sonraí SECURITY

The Anatomy of 5 Notorious Cloud Data Breaches

sonraí SECURITY

Table of Contents

Identity and authentication for data storage 4

Public cloud misconfiguration 5

Keys and secrets management 8

Overprivileged Identities 9

Insider threats 11

The damage of a data breach 13

It has been a year of shocking security breaches in the cloud. Gartner updated their evaluation of cloud security and concluded: “Through 2025, 99% of cloud security failures will be the customer’s fault.” This is a sobering thought.

The cloud is undeniably the future, and it can be secured with a bit of wisdom and some best practices that are newly evolving as this technology matures. We dissect the anatomy of five notorious cloud data breaches to share a bit of wisdom from our research.

There are five main ‘patterns’ of cloud data breaches. Each of these causes shares common characteristics. “For each pattern, there has been at least one notorious breach associated with it,” says Dan Woods, Principal Analyst at Early Adopter Research, in a recent Sonrai Security webcast. “For cloud security, there is little room for error.”

In this eBook, we dissect the following patterns:

- Identity and authentication for data storage
- Public Cloud misconfiguration
- Keys and secrets mismanagement
- Overprivileged identities
- Insider threats

The challenge is that the threat source and methods are constantly changing and a given threat may or may not rear its ugly head right away. Knowing how data breaches happen and how to prevent them from happening is key when it comes to defending your identities and data access. To understand the problem, it is important to see how it continues to evolve and the patterns that appear.

Data Breach Pattern: Identity and Authentication for Data Storage

One of the five major causes of cloud data breaches is weak authentication for data storage. This might include the lack of multi-factor authentication or insecure storage of the database credentials used by an application.

A common mistake is where you have a database on-premise and just your small team uses it, so you don't put authentication on the database. You move that database to the public cloud, someone makes a mistake and assigns it a public IP address and, all of a sudden, it ends up exposed on the Internet. At this point, anyone or anything that can find it can get access to it.

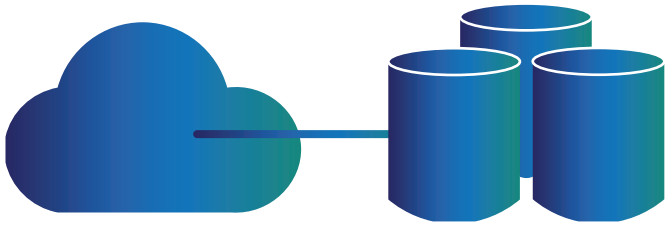
Unfortunately, we witnessed this mistake of weak authentication when an email platform company experienced a major data breach in March 2019. The breach included the names and email addresses of over 2 billion records released into the public domain. it's also easy for attackers to identify an unprotected database that might be exposed, but It's easy to accidentally let a storage depository out too.

Data Breach Pattern: Public Cloud Misconfiguration

Misconfiguration means that the public cloud instances, such as storage and compute, are configured in an organization's IT team in such a way that the servers are vulnerable to breaches.. One of the most dangerous misconfigurations provides the public with access to storage buckets, which are unprotected by traditional authentication procedures, such as passwords. In each of the scenarios below, data can be accessed. It is a challenge for DevOps to avoid the three major types of misconfiguration because configuring the cloud.

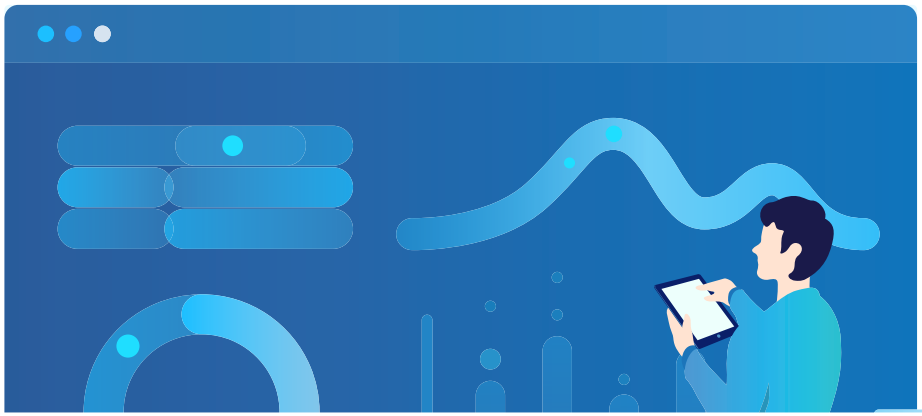
There are three main classifications of common misconfigurations in AWS to consider; **security group, access restrictions,** and **permission control misconfiguration**. Some organizations don't completely understand the configuration of the AWS "out of the box".

