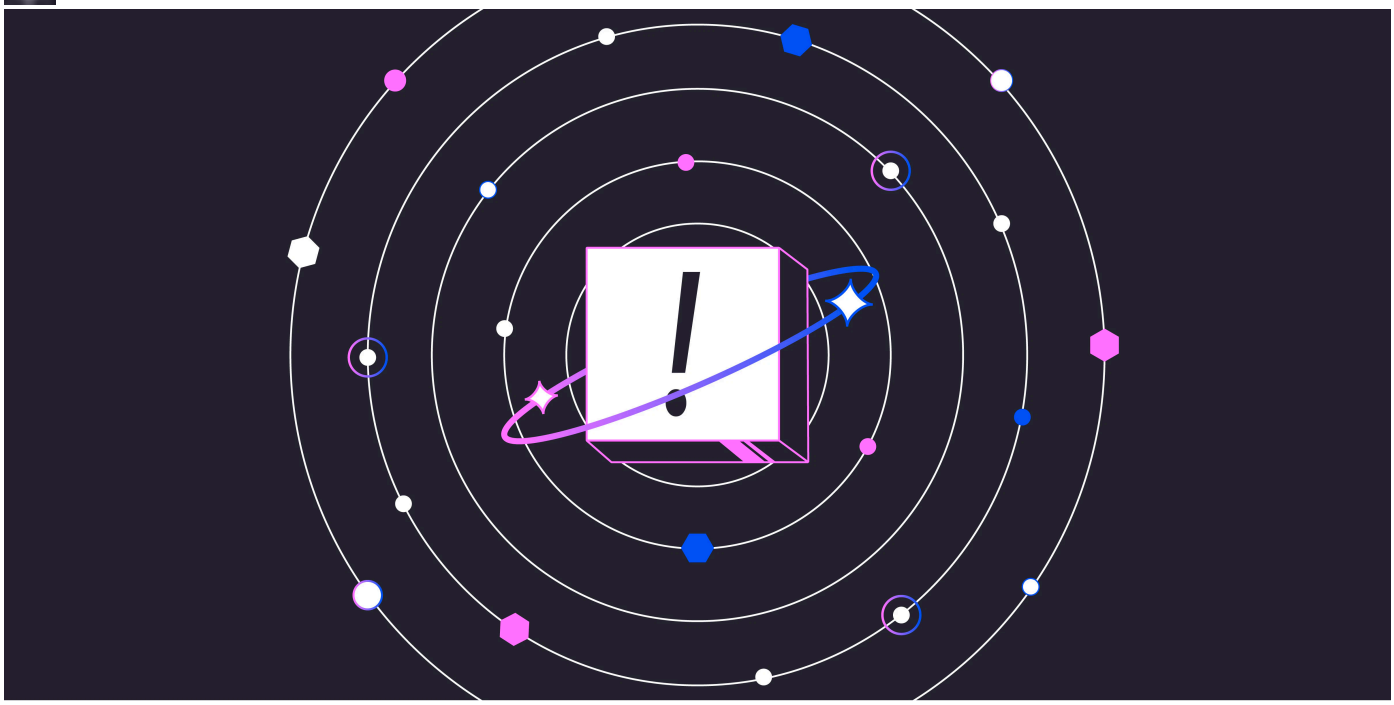
8 All-Too-Common Cloud Vulnerabilities

We outline the most common cloud vulnerabilities with real-life examples of attacks that exploited these vulnerabilities, and simple steps you can take to mitigate them.

Wiz Experts Team September 8, 2023 8 minutes read



What are cloud vulnerabilities?

Cloud vulnerabilities are weaknesses or gaps in a cloud computing environment that attackers can exploit to gain unauthorized access, steal data, or disrupt services.

According to Forrester, the top 35 data breaches in 2022 accounted for 1.2 billion compromised customer records. The consequences of such data breaches include reputational damage, reduced profit margins, organizational and operational disruption, and legal fines. Forrester revealed that the organizations targeted in the top 35 data breaches were ordered to pay a collective $2.7 billion in fines.

