Cloud Security
BEST PRACTICES

American
Technology Services
a WWTS Company

What you need to worry about in the shared responsibility model.

Use of the cloud drives multiple business benefits, including decreased time to market, increased security, and business growth. Additionally, the power of the cloud enabled the shift to working from home in response to the COVID-19 pandemic, minimizing disruption to operations for many organizations. Working from home has proven to be so effective that several large enterprises chose to make it a permanent shift early in the pandemic. But it's important to understand the technology and its unique attributes prior to migrating any infrastructure to the cloud. ATS provides key background info in our eBook, "Cloud Computing Best Practices: Tips to Maximize Your Benefits." In this eBook, we dive deeper into cloud security, specifically.

CONTENTS

What is Cloud Security?

The Shared Responsibility Model of Cloud Security

While public cloud providers dedicate extensive efforts to security, customers retain responsibility for how they use those services, including the data that is stored in them, and how it is shared and accessed.

Security of the Cloud Provider No Longer a Concern

The Oracle and KPMG Cloud Threat Report 2020 shows that trust has continued to grow in both public cloud infrastructure and business-critical applications as a service. In a laudably titled paper, "The Egregious 11," The Cloud Security Alliance (CSA) outlines the top threats to cloud computing. The paper begins with some excellent news regarding the reliability of cloud service providers' security efforts. "After analyzing the responses in this survey, we noticed a drop in the ranking of traditional cloud security issues under the responsibility of cloud service providers (CSPs). Concerns such as denial of service, shared technology vulnerabilities and CSP data loss and system vulnerabilities – which all featured in the previous Treacherous 12 – were now rated so low they have been excluded in this report."

The Modern Cloud Landscape & the Risks of Inadequate Security

The Pervasive Problem of Cloud Breaches

Breaches whether, on-prem or cloud, are expensive and can even be fatal to smaller organizations. 60% of small companies go out of business within six months of falling victim to a data breach or cyberattack.

Cloud Customers Are Failing to Secure Their Cloud Use

Unfortunately, most cloud customers are failing to adequately execute their shared responsibility for security. Gartner predicts that, through 2025, at least 99% of cloud failures will be the customer's fault.

According to the 2019 McAfee Cloud Adoption and Risk Report, "Most cloud customers aren't fulfilling their shared responsibility for security. ...trusted cloud providers now dedicate a tremendous amount of resources to security, all to protect their customers and the sustainability of their business model.

So what's left?

Breaches—whether on-prem or cloud, are expensive and can even be fatal to smaller organizations. 60% of small companies go out of business within six months of falling victim to a data breach or cyberattack.

The report cites the following shortcomings on the part of cloud customers:

- Only **26%** of companies say they can audit IaaS configurations.
- Only **33%** of companies say they can control application collaboration settings.
- Only **36%** of companies say they can enforce data loss prevention in the cloud.

Organizations are aware they are at risk, although too many are still not taking adequate measures to secure their infrastructure. Almost half of organizations surveyed believe they will experience a data breach in the next 12 months, according to a June 2020 451 Research survey. In a grim prediction, the report states the problem of breaches, **"will likely not improve soon as organizations adopt modernization and transformation initiatives that are outpacing the ability of security teams to adapt."**

Simple Errors Lead to Massive Problems

A September 2019 McAfee survey of 1,000 enterprises in 11 countries finds that, in most cases, the breach "is an opportunistic attack on data left open by errors in how the cloud environment was configured." Despite the great risk they pose, 99% of misconfigurations in enterprise IaaS environments go unnoticed, according to McAfee.

The fact is that most attackers aren't sophisticated. Instead, they opportunistically exploit simple mistakes. This is good news. Simply being more fastidious in how your workloads are configured can reduce your risk of breaches substantially.

According to the annual Cost of a Data Breach Report, malicious attacks were responsible for 52% of breaches in the 2020 study. The most frequent initial attack vectors included compromised credentials (19% of malicious breaches), cloud misconfiguration (19%) and vulnerabilities in third-party software (16%). Striving to prevent these types of attacks requires a comprehensive approach. Unfortunately, the lack of integration with many security solutions only impedes security efforts.

Cloud Complexity & Sprawl

Not only are organizations unclear about the misconfigurations inside their cloud environments, they don't even know what cloud environments they're leveraging. In McAfee's recent study, 76% of enterprises reported having a multi-cloud environment, but an examination of customer data found that actually 92% of those environments are multi-cloud.

Microsoft is continuously improving its security posture in Azure and combines key security features in their Azure Security Center, which allows technical staff to protect an organization's hosted environment and their workloads running in the cloud. It's challenging for security practitioners to keep up with the rapid pace of the new security features and functions, which in turn can lead to misconfigurations.

