**Cloud-Security Data Breach: Stages, Effects and Practices**



**Table of Contents**

[Introduction 4](#_Toc83565646)

[Cloud Security Data Breach 4](#_Toc83565647)

[Stages of Data Breach 4](#_Toc83565648)

[1. Research 4](#_Toc83565649)

[2. Attack 4](#_Toc83565650)

[3. Exfiltration 5](#_Toc83565651)

[Causes of Cloud Security Data Breach 5](#_Toc83565652)

[Security Misconfiguration of a Production Environment 5](#_Toc83565653)

[Lack of Visibility Into Access in a Production Environment 5](#_Toc83565654)

[Improper IAM and Permission Configurations. 6](#_Toc83565655)

[Effects of Cloud Security Data Breach 6](#_Toc83565656)

[Major Cloud Security Breaches 6](#_Toc83565657)

[1. Accenture 6](#_Toc83565658)

[2. Verizon 6](#_Toc83565659)

[3. Booz Allen Hamilton 6](#_Toc83565660)

[4. Republican National Committee Data Breach 7](#_Toc83565661)

[5. Election Systems and Software (ES&S) 7](#_Toc83565662)

[6. Capital One 7](#_Toc83565663)

[7. Docker Hub 7](#_Toc83565664)

[8. Autoclerk 7](#_Toc83565665)

[9. Yahoo 8](#_Toc83565666)

[10. Alibaba 8](#_Toc83565667)

[11. LinkedIn 8](#_Toc83565668)

[12. Sina Weibo 8](#_Toc83565669)

[13. Facebook 8](#_Toc83565670)

[14. Mariott International 9](#_Toc83565671)

[15. Adult Friend Finder 9](#_Toc83565672)

[16. My Fitness Pal 9](#_Toc83565673)

[17. Adobe 9](#_Toc83565674)

[18. Dubsmash 10](#_Toc83565675)

[19. MySpace 10](#_Toc83565676)

[20. NetEase 10](#_Toc83565677)

[21. Court Ventures ( Experian) 10](#_Toc83565678)

[22. State Farm 10](#_Toc83565679)

[Cloud Security Best Practises 11](#_Toc83565680)

[Identity and Access Management Solution 11](#_Toc83565681)

[Backup and Recovery Solutions 11](#_Toc83565682)

[Audit and Optimization of Configurations 11](#_Toc83565683)

[Cloud Security Breach Prevention Technology 12](#_Toc83565684)

[NetApp Cloud Insights 12](#_Toc83565685)

[Features of Cloud Insights 12](#_Toc83565686)

[Conclusion 12](#_Toc83565687)

# **Introduction**

Data plays an important part in our day-to-day life in this digital world. Cloud Solutions provide a powerful computing platform that performs multiple tasks like online storage systems, business applications, formation of a realistic network environment etc. The user easily accesses this common platform containing millions of data. This has increased the number of data breaches that exploit cloud security. Data breaches occur when a hacker gains access to a cloud customer's resources, locates valuable data, and steals that data. It targets data centers, networks and devices. The lack of cloud security can be improved by strengthening the system's defense. This article explains some of the top cloud security data breaches in this digital world.

# **Cloud Security Data Breach**

A cyber-attack in which sensitive, confidential, or protected data has been accessed or disclosed unauthorizedly is called a data breach. It includes personal health information, personally identifiable information, trade secrets or other confidential information. In the era of cloud computing, a data breach is one of the major security concerns that recorded plenty of incidents in the history of computing. Cloud service providers are striving to ensure the protection of their customers' data. However, the incident continues as cloud computing delivers on-demand infrastructure, software, and platforms services.

## **Stages of Data Breach**

The organization is data breached when the attacker penetrates the data source and extracts its sensitive data. The data can be extracted by physically accessing a network or remotely bypassing network security. The company is often targeted by the latter method. A typical breach operation involves

1. **Research**

The hacker researches the weaknesses of the company's security and leverages the native features of the cloud to execute their attack. This is done without the notice of the cloud customer.

* **Attack**

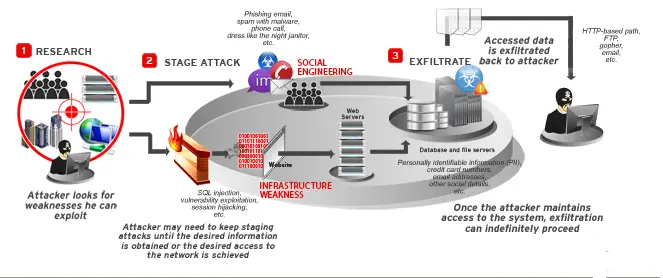
Cloud-native breaches include exploiting the errors in a cloud deployment without using the malware. Their access expanded through weakly configured or protected interfaces to locate valuable data. The data is transferred to the attacker's storage location.

