FORTRA™

Cloud Watching: Implementing Strategic Cloud Security

Cloud Watching: Implementing Strategic Cloud Security

Cloud computing has brought new possibilities—and new challenges—to IT teams worldwide. From data storage and transfer to hosting websites and running applications, the cloud supports expansion and flexibility for many common IT functions in a cost-effective manner.

The reliance on cloud platforms will only continue to increase. According to Gartner, cloud services are expected to grow to over $700 billion by the end of 2024—a staggering 47% growth from 2022. They also predict that by 2025, more than 85% of organizations will operate by the "cloud-first" principle when adopting platforms. Businesses will soon be unable to run without some sort of cloud component.

> Gartner predicts that by 2025 more than 85% of organizations will operate by the "cloud first" principle.

Why Attackers Target the Cloud

Unfortunately, with all the benefits of the cloud, many have developed blind spots when it comes to security. The 2023 Cloud Security Report by Cybersecurity Insiders indicates that 76% of organizations survey have experienced a public cloud security incident, in the last year. The most frequent reason for a breach is due to misconfigurations, which is only exacerbated by the fact that 72% of surveyed organizations have a multi-cloud solution, making consistent configuration more challenging.

Lack of qualified staff and strict budgets also contribute to security issues. Additionally, increased adoption means cloud environments house a great deal of sensitive data. The combination of these factors, combined with poor security measures, has made the cloud highly valuable and relatively easy to attack.

Reducing cloud infrastructure risk requires IT teams, providers, and trusted vendors to work collaboratively to establish and implement comprehensive security policies.

Cloud Security: Who is Really Responsible?

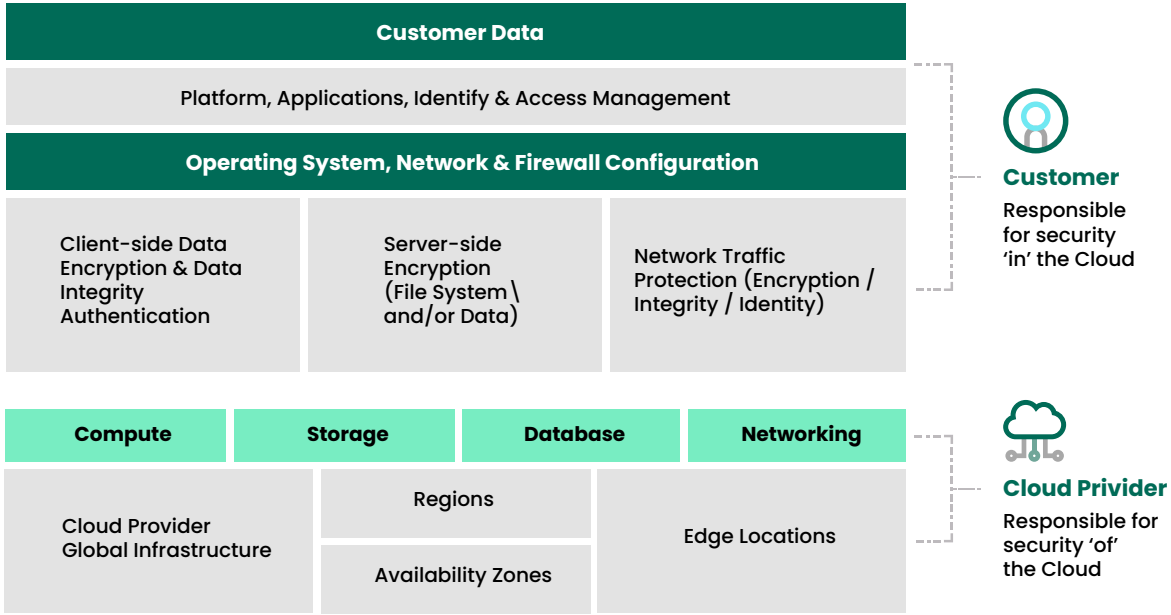
In cloud security, many customers assume that the cloud provider handles everything. Although major cloud computing providers such as Amazon Web Services (AWS), Google, HP, Microsoft, or IBM have built-in security capabilities, these platforms still require regular verification and updates by IT security teams to remain secure.

In reality, cloud security is a shared responsibility model between the provider and the user. The cloud service provider (CSP) creates a secure foundation for the user, but this is only the baseline.