> **In a complex multi-cloud environment, you need an expert for every single platform or service you're using to ensure that the appropriate security measures are in place.**
>
> —**John Yeoh**
> Global VP of Research
> *Cloud Security Alliance*

Where Are the Biggest Risks?

In their 2019 Cloud Adoption and Risk Report, McAfee assessed billions of aggregated, anonymized cloud events in the McAfee universe of enterprises to show where sensitive data resides in the cloud. An average of 31% of sensitive data resides in Microsoft's Office 365.

SaaS Apps: Convenient Drivers of Business Productivity & Attack Vectors

Files are the primary area where sensitive information tends to live. With many SaaS apps, users are able to not only interact with files, but also configure sharing and access for other users. Cloud security requires you to get a handle on these interactions and configurations. Unfortunately, a lack of granular control of file security in many SaaS apps makes this particularly challenging.

There are many different ways to configure the file sharing settings on platforms such as Office 365 and Box, and the implications of those settings are not always clear. Additionally, the behavior can vary from one app to another, making it very difficult to remediate violations.

While collaboration between users, both within and outside the organization, can help drive business productivity, it's important to maintain granular control over access. SaaS apps are another vector where security pros must strive for balance between productivity and security.

Tips to Properly Execute Cloud Security

01 Gain Complete Visibility

Components of cloud security are highly interconnected. Weaknesses in one area can reverberate in others. Cloud security requires a unique, tailored approach. Systems can interact much more easily in a public versus private cloud network, and this interactivity raises additional security concerns. A vulnerability that might otherwise have been inconsequential could result in attackers gaining access to sensitive information in another area.

Visibility and End-to-End Context Are Vital

It's important to understand how resources should behave so you can observe when that behavior deviates. This requires a complete picture of your environment and context around all your cloud log and event data, so you know what to expect, and can more effectively detect and visualize threats.

> **But it's far easier to understand how something should behave and then see when it changes than it is to constantly play Whack-a-Mole with intruders. If you have a complete picture of your environment and you know what to expect, you can more effectively detect threats such as misconfigurations.**
>
> —**Sam Bisbee**
> CSO
> *Threat Stacks*

Visibility also requires context in order to be useful. It can be nearly impossible to discern useful info from mountains of data logging cloud events. Look for cloud security solutions with consolidated dashboards that provide insights and intelligence needed to not only identify threats, but act in a timely manner.

An Excess of Security Tools Creates the Problem of the Gap

According to The Oracle and KPMG Cloud Threat Report 2020, 92% of companies surveyed have a «cloud security readiness gap» between their current and planned cloud usage and the maturity of their cloud security programs. 70% of those surveyed report too many tools are needed to protect public cloud environments. On average, each uses more than 100 discrete security controls. Multiple security vendors provide disparate, uncooperative solutions that are lacking shared intelligence and blocking on different attack vectors. The result is gaps, and those gaps create access points for attackers.

To overcome these gaps, it is imperative to implement tools and resources that help simplify the security management of the cloud and take control of security. Where possible, the goal should be to acquire security solutions that can replace multiple existing security tools within an organization, which allows the centralization of monitoring and reporting features within a single dashboard.

Regulatory Compliance

Compliance has been a key driver of security deployment. For many regulations, the challenges tend to be the same, and related to visibility and quick response at scale. In particular, visibility and continuous monitoring is needed to map to regulatory requirements and achieve compliance with laws and industry standards, such as NIST 800-171, CMMC, GDPR, CCPA, and HIPAA. With ever-expanding cloud sprawl, it becomes increasingly difficult to understand where you have sensitive info.

02 Trust But Verify

Zero Trust

Legacy security infrastructures are based on the outdated assumption that anything within the security perimeter can be trusted. They're ineffective and leave organizations exposed to cyberattacks. The concept of a secure castle surrounded by a moat is archaic.

Conversely, Zero Trust security is an approach that trusts no user, device, workload, or system, either inside or outside the perimeter. No one and nothing should be trusted by default, regardless of the location in which it is operating from, either inside or outside the security perimeter.

Implementing Zero Trust requires a unified approach to avoid the security gaps and complexities that result in attempting to use disparate technologies. Instead, Zero Trust requires you dynamically understand who your users are and dynamically permission them based on their credentials.

On October 15, 2020, Microsoft announced the launch of the Zero Trust Deployment Center, a repository of information and guidance to improve organizations' Zero Trust readiness and implementation. Microsoft also created a Zero Trust assessment tool to help measure your current maturity and identify possible next milestones and priorities along with technologies.

