WIZ

2023 Cloud Security Threat Report

With the migration of organizations to the cloud, cybercriminals follow suit. To enhance the protection of your cloud environment in 2023, consider the most critical cloud security threats and the methods to defend against them

Table of Contents:

The current cloud security landscape

Cloud security incidents are primarily caused by misconfigurations, making them a top concern for organizations. In addition, by the end of this year, Gartner predicts that 75% of security breaches will stem from poor management of identities, access, and privileges. This is also the top risk for applications, according to OWASP. Thus, organizations must prioritize properly managing these elements to prevent security failures. Here are a few other predictions from Gartner for the next following years:

- By 2024, most businesses will still need help accurately assessing cloud security threats.
- By 2025, 90% of organizations that fail to manage public cloud usage will inadvertently disclose confidential information.
- By 2025, 99% of cloud security failures will be caused by cloud customer negligence.

Gartner, 2019

Responsibility

Previously, security was the sole responsibility of security teams, not end-users such as developers. With the emergence of new cloud vulnerabilities, it's clear that the old model is insufficient. In the cloud, security is a shared responsibility, requiring a careful balance of different entities' responsibilities. Some vulnerabilities require a unique solution with varying obligations from both cloud service providers and their customers. Other vulnerabilities arise from developers who ignore security teams and policies when using the cloud. However, there is no uniform approach to addressing cloud security issues.

Security Awareness

The rapid adoption of cloud technology leaves little room for educating users on best practices and potential risks of improper use - no one can be an expert at everything. For instance, a developer may unintentionally introduce a secret-laden asset into the CI/CD pipeline, making it vulnerable to external exposure and abuse by hackers. In addition, the limited expertise of users amplifies security risks in the cloud's constantly changing and complex environment. As more organizations shift to the cloud, so do attackers. They adapt faster than users, taking advantage of the lack of security awareness and knowledge about new cloud features to cause harm.

Visibility

Many organizations are unaware of the extent of their cloud presence - the number and types of assets they have running in the cloud, who is using them, how well they've been configured or if they are vulnerable. This lack of visibility is a significant issue and source of frustration for organizations. This problem only grows as cloud technology becomes more widespread.

Cloud security threats

This report encompasses our research and practical experience from the past year in ensuring the security of enterprise cloud environments. The report focuses on specific, significant, and high-impact risks that should be recognized and incorporated into your 2023 cloud security plan.

Data exposure

Data exposure remains a widespread problem. Our research shows that over 55% of companies have at least one database currently accessible to the public on the internet. Many of these databases have weak passwords or do not require authentication at all, making them vulnerable to attackers who continuously scan the internet for such exposed databases. These days, an unsecured Elasticsearch server will be breached within eight hours on average, making it crucial to address these exposures immediately.

Speaking of data breaches, the scale of damages caused by exposed databases is astonishing. Unintentionally exposed databases are one of the leading causes of data breaches, and security teams are struggling to keep up with the growing challenge, especially as cloud environments become increasingly complex. The following is just a partial list of cybersecurity breaches involving data exposure between 2021-2022:

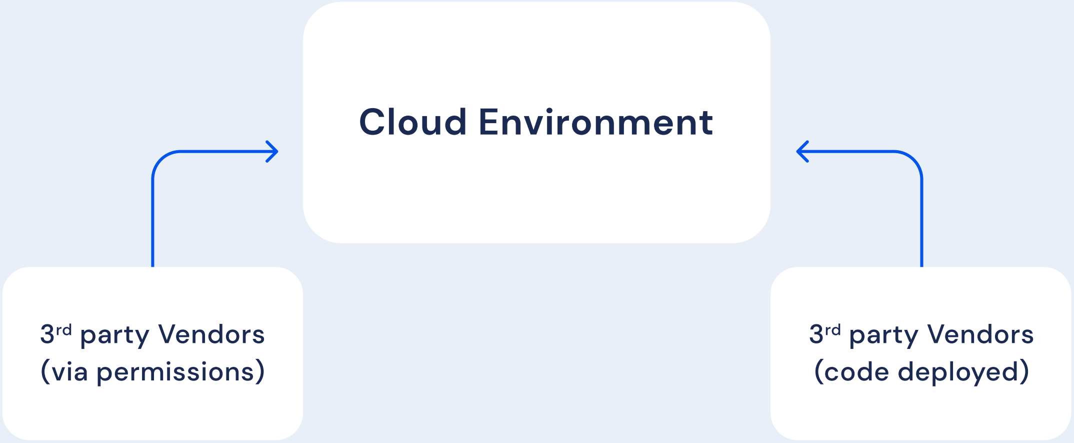
- VIP Games (2021)
- Reverb (2021)
- The Telegraph (2021)
- Acer (2021)
- Alteryx (2021)
- ViacomCBS (2021)
- Zoom (2021)

