cloud environments being deployed today. They must fully embrace new solutions which have been designed and developed specifically for cloud platforms and find ways to integrate them with their legacy toolsets.

ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner's perspective.

IMPORTANT INFORMATION ABOUT THIS PAPER

Contributor: John J. Masserini

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non-analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by Sonrai Security. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.