A real world example of this type of cloud data breach is the unfortunate story of Nice Systems. Nice Systems experienced a data breach that exposed 14 million phone records on an unsecured AWS server. The server was open to the public for anyone who stumbled upon the URL, containing logs of customer service calls, names, phone numbers, and PINs.



Data Breach Pattern: Public Cloud Misconfiguration

Most people you talk to don't know that a misconfiguration can happen in Azure, but it can. By far the most common misconfiguration in Azure when it comes to user access control is giving people more permission to cloud resources than is required to do their job. Microsoft's Role Based Access Control (RBAC) provides fine-grained access control which can be applied to cloud resources hosted in Azure. When possible, do not create custom roles with subscription ownership. It is recommended to use the principle of least privilege, assigning only needed privileges to the necessary resources or resource groups instead of allowing full administrative access to everything in a subscription.

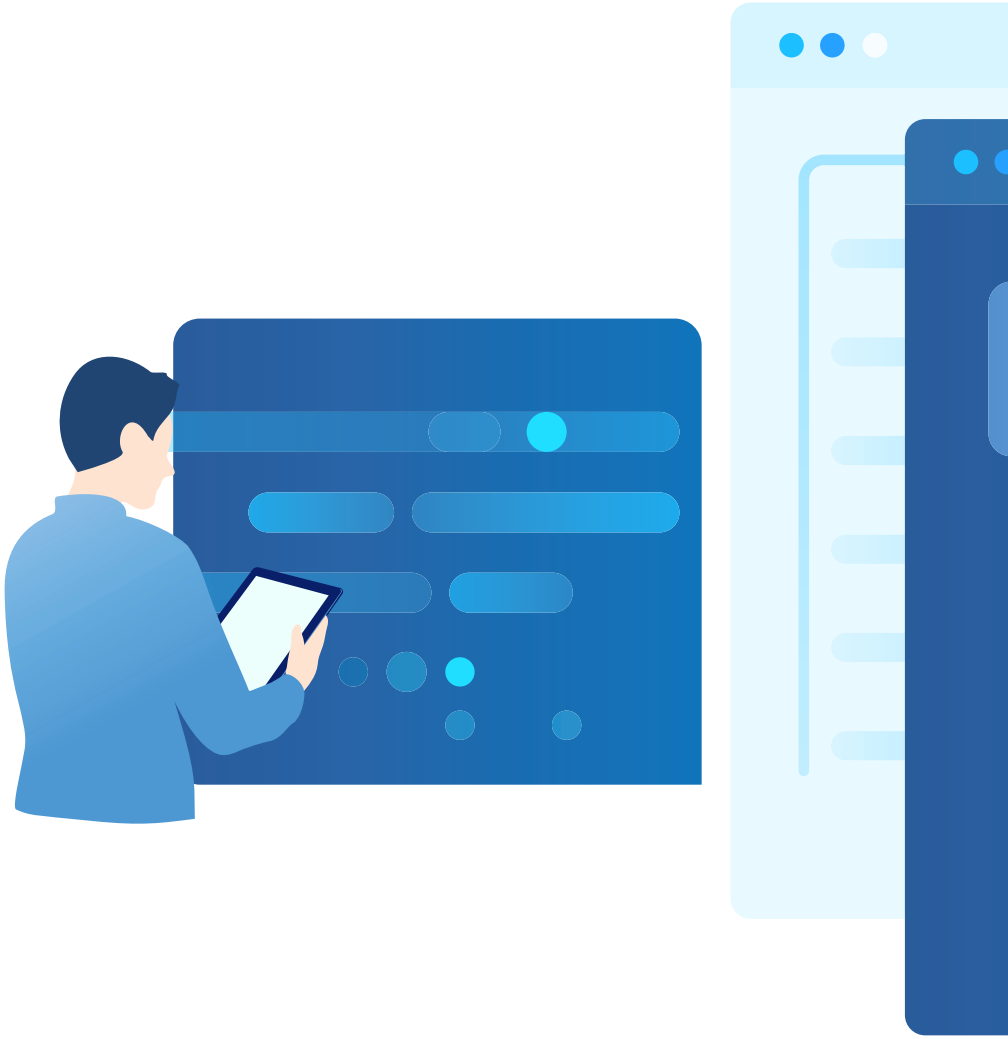


A real world example of this type of cloud data breach is the unfortunate story of TrueDialog, an American communications company. Based in Austin, Texas USA, TrueDialog creates SMS solutions for large and small businesses and currently works with over 990 cell phone operators and reaches more than 5 billion subscribers around the world. The TrueDialog database, hosted by Microsoft Azure, included 604 GB of data. This breach included nearly 1 billion entries of highly sensitive data.

