helpsystems

The Truth About Cloud Security

The Cloud: A Double-Edged Sword

Cloud computing has brought new possibilities—and new challenges—to IT teams worldwide. Many have eagerly expanded their capabilities and capacity via cloud servers or a hybrid approach of on-premises and cloud environments.

In fact, Forrester predicts that 2018 will be a tipping point for cloud usage. In a November 2017 blog post, Forrester Vice President and Principal Analyst Dave Bartoletti wrote that the firm expects more than 50 percent of global enterprises will rely on at least one public cloud platform.

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.

Unfortunately, with all the benefits of the cloud, many have developed blind spots when it comes to security.

In LinkedIn Group Partner's Cybersecurity Trends 2017 Spotlight Report, only 53 percent of respondents said they'd be able to resist cyber threats in their cloud infrastructure and applications. In addition, only 24 percent routinely monitor cloud instances for security risks, meaning a cybersecurity attack could go unnoticed on most systems.

The fact is, the cloud isn't inherently secure, even if you're working with a well-known cloud computing provider such as Amazon Web Services (AWS), Google, HP, Microsoft, or IBM. Security capabilities are built into these platforms, but IT security teams often fail to verify or update them over time.

The tiniest fissure in your cloud security settings can have disastrous consequences. A simple mistake or misconfigured security setting can expose sensitive data to attackers or wayward employees. A breach like this can cost your organization millions in fines, reputational damage, lost customer trust, and legal fees.

only
53%
of global enterprises are able to resist cyber threats in their cloud infrastructure and applications

The fact is that when it comes to using the cloud effectively to protect the data in its realms, IT teams, cloud providers, and trusted vendors need to work together to establish and implement well-thought-out policies to keep data secure.

The Cloud Has Given Us a False Sense of Security

IT teams are commonly some of the busiest people in any organization. They're short staffed and increasingly lack cybersecurity expertise. The result is that staff in charge of sensitive information may not know how to handle security in this ever-changing world of threats, hackers, and data stored both on the server in the next room and on the other side of the country in the cloud.

It's all too common to have a programmer or developer spinning up a new server, partition, or instance without understanding the predetermined security policies that should be applied before it can be used to store data effectively and securely. And that's where things start to break down.

Although it may sound obvious that it's important to check security settings for cloud servers, recent incidents such as those noted below suggest that IT professionals mistakenly believe data in the cloud is inherently more secure.

2017 was a banner year when it came to the number of high-profile data breaches and leaks for information stored in the cloud. Several of these incidents were caused by little more than human error—a series of blunders reminding us that simple misconfiguration can precipitate unforeseen events just as much as malicious hackers carrying out cyberattacks.

Below are several of the recent headline-making stories that have jolted businesses and their customers awake when it came to the downfalls of cloud usage.

Consumer database exposure: Data analytics firm Alteryx and its partner, the consumer credit reporting agency Experian, left exposed a cloud-based data repository that contained sensitive information about more than 120 million American households. This repository was accessible to anyone with an AWS account who knew the URL. No names were exposed, but each record contained 248 data fields (including address and income), making it very easy to link the data to specific individuals.

Scottrade data breach: 20,000 Scottrade Bank customers learned that their passwords had been left open to the public due to the negligence of a third party, Genpact. A file of plaintext information had been uploaded to a cloud server without the proper security controls in place.

AWS outage: The Amazon Web Services outage in February 2017 ostensibly "broke" the internet after an employee performed well-meaning maintenance and botched codes. It was labeled a typo. The outage affected well-known companies such as Netflix and Airbnb and brought into clear focus the impact of simple mistakes.

The Pentagon's web monitoring data: In September 2017, a cybersecurity researcher discovered that a database of 1.8 billion internet posts the U.S. Central Command (Centcom) and U.S. Pacific Command (Pacom) had pulled from social, news, and other forums was open on AWS. Although the publicly available information wasn't sensitive, the fact that the U.S. government hadn't secured evidence of their tracking practices raised questions about how other cybersecurity measures were being handled.

RNC voter data breach: The Republican National Convention's work with data firm Deep Root Analytics ended in disaster following the discovery of an unencrypted database of sensitive information for 198 million voters in the U.S. To add insult to injury, this database was also stored on an unsecured AWS server. The June 2017 breach could have been prevented if the firm had evaluated the cloud for security weaknesses, but it didn't.