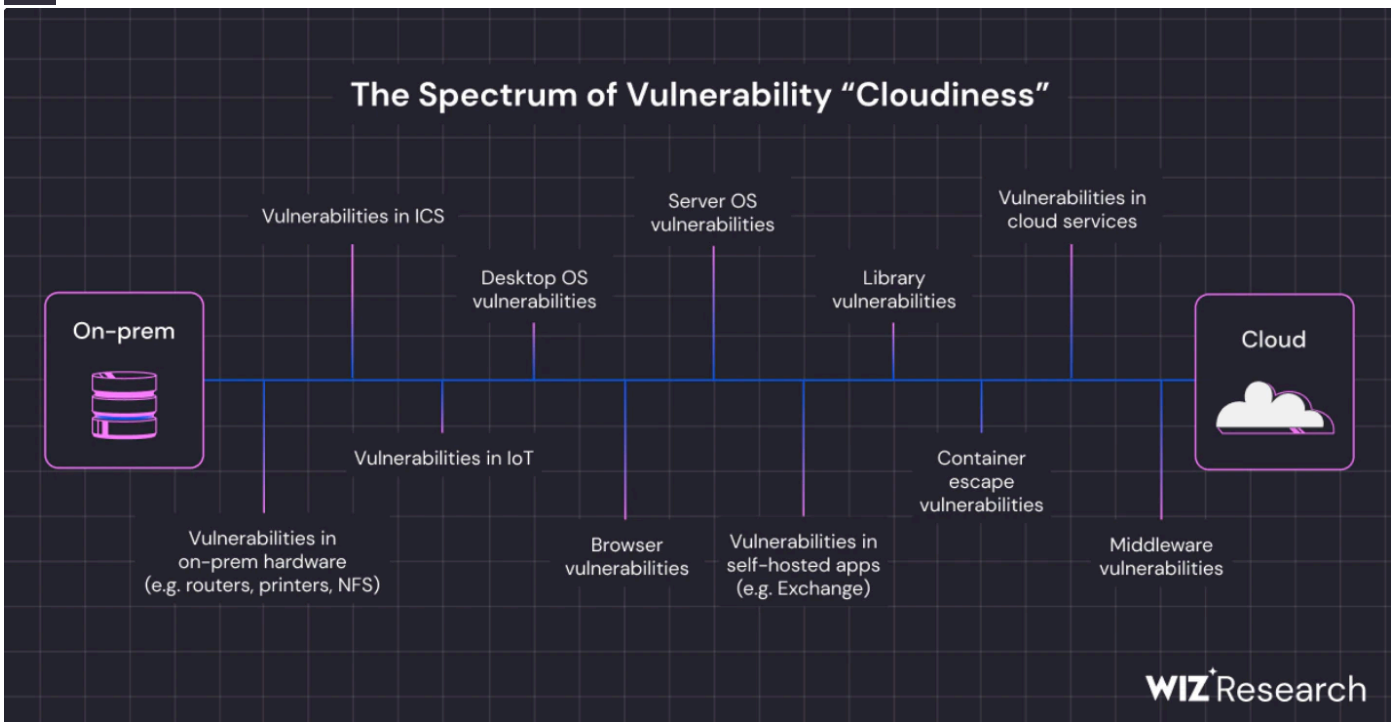
Time and time again, **most cloud breaches are caused by several of the same types of vulnerabilities**. Attackers continue to seek out these vulnerabilities because they are easier to exploit. Even though they are common, organizations still do not take the proper steps to protect against these vulnerabilities, either because they are not aware of the risk or simply do not know how to mitigate them. This article hopes to address both of these issues.

The 8 cloud security vulnerabilities you're sure to encounter

The most common cloud security vulnerabilities include:

1. Misconfigurations
2. Lack of visibility
3. Poor access management
4. Insider threats
5. Unsecured APIs
6. Zero-days
7. Shadow IT
8. Lack of encryption

We'll explain each of these vulnerabilities below with real-life examples of attacks that exploited these vulnerabilities, and simple steps you can take to mitigate them.



Source: The Good, The Bad, and The Vulnerable Report

1. Misconfigurations

Misconfigurations are errors in the security settings of cloud applications and systems, including virtual machines, containers, serverless environments, and infrastructure as code (IaC). Misconfigurations are often the byproduct of administrative oversights, high-velocity development environments, a lack of awareness, and security misconceptions.

Ultimately, misconfigurations are among the main attack vectors for data breaches. Common cloud misconfigurations include open ports for outbound server traffic, overprivileged identities, a lack of monitoring, unsecured storage (like open S3 buckets), the use of default passwords and credentials, and third-party misconfigurations.

Real-life example:

In 2022, McGraw Hill was informed that 22 TB of data, including student grades and personal information, had been exposed since 2015 because of a misconfigured AWS S3 bucket. This misconfiguration meant that around 117 million files could have been accessed and leveraged by any threat actor with a simple web browser.