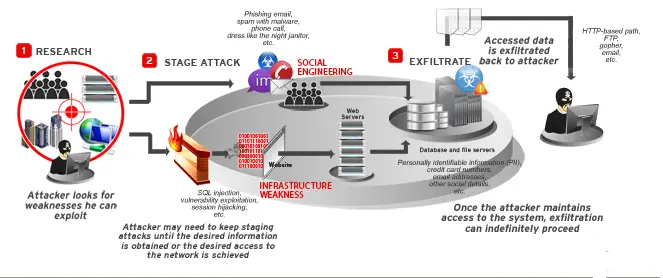
In on-premises attacks, the initial contact is made either using a network or introducing malware into the system. The company access is obtained, and the sensitive information from the company database is extracted.

* **Exfiltration**

Exfiltration is the process of extracting the company's confidential data by tunneling it into its network.

* The data is copied from the storage account to anonymous nodes on the internet.
* A storage gateway is created to access the data from a remote location.
* The data is copied from the storage accounts to a remote location outside the virtual cloud.





<https://marvel-b1-cdn.bc0a.com/f00000000017219/documents.trendmicro.com/images/tex/articles/data-breach-diagram.jpg>

**Figure 1:** Stages of Data Breach

# **Causes of Cloud Security Data Breach**

According to the cloud access risk security company Ermetic, the top three cloud security threats are

* Security misconfiguration of a production environment.
* Lack of visibility into access in a production environment.
* Improper IAM and permission configurations.

The Verizon Data Breach Investigations Report 2020, Hacking ranked the highest source of data breaches. Yahoo, Alibaba are some companies that prey on hacking.

## **Security Misconfiguration of a Production Environment**

Security misconfiguration means the execution of insufficient control assigned to the security of a cloud. The insufficient personal/expertise in cloud security access, integration of unequal security solutions that can meet their needs account for half the concerns for the data breach.

## **Lack of Visibility into Access in a Production Environment**

The rapid expansion in the network leads to a gap in cybersecurity skills. The lack of cloud security knowledge of security professionals is a big challenge for companies to adopt cloud services. This issue is addressed by providing adequate training to the security professionals to strengthen the organization's security.

## **Improper IAM and Permission Configurations.**

Public cloud infrastructure's dynamic and on-demand nature provides users and applications accumulate access permission beyond their legitimate needs. These excessive permissions granted by default often go unnoticed when a new resource or service is added to the cloud environment. This becomes a primary target for attackers for disrupting critical processes and business operations.

# **Effects of Cloud Security Data Breach**

* Loss of customer trust.
* Loss of the company's reputation.
* Loss of money, fame, sensitive data.
* Threat to the Nation'sNation's safety.

# **Major Cloud Security Breaches**

1. **Accenture**

The Cyber Risk Survey made by UpGuard [discovered](https://www.upguard.com/breaches/cloud-leak-accenture) that Accenture left a minimum of 4 AWS S3 Storage Buckets unsecured. This results in authentication credentials, secret API data, digital certificates, decryption keys, customer data and other meta info available for download. Security analysis revealed that more than 137 GB of data was available for public access. This data might be posted on the dark web by hackers.

1. **Verizon**

Nice Systems is the 3rd party vendor working for Verizon. One of the Nice Systems Engineers committed the configuration blunder on an AWS S3 bucket while creating a cloud-based file repository for storing customers' call data. Verizon uses it for backend office and call center operations. It [exposed](https://awsinsider.net/articles/2017/06/20/voter-data-leak.aspx) names, addresses, account details and PINs of millions of US-based Verizon customers, which attackers can use to gain false access to the accounts and get cloned SIMS. This incident showed the impact of the storage of sensitive information on a third-party vendor.

1. **Booz Allen Hamilton**

Booz Allen hired UpGuard for security assessment on its internal and external computer systems. It discovered that 60,000 files owned by an Intelligence and Défense Contract of Booz Allen were on public access on the AWS S3 bucket.

It includes credentials of senior Engineers, passwords of US Government systems and unencrypted passwords of government contractors holding top-secret exposed**.**

1. **Republican National Committee Data Breach**

Deep Root Analytics commissioned a third-party investigation. They confirmed that the security flaw on AWS S3 Bucket exposed the personal details of more than 198 million American voters. The security report states that the engineer working for Deep Root Analytics configured the storage platform as public instead of private. This exposed data like birth dates, phone numbers, self-reported racial background, home and mailing address and party affiliation.