Verizon leak: The PINs, names, addresses, and account information for more than six million Verizon customers were openly available the same month due to a misconfigured data repository. It took Verizon more than a week to fix the issue and caused untold damage to their brand.

How Do Security Settings Become Misconfigured?

According to Gartner, 95 percent of security issues and failures of cloud services in 2020 will be the fault of the customer, rather than the service provider.

This is quite a wake-up call for IT teams that feel confident their cloud computing partner has their back when it comes to securing the information stored in the cloud.

> *Unlike other cases involving breaches of government data, the case in Sweden does not appear to involve hacking or other malice. Instead, the focus has been on an apparent absence of proper safeguards and oversight.*

What often happens is that even when security policies are properly configured at the start, they can be changed accidentally or intentionally at any time. These changes can go unnoticed for days, weeks, or months. Meanwhile, the information your team thinks is secure is actually accessible by anyone who either stumbles upon it on the public cloud or searches for it with malicious intent.

Is Outsourcing Cloud Security a Good Idea?

By uploading data to the cloud, you're essentially outsourcing your security to the cloud provider while retaining all the risk. The onus is on you to ensure your cloud server is properly configured.

Neglecting your cloud security configuration can have disastrous consequences. The world learned in July 2017 that the Swedish Transport Agency was responsible for a massive breach of confidential information, including details about Swedish infrastructure and possibly the identities of undercover agents. This had occurred when a vendor, contracted to manage databases of sensitive information, failed to adopt the appropriate cloud security safeguards. In fact, they had free rein to pass over security clearance for credentialing any users they saw fit due to the complete deference of leadership at the Swedish Transport Agency. This enabled their vendor's employees in Eastern Europe to access classified information with no trouble.

Swedish Prime Minister Stefan Lofven called the breach of information "a total breakdown." He said: "It is incredibly serious. It is a violation of the law and put Sweden and its citizens in harm's way."

The Consequences of Poor Cloud Security

The data breach at the Swedish Transport Agency threatened national security, and data breaches at private organizations can also have serious consequences. In the 2017 Ponemon Cost of Data Breach Study, researchers put the average cost of a data breach at $3.62 million. One industry expert estimates the cost of the 2013 Target data breach will reach $1 billion by the end of 2017. Most companies can't afford the aftereffects of a small breach, much less one reaching the billion-dollar mark.

Here are some of the most common ways a misconfigured cloud server can affect your organization:

Data breaches

When external hackers or unauthorized insiders gain access to protected information, you've suffered a data breach. Depending on what data was exposed, you may be required to comply with breach notification laws—an expensive and time-consuming project that carries the added burden of damaging your organization's reputation.

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.

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.

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.

Lost revenue

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. One report estimated that one hour of downtime costs Netflix $200,000.