The Zero Trust Approach should be based on six foundational pillars of critical resources to be defended.

(see diagram on the next page)

Zero Trust Security

VISIBILITY, AUTOMATION, ORCHESTRATION

Identities | Devices | Apps | Network | Infrastructure | Data

Identity & Access Management (IAM)

Identity and Access Management (IAM) is the process of managing who can do what on which resources. The role of identity and access is to facilitate access and authentication to all IT infrastructure, including SaaS apps and on-prem apps. Azure describes IAM as 'protecting your applications and data at the front gate,' which can be managed with products such as Azure Active Directory to enable:

- Single sign-on
- Conditional access
- Multi-factor authentication (MFA)
- Single-identity platform
- Integration of identity into your apps and services

IAM that maximizes security while minimizing friction for the end user is a challenge. Chenxi Wang, founder and general partner, Rain Capital, states that among the top three cloud migration security risks is, **"Proper setup and protection of user identities while accessing the cloud."**

Cloud security must manage access both in terms of user identity and their origin. Look at federated domain services to allow synchronization of user permissions and policies between on-premise and cloud services and applications.

The Challenges of Enabling the Business Without Enabling the Attacks

Multi-cloud is the norm and the complexity continues to increase. According to Flexera's annual state of the cloud report for 2020, of those organizations using cloud services, 93% have a multi-cloud strategy that combines multiple public and private clouds. 62% of organizations using public cloud are using more than one public cloud. More than half of organizations (53%) are using multiple public and multiple private clouds, followed closely by 33% using a single private cloud and multiple public ones.

Security must tackle the challenge of enabling the business without restricting such expansion in order to make their jobs easier.

Data-Centric Approach

Cloud security controls need to accompany workloads and data while at rest and in transit. As part of the data-centric approach cloud security requires, make sure your data is always encrypted. Protect data at rest, in motion, and in use, and ensure access to the data is only on an as needed basis. You can also manage your encryption keys in the cloud in order to have more complete control of your data.

03 Deploy Securely

Understand the Unique Security Requirements of Cloud Native Tech

Cloud native technologies like serverless and containers minimize the burdens of infrastructure ops orchestration. However, they bring unique security challenges which traditional security tools that were not designed to monitor such technologies.

A container is a standard unit of software that packages up code and all its dependencies, helping simplify the process of building and deploying cloud native applications. To adequately secure containers, you must also secure images, hosts, runtimes, registries, and orchestration platforms.

Containers are replaced frequently, making the processes associated with remediating vulnerabilities much simpler. On the other hand, container security is made more complex by the frequency of updates and the high quantity of containers most organizations have. Each update is an opportunity for vulnerabilities to be introduced. Most images, even those that are custom made, are built on third-party code and thus at risk of third-party vulnerabilities.

Dedicated container security must monitor things such as drifts and rogue containers and continually scan for errors in your container setup.

> **Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.**
>
> —**Jerome Saltzer**
> Communications
> *ACM*

Wrap Security Tightly with Least Privilege

Serverless functions, such as Microsoft Azure Functions are a compute service that enables users to run event-triggered code without having to provision or manage infrastructure.

In leveraging serverless functions, you cede control over most of the stack to your cloud provider. However, you retain control over configuration and the application, and that is where security must come from. This includes applying perimeter security at the function level as well.

Security must be tightly wrapped around your application and applied correctly to each individual resource, function, Azure Blob, etc. IAM roles are critical in ensuring adherence to the principle of least privilege and making your app as secure as possible. Achieving least privilege is always hard, but it's even harder with containers and serverless due to the high quantity of different resources and the frequency with which developers update them.

Shift-Left with Automation

Security needs to work within the operational context of your environment – and that means fast deployments. When new accounts or code are launched, you must automate the necessary security steps, such as launching the firewall, implementing workload protection, automatically creating profiles, and automatic remediation. Security must be automated because the agile development process it's integrated with is also automated. Manual intervention is incompatible.

Provide DevOps with toolsets to evaluate security posture, configuration guidance, alerts, and governance during CI/CD, and integrate within the developer's toolchain to make the process as seamless as possible.

Unified security solutions, such as Check Point CloudGuard, Microsoft 365 and Azure security features, and Check Point CloudGuard Dome9, can help you ensure your security protections scale while keeping pace with all changes to your cloud.

Automate File Security

To secure your cloud, you need visibility into users' actions. Using a SaaS management platform, you can automatically scan files for sensitive data and enable alerts when configurations are made that might increase risk, and then automatically remediate.

Instead of just blocking everything, effective security pros need to take action to notify users or work with them to understand what they're trying to accomplish.