Data Breach Pattern: Public Cloud Misconfiguration

Misconfigurations can happen in Google Cloud too.
Misconfigurations can happen in Google Cloud too. Some common mistakes include, firewall rules that are configured to be open to public access, cloud storage buckets that are publicly accessible, instances configured with public IP addresses, instances with SSL not being enforced, and resources where the Web UI isn't enabled.

A real world example of this type of cloud data breach can occur with any organization. A staggering new report from CyberNews claims the discovery of an unsecured database comprising 800 gigabytes of personal user information, including more than 200 million detailed user records. This unidentified database exposes 200 million Americans due to a database that was hosted on a Google Cloud server that was exposed to the internet and did not require authentication to gain access.



Data Breach Pattern: Keys and Secrets Management

People who access unauthorized keys and digital authentication credentials, such as passwords, APIs, and tokens ("secrets") can accidentally expose a company's most valuable data on the internet. Organizations need to keep all the information contained in services, apps, privileged accounts, and other parts of the cloud ecosystem secure, otherwise, they could jeopardize their entire business.

A Security vendor had this problem in August 2019, when a series of unfortunate events resulted in one of the biggest cloud data breaches of the year. A misconfiguration of AWS allowed hackers to steal information from customers using the company's Cloud Web Application Firewall (WAF) product.

Attackers stole an administrative API key from one of the security vendor's AWS accounts and accessed a database snapshot that contained hashed and salted passwords, email addresses, and some customers' TLS and API keys.

This can be a common scenario: Someone accidentally checks a key into a public GitHub repository. Within an hour or two, people can quickly clone that whole repository.

As you can see, **a simple mistake can have a significant impact on data security**. In the security vendor example, they had been doing some testing with the cloud. They had taken a snapshot of the database they had and moved it up into a test account. Even though it was only a test account, it had real data on it.

Data Breach Pattern: Overprivileged Identities

72%

of organizations say they have “stealthy admins”

You’ve heard the age-old adage, “Too many cooks spoil the broth,” but what about too many admins?

Or IT users with access to more data than they require? This is an ongoing debate in identity management: Users with too many administrative privileges — “overprivilege” — can make it difficult for organizations to properly manage user identities and data access.

Overprvilege is a growing problem:

Too many users with excessive administrative privileges with 72 percent of organizations saying they have “stealthy admins”. The problem is, many organizations struggle to control overprivileged identifies, and this causes issues in cloud environments and risks major data breaches.

The biggest?

Probably the aforementioned major financial institution SSRF attack, where an attacker obtained bank accounts and government I.D. numbers in one of the largest data breaches in history.

Data Breach Pattern: Overprivileged Identities

59% of business leaders saying privileged administrators and IT users pose the biggest security risk to their organization, there are lessons to be learned from this type of breach.

Unfortunately, there was a crack in the armor and once exploited it was an over privileged Identity that enabled the breach. The attack impacted around 100 million American and Canadian customers, causing this financial institution to crank up their cloud security credentials.

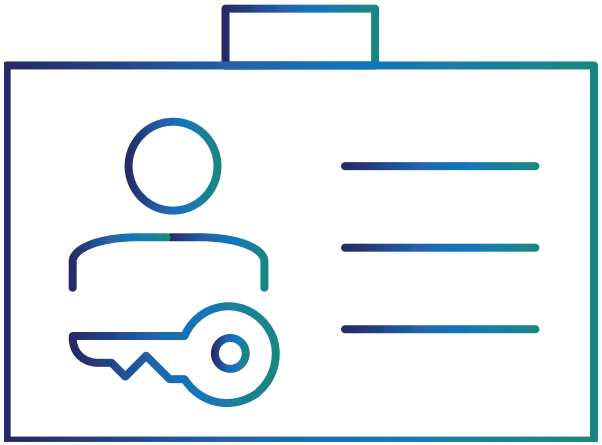
It wasn't the fact that somebody stole a key through a piece of malware, or somebody gained access to a system with no authentication on it. This was a case of overprivilege. The attack impacted around 100 million American and Canadian customers, causing this financial institution to crank up their cloud security credentials.

When it comes to the cloud, the problem is that getting to least-privilege can be complex, often times much more complex than a traditional environment, and people get frustrated when things break and it is difficult to debug. So they relax the privilege of the Identities to "get it working", which can lead to this type of data breach.

We recommend organizations define adequate privilege for each account and workload, establish protections for highly-privileged accounts, and continuously monitor for changes within the organizations. In addition to this, build in multiple layers of defense should one control fail the damage that can be done is minimized.

Data Breach Pattern: Insider threats

The fifth major cause of cloud data breaches might surprise you.
The media warns people about the dangers of sophisticated hackers who can expose an organization's sensitive data, but current and former employees can pose just as much of a threat. Research suggests that these "insiders" are responsible for at least 40 percent, and as much as 75 percent, of all data breaches.