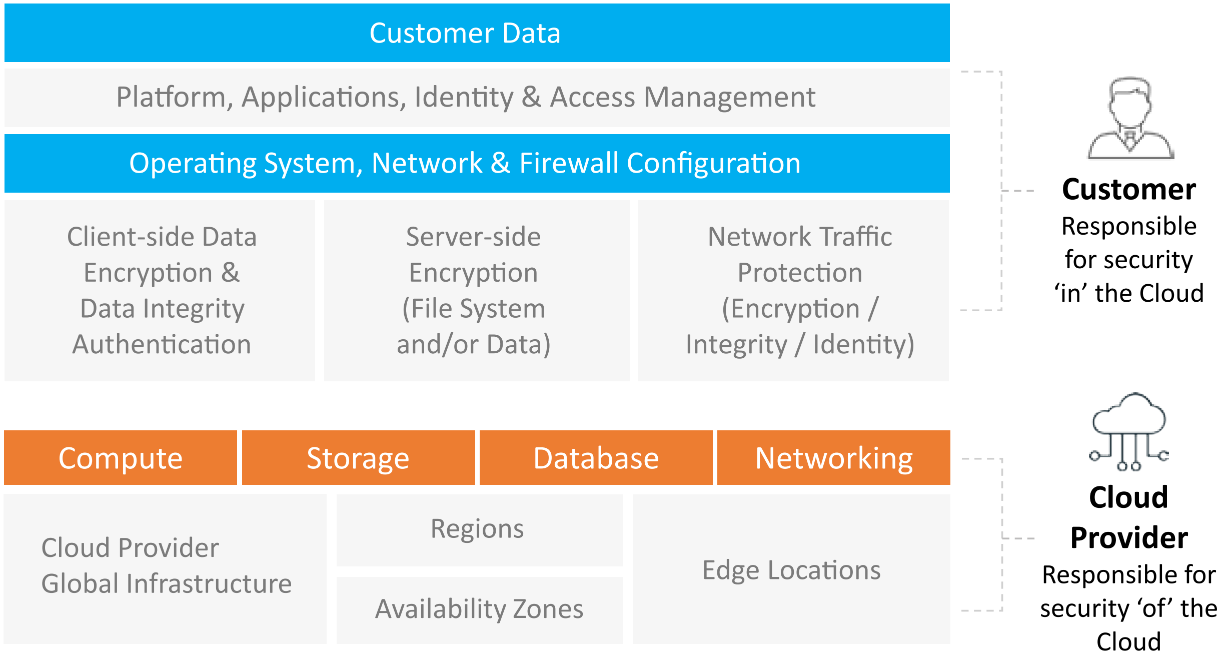
Settlement costs

Anthem announced in 2017 that it would pay $115 million to settle consumer claims related to the 2015 cyberattack that affected the data of 78.8 million customers.

Do Cloud Providers Offer Strong Security?

Vendors such as AWS (Amazon Web Services) proudly tout security capabilities such as firewalls, data encryption, and identity and access control on their sites. AWS also discusses the latest news in its security blog. The important thing to remember is just because cloud providers offer high levels of security doesn't always mean policies are in place at all times.

Settings can inadvertently be changed over time as more and more people gain access to that cloud infrastructure. Think of cloud security as being jointly owned by the cloud computing provider and your IT team (as well as trusted third parties you work with). This is called the "shared security model."



Customer Data

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption & Data Integrity Authentication

Server-side Encryption (File System and/or Data)

Network Traffic Protection (Encryption / Integrity / Identity)

Customer Responsible for security 'in' the Cloud

Compute | Storage | Database | Networking

Cloud Provider Global Infrastructure

Regions

Availability Zones

Edge Locations

Cloud Provider Responsible for security 'of' the Cloud

As shown in the graphic above, AWS or your cloud provider of choice is responsible for the security **of the cloud** and you as the end user are responsible for your own security **in the cloud**.

Security Settings Require Regular Attention

As with any server, cloud security is not a set-and-forget project; cloud servers require regular attention to ensure they are configured properly. Having a documented security policy is an important step in this process, and including cloud servers alongside on-premises instances means they won't be overlooked during periodic check-ups.

Regular monitoring of every server's security settings means that any altered configurations can be caught early and rectified before they cause the potential for harm or intrusion. This step also helps eliminate simple human errors, particularly when automated detection software is in place.

To help you get started, to the right is a list of issues to consider when configuring your cloud security settings:

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?

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 systems 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 auitors?

Keep Tabs on Your Cloud Security with Confidence

IT administrators are often overburdened with tasks or lack the security expertise for the ever-growing needs of managing cloud infrastructures. With new cloud instances spun up every day, it’s impossible to manually keep tabs on cloud security settings.

A simple solution is to turn to proven tools that automate security administration and compliance tasks as well as manage scripts across servers both on premise and in the cloud. Policy Minder from HelpSystems is a Linux, IBM AIX, and Windows security administration and compliance reporting product. It simplifies and automates security administration tasks and compliance reporting requirements from an easy-to-use, web-based console.

Policy Minder enables you to:

- Document your security policy automatically
- Automate security policy adherence
- Make changes across multiple servers at the same time, manually or automatically
- Manage compliance with security policies from a single screen

> *Policy Minder reminds me of any policy exceptions every day, so nothing slips through the cracks. We're doing more with less, and we don’t want to go looking for the problems, we want them to come to us. Policy Minder accomplishes that for us.*
>
> **Steve Mulder,**
> **Lead Systems Support Specialist, Amway**

Conclusion

Cloud servers offer an effective, scalable way to provide access to your organization's data—but you can't overlook the need to protect them with a properly administered security policy.

However, with the incidence of misconfigurations and simple human error—in addition to hackers looking for vulnerabilities at every turn—IT security teams must be on the offensive. It's critical to routinely evaluate security for cloud environments to ensure the proper settings and precautions are in place. The sensitive information you house as well as your organization's reputation are at stake.

Request a Free Security Scan

HelpSystems can help you simplify and automate your approach to security in the cloud, on premises, and in hybrid environments. Request your free Security Scan at https://www.helpsystems.com/cta/free-network-security-vulnerability-scan to identify security configuration errors and vulnerabilities.

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.