04 Monitor and Investigate

Securing Your Cloud at Scale

To secure your cloud, you not only need to secure data across disparate systems such as Azure Files and SaaS apps, you need to do it at scale. Scale brings an additional challenge as the scope of the threat landscape is accelerating simultaneously as many organizations are accelerating cloud adoption.

A June 2020 451 Research survey states, **"One of the main characteristics of effective security operations is the ability to perform at high velocity and with maximum efficiency. This is becoming increasingly difficult to achieve and maintain considering the ever-expanding and complex IT ecosystem, staffing shortages, the evolving threat landscape and the growing number of disconnected point security products."**

Organizations need threat protection across multiple vectors:

- Network
- Endpoint
- Log sources
- Applications
- User behavior
- Cloud

Securing your public cloud requires continuous assessment and protection tightly integrated into the infrastructure and apps. You must monitor threats at scale in addition to achieving complete visibility, deploying securely, and verifying. An automated Continuous Security Monitoring solution constantly watches events and applies smart filters to help you see what matters. Managed security services, such as those offered by ATS, take a comprehensive approach to detecting threats and attacks before they happen, which includes use of a Unified Security Management (USM).

The Insidious—and Deceptive—Risk of Insider Threats

Many organizations are concerned about the risk of malicious insider threats, such as disgruntled employees committing sabotage or stealing intellectual property. However, the greatest risk lies with employees who are well-meaning, but negligent. And unfortunately, this group is sizable.

Some organizations use a Cloud Access Security Broker (CASB) to understand what cloud services their employees are accessing, which might be outside the acceptable SaaS solutions of the organization and with whom they are sharing documents. In the "State of the Insider Threats in the Digital Workplace 2019" survey conducted by BetterCloud, 91% of respondents felt vulnerable to insider threats. Even those who had deployed technologies to combat those threats still felt vulnerable, including 95% of those using a CASB.

In most cases, it's all too easy for well-intentioned users to make choices that increase risk and make your organization incompliant. It's important to gain visibility into the choices users are making in apps, such as sharing confidential documents with external consultants or making public cloud databases freely accessible via the internet. You need to be alerted to certain configurations that might increase risk, and, ideally, be able to automatically remediate.

Context, again, is key. A SaaS management platform can provide such alerts and enable you to build flexible workflows to cope with security risks differently based on the context, such as the user's department and seniority.

Threat Hunting

Threat hunting is the practice of searching for cyber threats that might otherwise remain undetected in your network. According to Infosec, “Cyberthreat hunting can be quite similar to real-world hunting. It requires a uniquely skilled professional possessed of considerable patience, critical thinking, creativity and a keen eye for spotting prey, usually in the form of network behavior abnormalities.”

Threat hunting is necessary because, unfortunately, no cybersecurity solutions are always 100% effective. Additionally, successful attacks frequently remain undetected. A recent study by the Ponemon Institute on behalf of IBM found that the average time required to identify and contain a breach is 280 days.

To hunt threats, you need to collect enough quality data, use tools to analyze it, and have the skill to make sense of it all to search for patterns and potential indicators of compromise (IOCs). Some of the tools that help you detect threats virtually anywhere include USM Anywhere from AT&T Cybersecurity, which centralizes security monitoring of networks and devices in the cloud, on premises, and in remote locations.

Vulnerability Assessment & Penetration Test (VAPT)

VAPT tests the efficacy of your existing security controls to show you how real attackers could exploit your organization’s vulnerabilities. Automated scans can detect some vulnerabilities, but VAPT services go further to find flaws in custom code, business logic, and more. Comprehensive VAPT methodologies include internal vulnerability assessments as well as external penetration testing. The output is a prioritized list of not only what to fix, but when and how to fix it.

Selecting a Cloud Security Services Provider

With the complexity of cloud services, it's advantageous to have the support of an experienced services provider. ATS has over two decades of continuing commitment to high-quality technology services to help clients innovate and improve IT operations.

ATS can design the systems with secure solutions, help you develop a plan, and work with you to implement policies and best practices, including a plan for incident response and recovery.

Services Include:

- Continuous Security Monitoring (CSM)
- Vulnerability Assessment and Penetration Test (VAPT)
- Security Consulting
- Security Awareness Training

Microsoft has many cybersecurity features built into their Azure and Microsoft 365 offerings. An experienced Microsoft Gold partner like ATS can ensure those features are active and configured properly.

FAIRFAX

2751 Prosperity Ave
Suite 600
Fairfax, VA 22031

NEW YORK

140 Broadway
Suite 2410
New York, NY 10005

(888) 876-0302
info@networkats.com
networkats.com