The user's portion of the shared responsibility is critical for maintaining a secure and compliant cloud environment. Responsibilities of the user in this model can include:

In reality, cloud security is a shared responsibility model between the provider and the user. The cloud service provider (CSP) creates a secure foundation for the user, but this is only the baseline.

1. **Configuring security settings:** Configuring cloud resources such as firewalls, databases, storage, and services is crucial for a secure cloud.
2. **Securing user access:** The cloud customer must manage access efficiently, maintaining only active accounts and tailoring permissions to users' needs.
3. **Securing data:** In order to maintain privacy, users must take primary control of their data and its security. This means users must take care to encrypt data, have data loss prevention processes in place, and more.
4. **Testing security:** Cloud security is not one and done. Users must conduct ongoing assessments of their cloud environments with offensive security measures like vulnerability scanning, pen testing, and red teaming.



Responsibilities may be further muddied by a multi-cloud or distributed environment. For example, data may be created on-premises, stored in a cloud, and used for development in another. This can require coordination with several providers, each with different policies on who is in charge of what. The shared responsibility model requires customers to proactively and diligently manage the security for every one of their cloud environments, including regular assessments.

The Consequences of Poor Cloud Security

Failure to implement processes to proactively validate and test cloud environments can leave the most reputable providers susceptible to security breaches. Small misconfigurations or security setting errors can expose sensitive data to attackers or wayward employees. The consequences of such exposures can be severe, including millions in fines, reputational damage, lost customer trust, and legal fees.

The price organizations pay for breaches of their cloud environments is steep, and can include:

- **Loss or theft of IP:** Your company's information, whether that includes product specifications, strategic initiatives, employee details, or customer contacts, is not something you want made available for all to see.
- **Time and Revenue:** Recovery from a breach is a slow, often years long process that not all companies survive—many end up going out of business within six months of a breach. Those that do survive will need to brace themselves for an arduous process that takes up significant resources, even taking time away from projects that are focused on primary business goals and functions. Additionally, customers will likely stay away, at least for a while, following the news of a breach or other security-related incident. For websites hosted in the cloud, the cost of downtime can be enormous.
- **Loss of Customer Trust:** Whether your company is a household name or a trusted brand in a niche market, your customers should feel confident you are doing everything in your power to protect their sensitive data. The last thing you want is for customers to hear your company has sloppy security standards or that their protected information has been open to the public on the internet. There are certainly better and worse ways to handle a data breach should it occur, but prevention is always the best route.
- **Compliance Violations:** Regulatory requirements such as Sarbanes-Oxley (SOX), GDPR, HIPAA, and PCI DSS mean that specific measures need to be taken to protect sensitive data. Violations of these rules can subject you to fines, firings, audits, and legal action.
- **Settlement Costs:** Depending on what data was exposed, you may be required to pay fines and comply with breach notification laws—an expensive and time-consuming project that carries the added burden of damaging your organization's reputation. For example, the Equifax data breach from 2017 resulted in a $700-million settlement, announced by the Federal Trade Commission in July 2019. The data breach, which impacted nearly 147 million people, according to the Equifax Data Breach Settlement website and reported by the Los Angeles Times, is one of the largest data breach settlements ever recorded.

Cloud Security Breach Examples

Below are examples of cloud security breaches. No industry is spared, making the need to prioritize cloud cybersecurity universal.

Transportation Misconfigurations:

Confidential flight data, crew information, and Electronic Flight Bag (EFB) source code were exposed after the breach of an airline's cloud database. Attackers were able to gain access to the data after discovering their AWS bucket did not have proper security configurations. Additionally, an automotive company discovered a misconfigured cloud environment had led to vehicle and customer data being exposed for over eight years.

Unsecured Database:

An adult website disclosed 200 million records for 64 million users, disclosing information about performers and customers engaging with the service. The disclosure was due to an unsecured Elasticsearch database easily accessible to the public internet and discovered by an independent researcher.

Healthcare Under Siege:

One cloud-based electronic health records (EHR) vendor disclosed a data compromise stemming from stolen credentials. As healthcare increases their digital footprint with more remote and online care options, the reliance on cloud services has grown substantially, creating a larger attack surface and not enough personnel to manage it. Additionally, EHR are frequently stored in cloud environments. Attackers know this and hunt for EHR-rich targets.