1. **Election Systems and Software (ES&S)**

The database created at the US 2016 General elections by the Chicago Board of Election Commissioners was available for public access done by the engineer working for ES&S. The data of more than 1.8 million Chicago voters was available in downloadable format. The data includes names, addresses, phone numbers, driver's licenses, and Social Security Numbers.

1. **Capital One**

Capital One is the tenth largest bank in the USA. The Web application Firewall in Amazon Web Services (AWS) was misconfigured. The attacker generated a fraudulent access token from the misconfigured Web Application Firewall. The misconfigured Web Application Firewall is exploited to fetch data from AWS Storage. Datasets containing customer information and 700 folders were exfiltrated. The alerts were not triggered because the volume of transferred data was in line with the regular daily load of network traffic.

1. **Docker Hub**

The compromise of the popular Docker Hub repository hit hard the Container users, where 190,000 accounts were exposed. The unauthorized access to one of the Docker Hub databases included token and access keys. This was used in the auto-build features of GitHub and Bitbucket. It affected 5% of Docker Hub Customers.

1. **Autoclerk**

Autoclerk is a Hotel Reservation Management System. It hosted an Elastic Search database on AWS that published hundreds of thousands of bookings. The public data revealed sensitive information about the military travel of the military personnel and deployed troops. Elastic search is commonly used for big data, which can generate much information in database corruption. It is not easy to protect. Advanced license users are only offered data protection security features.

1. **Yahoo**

Yahoo secured the highest spot in terms of sheers numbers. The breach took place in 2013 but came out in 2016. It was discovered that more than a billion of its customer's account information had been accessed by a hacking group. The account information accessed were security questions and answers, plaintext passwords, payment card and bank data. Yahoo announced that the actual figure of accounts exposed was 3 billion.

1. **Alibaba**

In November 2019, the Chinese shopping website Alibaba, Taobao, noticed a breach that impacted 1.1 billion of its user data. The stolen data include user ID, phone numbers and customer comments. However, the hacker cannot access encrypted information like passwords. The Chinese Software developer secretly scraped user information over an eight-month period using crawler software he created. The data collected were used for their purpose.

1. **LinkedIn**

In 2021, LinkedIn fell victim to a data scraping breach affecting 700 million primarily public profiles. While LinkedIn argued that no private personal data was exposed, the incident is considered a violation of its terms of service rather than a data breach. The data sample was scraped and posted on the dark web in June 2021. The scraped data sample in the dark web post included email addresses, phone numbers, geo-location records, genders, and other social media details. This data can be used for social engineering attacks.

1. **Sina Weibo**

Sina Weibo is one of the largest social media platforms in China. It has over 600 million users who are impacted as attackers obtained part of its database. The 538 million user's details, including real names, site usernames, gender, location, and phone numbers, were sold on the dark web for $250. Sina Weibo argued that an attacker had gathered publicly posted information that helped users locate friends' accounts by using phone numbers, and no passwords were exposed. They admitted that the exposed data would access passwords if passwords were reused on other accounts. The company strengthens its security strategy.

1. **Facebook**

In April 2019, two datasets from Facebook apps that include 530 million Facebook users' data were exposed to the public internet. The data included phone numbers, account names and Facebook IDs. It was reported on April 2021, while Facebook says it immediately found and fixed the issue. The data was posted to the public. It created a real criminal intent for the data. This issue hit the founder Mark Zuckerberg to answer federal regulators to settle a privacy case to pay $5 billion penalties paid by the company to Federal Trade Commission.

1. **Mariott International**

Hotel Mariott International suffered an attack that exposed half a million Starwood guests' sensitive details in September 2018. The alert from the internal security tool regarding the attempt to access the Starwood guest reservation database exposed the breach. The data copied include guest names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates and communication preferences. Some person's payment card numbers and expiration dates were also included. The investigation assessed by the security experts announced to phase out Starwood systems and enhance security to its network. The UK data governing body, the Information Commissioner'sCommissioner's Office, fined 18.4 million Euros for failing to secure customers' data.

1. **Adult Friend Finder**

Adult Friend Finder is an adult-oriented Social networking service. It encountered the expose of 412 million user accounts from multiple sites in October 2016. It made the biggest hack of that year. The six databases stolen by cyber thieves included names, email addresses and passwords. The majority of passwords are hashed through weak algorithm SHA-1, with an estimated 99% of them cracked by the time.

1. **My Fitness Pal**

This diet and exercise application was exposed in February 2018. The 150 million uni1ue email addresses, IP addresses and login credentials such as user names and passwords stored as SHA-1 and bcrypt hashes appeared for sale on the dark web. The breach made the company to upgrade its security.