Basic mitigation steps:

- Use a cloud security posture management (CSPM) tool to regularly audit and remediate cloud configurations
- Implement least privilege access to cloud resources
- Implement Infrastructure as Code (IaC) to maintain consistent and correct configurations

2. Lack of visibility

Enterprises mix and match cloud technologies from various providers ad hoc, creating complex, interconnected, and constantly evolving IT environments. Cloud security vulnerabilities of different proportions may be scattered across this dynamic infrastructure. Unfortunately, a lack of visibility can be detrimental to identifying, contextualizing, prioritizing, and mitigating these vulnerabilities. It's impossible to assess the risk of cloud computing vulnerabilities without centralized, context-based visibility of the entire cloud ecosystem.

Real-life example:

A lack of visibility also means that companies can be vulnerable for years without knowing it. Toyota Japan unknowingly exposed the personal and vehicle data of 2.15 million customers for almost 10 years. With better visibility, Toyota could have identified and addressed the cloud misconfiguration that caused the data exposure.

Basic mitigation steps:

- Implement centralized logging and monitoring solutions for all cloud resources
- Employ a CNAPP solution to gain visibility into all cloud assets and activity
- Set up alerts for unusual or unauthorized activities
- Regularly review and prune unnecessary resources

3. Poor access management

Digital identities vastly outnumber human identities in cloud environments, which makes them alluring targets for threat actors. Identity access management (IAM) and other identity-related cloud vulnerabilities can be powerful initial attack vectors for cybercriminals to infiltrate an IT environment, exfiltrate data, and cause lateral damage.

IAM is notoriously complex, and is noted in Verizon's 2021 Data Breach Investigations Report as being responsible for 61% of analyzed breaches

Subpar access management vulnerabilities include a lack of MFA; poor password and credential hygiene; misconfigured policies; mushrooming of administrative entitlements; and a lack of standardized, automated identity lifecycles and centralized access management capabilities.

Real-life example:

Third-party access management is particularly crucial because cybercriminals often use overprivileged third parties to infiltrate enterprise cloud environments. The Broward Health data breach was enabled by an overprivileged third-party medical provider and resulted in a data compromise of 1.3 million patients' records. Sensitive data included names, addresses, social security numbers, and medical information.

Broward Health has proof that cybercriminals stole exposed data, but there's no word yet on whether that data was abused. Stolen data is known to appear in illicit marketplaces years after data breaches, so it's impossible to gauge the full extent of damage caused by poor access management.

Basic mitigation steps:

- Implement least privilege access to cloud resources
- Use role-based access control (RBAC) to grant users only the permissions they need
- Adopt MFA and Single Sign-On (SSO) solutions
- Conduct training sessions for proper access management practices
- Use a CASB to monitor and control access to cloud resources

4. Insider threats

Insider threats are vulnerabilities attached to individuals or entities that already have some degree of access to and knowledge of an enterprise's IT environment. Insiders could include current and former employees, third-party vendors, and partners.

Insider threats could be due to accidental errors, negligence, or malicious intent. Insider attacks via phishing and other social engineering techniques are common because humans remain the weakest link in a company's cybersecurity posture.

Real-life example:

Disgruntled cloud professionals and experts are major security threats to enterprises because of their in-depth knowledge of cloud computing vulnerabilities and how to exploit them. The Capital One breach, which compromised the data of 100 million Americans and 6 million Canadians, was engineered by a former employee of Amazon Web Services. This threat actor had the know-how and technical expertise to hack Capital One's Amazon cloud infrastructure. The result was a cyberattack whose estimated remediation cost hovers between $100 and $150 million.

Basic mitigation steps:

- Monitor employee activity for suspicious behavior
- Implement strict access controls, even for trusted insiders
- Conduct background checks on employees with critical access
- Offer training and create a company culture that emphasizes cybersecurity

5. Unsecured APIs

Cloud APIs are the connective tissue that facilitates communication and data exchange between cloud software and applications, and API vulnerabilities are a prominent attack vector for threat actors. Examples of vulnerabilities associated with unsecured APIs include suboptimal access controls, weak authentication protocols, wrong rate limits, and accidental data exposure.

Real-life example:

The attack vector for the Optus data breach in 2022 was an unsecured and publicly available API that didn't require any authentication protocols to access. The breach compromised the sensitive records of around 10 million customers.

Optus isn't alone. According to Google Cloud, 50% of surveyed organizations faced an API-related attack between 2021 and 2022. Forty percent of IT executives cited API misconfigurations as the cause of these attacks, while 35% claimed that outdated APIs were the primary vector.

Basic mitigation steps:

- Implement strong authentication and authorization mechanisms for cloud APIs
- Use rate limiting and other controls to prevent abuse of APIs
- Regularly scan APIs for vulnerabilities

6. Zero-days

Zero-day is an umbrella term for cloud security vulnerabilities that cybercriminals may identify before vendors do. Zero-day exploits are when threat actors take advantage of these unidentified and unknown security vulnerabilities.