The example of Steffan Needham from Manchester, United Kingdom, who was jailed for 2 years for wiping his organization's critical cloud data highlights this type of breach. Needham worked as an IT consultant in digital marketing and software agency Voova in 2016. After the company sacked him for poor performance, he used a co-worker's AWS account to access 23 different servers, where he deleted valuable customer information.

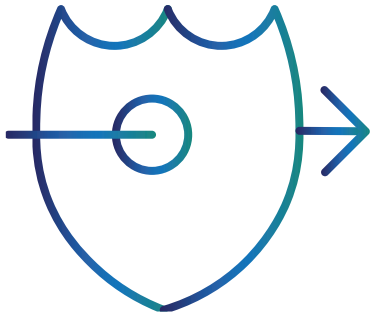
This is an example of privilege escalation. A malicious user gains access to another user's privilege in the same target system. Businesses will also need to avoid something called "toxic combination," which can happen when someone gains unnecessary access rights. Both can have a detrimental impact on an organization.

Data Breach Pattern: Insider Threats

Unfortunately, Voova suffered a massive loss from this, and they actually started losing contracts because projects were deleted. We've also seen the pattern where someone, who knows they are going to be removed from a company, creates an alternative identity. This identity lies dormant until it is ready to be accessed and create havoc.

How can you avoid a similar situation?
Separation of duties for critical data activities is "vital." Some security architecture makes this separation difficult, so root accounts are required for some functions. As well as a separation of duties, organizations should monitor dormant identities and delete an employee's access when he or she leaves the company.

Ultimately, it's all about trust. You should work toward a "zero-trust" or "least privilege" model until you are confident that employees warrant privileges. Monitoring user activity, enabling logs that can't be deleted, and not using administrative privileges for day-to-day activities will reduce risk.



The Damage of a Data Dreach Should Not Be Underestimated.

There's a misconception that the public cloud provides businesses with water-tight protection against security threats, but this isn't the case. Organizations that use providers such as Amazon Web Services, Google Cloud, and Microsoft Azure can be vulnerable to data breaches, and these happen far more often than you think.

25%
file for bankruptcy

37%
experience a significant financial loss after a data breach.

In 2019 alone, billions of records were stolen in cloud data breaches. These breaches impacted organizations of all sizes, but some of the more high-profile ones include:

- **In April,** a digital media company in Mexico exposed more than 540 million Facebook records on an unsecured Amazon Web Services (AWS) server.
- **In September**, hotel reservations management system Autoclerk exposed travel reservation data on an unsecured Elasticsearch database in AWS. Some of these reservations included U.S. government and military personnel data.

Unfortunately, this is just the tip of the iceberg. Many companies never recover from data breaches. Ten percent of organizations go bust, 25 percent file for bankruptcy, and 37 percent experience a significant financial loss after a data breach.

Sonrai Security can help

Cloud data breaches follow distinct patterns that can be studied and learned from. These five patterns of cloud data breaches have happened, in one way or another, to businesses of all sizes, from small companies to major international corporations. Regardless of the size of your organization, you need to take proactive steps to reduce risk and safeguard your most critical data.

Sonrai's public cloud security platform provides a complete risk model of all identity and data relationships, including activity and movement across cloud accounts, cloud providers, and 3rd party data stores. Sonrai's Public Cloud Security Platform provides you with a suite of identity monitoring, data monitoring, and platform compliance so you can improve identity and access governance across the public cloud.

SEE THE PLATFORM

GET A FREE SECURITY ASSESSMENT

On-Demand Webinar : Anatomy of 5 Notorious Data Breaches

Cloud data breaches follow distinct patterns that can be studied and learned from. In this webinar, Dan Woods, Principal Analyst at Early Adopter Research, and Sandy Bird, CTO of Sonrai Security, dissect five notorious and distinct types of cloud data breaches, breaking down how each was caused and how they could have been prevented. Each of these five is an archetype of a family of breaches. This webinar will detail the anatomy of each type of breach, what we can learn, what allowed the breach to happen, and preventative measures.
Breakdown of the 5 breaches:

- Identity and authentication for data storage
- Public cloud misconfiguration
- Key and secret management
- Overprivilege
- Insider threats

Watch Now

About Sonrai Security

Sonrai Security delivers an enterprise security platform focused on identity and data protection inside AWS, Azure, and Google Cloud. We can show you all the ways data has been accessed in the past and can be accessed in the future. Our platform delivers a complete risk model of all identity and data relationships, including activity and movement across cloud accounts, cloud providers, and third-party data stores.

Sonraí Security Headquarters
261 Madison Ave, 9th floor, NY, NY 10017
P: (646) 389-2262 E: info@sonraisecurity.com