1. **Adobe**

Adobe reported that hacking had exposed 3 million encrypted customer credit card records and login data for an undetermined number of user accounts in October 2013. The weeks of research exposed that over 150 million active user names, passwords, debit and credit card information were stolen. This event called for an Agreement in August 2015 to pay $1.1 million in legal fees and $1 million to users to settle claims of violating the Customer Records Act and unfair business practices.

1. **Dubsmash**

The New York-based video messaging service Dubsmash in December 2018 witnessed 162 million user details put up for sale on the Dream Market dark web. The details include email addresses, usernames, PBKDF2 passwords hashes and other personal data such as date of birth. The breach was acknowledged, and a change of passwords was advised to the Dubsmash users.

1. **MySpace**

Social media site MySpace hit the headlines as its 360 million user accounts were put up for sale in the dark web market. The company investigation showed that lost data were created before June 11, 2013, on the old Myspace platform. The lost data included email addresses, passwords, and usernames. The company initiated the affected users to authenticate their accounts and reset their passwords.

1. **NetEase**

In October 2015, the mailbox services provider NetEase suffered a breach through the likes of 163.com and 126.com, which affected 235 million accounts. Dark web marketplace vendor Double Flag sold these accounts' email addresses and plaintext passwords. But the company maintained no data about the breach.

1. **Court Ventures (Experian)**

In October 2013, Experian Subsidiary Court Venture was tricked by a Vietnamese man to expose 200 million personal records. He acted as a private investigator from Singapore to access the database. The database, including the personal information of US residents, was sold to cyber criminals across the world.

1. **State Farm**

American Insurance and Financial Service Company, State Farm encountered a credential stuffing attack. In an unrelated data breach, the attacker attempted to log into the cloud service using a previously stolen password. State Farm assured its Customers that unauthorized access to their accounts would not result in fraud or disclosing personally identifiable information, but this claim is not externally verified.

# **Cloud Security Best Practises**

The Global intelligence Firm IDC reports that nearly 80% of the Companies surveyed had experienced at least one cloud data breach in the past 18 months, and nearly half reported 10 or more. Since Cloud security plays a major part in an organization. Few Best practices include

* Preventing Privileged Account Compromise with IAM
* Prevent Data loss by Setting Up Backup and Recovery Solutions
* Audit and Optimize Configurations

Top Cloud Access security priorities are maintaining the confidentiality of sensitive data, regulatory compliance and providing the right level of access. The cloud security priorities include compliance monitoring, authorization and permission management and security configuration management..

## **Identity and Access Management Solution**

Identity and Access Management solution is used for privileged user accounts to prevent abuse. Alerts can be set by monitoring behavior, and pre-configured responses can trigger unusual activity. The basic features of an IAM System are to prevent the takeover of key user accounts include Two-Factor Authentication (2FA) and Security Assertion Mark-up Language (SAML) called Single Sign-On (SSO).

## **Backup and Recovery Solutions**

Data loss can be avoided by creating redundant copies of data on different storage systems. The storage systems include data stored in different cloud accounts or clouds to prevent an attacker from deleting them. Automatic backups, automatic disaster recovery and user management are reliable methods of recovering lost data.

## **Audit and Optimization of Configurations**

The application and infrastructure of the cloud should be monitored for configuration errors. The configuration errors can be

* a lack of validation in maintaining services and permissions.
* More permissive access to Hosts, Containers and Virtual Machines.
* Unsecure passwords, API keys, admin credentials and encryption keys
* Misconfiguration of the control settings.

The updates and changes in the application workflow should be verified for proper services and permissions. This will help in a secure cloud work platform. Third-party services like Cloud Security Posture Management can help analyze resources and configuration.

# **Cloud Security Breach Prevention Technology**

## **NetApp Cloud Insights**

NetApp Cloud Insights is an infrastructure monitoring tool. It gives complete visibility of the cloud infrastructure and applications. It identifies the risk from ransomware attacks by analyzing the data access pattern. The data in the entire technology can be monitored, troubleshoot and optimized in the cloud.

## **Features of Cloud Insights**

* Advanced machine learning and anomaly detection protect organizational data from being misused by malware.
* It quickly finds problems and fixes the issue.
* Resources can be managed more effectively.
* It protects intellectual property from the hacker
* The auditing of access patterns to critical data ensures corporate compliance.

# **Conclusion**

In this data-driven world, on-demand services about infrastructure, software and platforms are vulnerable to different kinds of data breaches. It is impossible to stop data breaches, but security mechanisms must be improved to ensure data owners outsource their data to the cloud. Cloud Service providers are striving hard to ensure the data protection of customers. It can be done by creating a disaster recovery plan, building highly secure infrastructure and investing in prevention and detection technologies.