Real-life example:

Microsoft and Google are two of the most prominent victims of zero-day attacks. Recent glitches in Microsoft Windows and Office products could have allowed threat actors to conduct remote code execution (RCE) attacks, exfiltrate data, and lock access for legitimate users. Similarly, Google had to address a series of zero-day Chrome vulnerabilities in 2023, one of which had a high severity score. Though the exact details of Google's latest vulnerability are unreleased, patterns suggest that more vulnerabilities and exploits may follow.

Basic mitigation steps:

- Keep all software and systems up-to-date
- Implement intrusion detection and prevention systems.
- Use virtual patching to mitigate risks until vendors release patches

7. Shadow IT

Shadow IT is the use of your cloud assets without the approval or support of your IT department. There are several risks associated with this, including the financial impact of staff creating cloud workloads for personal use, data loss via unauthorized file-sharing services, and the use of unauthorized messaging services for communications. Some users may be motivated by frustration at in-house technology and look to familiar tools to improve productivity, while others are looking to leverage loopholes to spend their time on non-work activities, or even steal company data.

Real-life example:

One well-known example that could be partially attributed to Shadow IT is the massive data breach at Target in 2013. While the exact details involve multiple layers of compromise, one significant factor that made this breach possible was an HVAC (heating, ventilation, and air conditioning) vendor. The vendor had access to Target's network for legitimate purposes, but their system was compromised, giving the attackers a foothold into Target's network. From there, they were able to move laterally, exploit further weaknesses, and eventually access the point-of-sale systems to harvest card details. The compromised vendor access point can be seen as an example of Shadow IT because the risks associated with such third-party connections were not adequately assessed or monitored.

Basic mitigation steps:

- **Eliminate Shadow Code:** Shadow code refers to unauthorized code that's used by developers.
- **Design business-specific security policies:** Security policies should be attuned to an organization's unique requirements and objectives.
- **Leverage access controls:** Establishing, embedding, and implementing access controls across cloud environments can help police what IT assets are allowable, where they can be integrated, and who can commission them.

8. Lack of encryption

Lack of encryption presents a significant vulnerability in cloud storage, allowing unauthorized individuals to access sensitive data if they manage to infiltrate the cloud environment. When data is encrypted, it is transformed into a format that cannot be read without the encryption key. Thus, even if unauthorized individuals obtain the encrypted data, they cannot decipher it.

Real-life example:

One of the most significant data breaches in history was suffered by Equifax, one of the three major consumer credit reporting agencies. The cyberattack compromised the personal data of nearly 147 million people. While the root cause of the breach was an unpatched vulnerability in the Apache Struts web framework, subsequent investigations found that Equifax had stored sensitive data without encryption, which significantly exacerbated the impact of the breach.

Basic mitigation steps:

We need to concern ourselves with encrypting data in transit, as well as at rest, to avoid unknowingly giving third-party access to cloud data.

Encryption in transit for cloud services ensures a malicious user is prevented from accessing data as it moves between systems. This is covered in the cloud by use of secure protocols, most notably HTTPS. You should configure your systems and data stores to only be accessible via secure protocols and use firewalls to block insecure access methods.

Encryption at rest ensures that data stored on a disk or other storage medium is kept safe from anyone who should not be accessing it. Full disk encryption (FDE), utilizing AES256 for maximum security, is recommended for virtual machine disks. Transparent Data Encryption (TDE) is available to keep databases secure while in use.

A better approach to combating cloud vulnerabilities

The volume of cloud security vulnerabilities in dynamic IT environments can potentially overwhelm businesses. And while traditional vulnerability management solutions can identify and remediate many vulnerabilities, they lack context and often prioritize low-risk vulnerabilities. Wiz tackles these challenges by focusing on the most crucial and high-risk cloud vulnerabilities, which are excavated via agentless deep cloud scanning and analysis.

> As we scale and gain more customers, we are confident that we can tell them we are aware of all known vulnerabilities, and that new vulnerabilities will be quickly visible to us too.
>
> Kashfun Nazir, Information Security Lead & Data Protection Officer, Atlan

Wiz's cloud vulnerability risk assessment considers workload, cloud, and business context. It doesn't just uncover vulnerabilities; it illustrates how and why they impact your organization, helping you keep your IT environments safe from cloud computing vulnerabilities without alert fatigue. Get a demo now to learn how Wiz's unique approach to mitigating cloud security vulnerabilities can fortify your cloud environments.