Cloud Experts Exposed:

Cloud providers are also not immune. One cloud provider had to inform their customers that all of their data was lost after a ransomware infection that likely occurred in the midst of moving datacenters. Though data wasn't stolen, the provider's refusal to pay resulted in permanently frozen cloud servers.

Government Agencies Attacked:

A city's law enforcement agency had over 20 terabytes of data stolen from their cloud database. The information, which included sensitive data including names, addresses, ID card numbers, and criminal case details, was placed for sale on the internet. The breach is alleged to have been achieved after a dashboard for managing the database was left open on the internet, with no password needed for access.

A Cloud Security Check List

As the cloud becomes prevalent in nearly every aspect of business, cloud security becomes an increasingly larger endeavor to manage. It can be easy to overlook areas that need to be regularly assessed. Consider the following areas when developing your cloud security processes:

User and group configurations

- ✓ Who has access to your systems, from where, and what rights have they been granted?

Network settings

- ✓ How are people able to access your systems and services—through what ports and protocols?

Critical system services status

- ✓ Are all your critical services such as auditing and firewall restrictions on?
- ✓ Are all non-necessary services disabled and blacklisted?

Privileged log-on and password policies

- ✓ Who has access to perform administrative functions?
- ✓ Are your credential policies hardened to the level required for the criticality of your data?

Data transfers and malware protection

- ✓ Are your data transfers performed securely in an auditable fashion?
- ✓ Are unencrypted file transfers of any type allowed into your system?
- ✓ Are your systems protected from ransomware and malware attacks by native anti-virus solutions?
- ✓ Vulnerability management and prioritization
- ✓ Are you aware of what vulnerabilities are present and posing the greatest risk to your cloud environment?
- ✓ Do you have intelligent remediation plans in place to close the most critical security gaps?
- ✓ Defensive practices
- ✓ How often do you have security awareness training or simulate phishing campaigns to ensure cloud users are using security best practices?
- ✓ Do you run red teaming exercises to test the defensive processes of your security team?

Infrastructure discovery and documentation

- ✓ Is your DevOps team deploying systems without your knowledge?
- ✓ Are proper security controls immediately deployed to all systems as they are created?
- ✓ Do you have automatic discovery and documentation of all your cloud assets?
- ✓ Are you instantly alerted when a new system is created in your cloud environment?

Auditing and reporting

- ✓ Can you produce an audit report showing the state of your system's security.
- ✓ Can you produce such a report for all systems, even the ones you just deployed?
- ✓ Historically, how did it look last week or last month to satisfy your auditors?

Proactively Keep Tabs on Your Cloud Security

Cloud security is an essential part of IT infrastructure management, and an offensive security approach is critical in proactively monitoring your cloud security. Assessing your cloud security posture can help identify potential vulnerabilities before they are exploited.

Regular vulnerability scans are a crucial component of cloud security. Choose a scanner that doesn't rely solely on CVEs to identify vulnerabilities and includes some cloud-specific scans. Advanced scanners have cloud-specific scans as a part of a more holistic scanning solution that identifies and prioritizes vulnerabilities using external intelligence. Scheduled, automated penetration tests build on vulnerability scanning by testing the effectiveness of your security controls. They help identify weaknesses in your system that attackers could exploit and identify the sensitive data they can access through a breach. Security teams can use automated tools to conduct penetration testing, efficiently streamlining their testing efforts.

Red Teaming is another way to test your defenses by simulating a real-world attack on your cloud infrastructure. This approach involves using highly skilled security professionals who act as attackers to identify weaknesses in your system. These red team security services are an in-depth way to uncover attack avenues with specialized red teaming tools.

An Offensive Approach to Security with Fortra Solutions

Cloud servers offer an effective, scalable way to provide access to your organization's data. However, with threat actors looking to take advantage of weaknesses like vulnerabilities, misconfigurations, or simple human error, security teams must be on the offensive. With both the sensitive information you house as well as your organization's reputation at stake, it's critical to routinely evaluate security for cloud environments.

With the incidence of misconfigurations and simple human error—in addition to hackers looking for vulnerabilities at every turn—IT security teams must create a proactive strategy that includes offensive security tools. **Learn more about offensive security solutions from Fortra.**

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-gd-0923-vm-r2