- Verkada (2022)
- GitLab (2022)
- Ascena Retail Group (2022)
- Evite (2022)

Software supply chain risks

You are probably highly familiar with the cloud shared responsibility model. But how much trust do you put in cloud providers to uphold their responsibility in the era of zero trust? Cloud environments face a unique security risk due to cloud service providers' use of pre-installed software, also called middleware. In addition, cloud providers often do not explicitly disclose the third-party software they are running in your cloud environment, leaving you at risk from software you may not even know that you have installed or trust to run in your production environments. Understanding and addressing the security implications of these unknown software components is crucial to safeguard your cloud environment.

As depicted in the illustration below, there are two primary categories of supply chain risks in cloud environments: identity/permission-based and software/code-based.



Cloud Environment

3rd party Vendors (via permissions)

3rd party Vendors (code deployed)

- New type of risk in the cloud via 3rd party permissions
- Widely used in almost all cloud environments
- Enabled by lack of awareness and control by security teams

- Software risk in the cloud is much more complex
- Varied compute types: VMs, containers, serverless, etc.
- Enabled by lack of unified cloud asset inventory

Let's briefly examine supply chain attacks at a high level. These occur when attackers manage to infiltrate a third-party vendor. The CNCF TAG Security team keeps a catalog of the latest software supply chain incidents. By compromising the third party, attackers can insert malicious code into their software, thereby abusing the trust relationship between vendor and customer. As a result, attackers can gain initial access to thousands of otherwise secure organizations using that vendor's products, all enabled through a single breach.

Identity-based risk

This risk stems from granting third-party vendors access within your cloud environment (as opposed to installing third-party software). Cloud identity permissions can be complicated - without adequate security awareness, seemingly harmless permissions could result in unintended exposure. For instance, if a third-party service with extensive access privileges to your account experiences a breach, your data and infrastructure could also be at risk.

In 2021, Microsoft revealed that the Nobelium threat actor group (also responsible for the SolarWinds hack in 2020) targeted multiple cloud service providers (CSPs) and managed service providers (MSPs) to which other organizations had granted administrative or privileged access. The goal was to exploit these trusted relationships to move laterally within cloud environments, from the service providers to their customers. This campaign highlights that threat actors are acutely aware of the vulnerable identity supply chain and aim to gain access to downstream customers through their vendors, to widen their reach, carry out further attacks or access specific systems. Such operations are highly effective for attackers. They can gain privileged access to thousands of targets by carefully selecting their CSP/MSP target.

Our team conducted extensive research to assess the potential extent of the issue, and the results showed the extent of this attack surface:

- **82%** of companies grant third-party vendors highly privileged roles.
- **76%** of companies have third-party roles that permit complete account takeover.
- More than **90%** of cloud security teams were unaware they had granted high privileges to third-party vendors

Vendors are frequently granted excessive privileges. The most widespread instance is the AWS "ReadOnlyAccess" policy, which is required by many third-party vendors (our research shows that 25% of vendors request it by default). Both vendors and customers often consider it a harmless policy, but in fact it grants full read access to many databases, including DynamoDB, S3 buckets, SQS queues, and others.

Furthermore, security teams rarely keep track of these permissions once granted, to ensure they are used as intended.

Software-based risk

Supply chain attacks via software are emerging as a critical threat, gaining notoriety with the SolarWinds breach in late 2020 and the Log4Shell vulnerability in the end of 2021, which impacted many organizations both directly and indirectly.

Challenges

The cloud has an additional risk factor that originates from cloud providers themselves, who are also using pre-installed software on their workloads. Cloud providers often don't share what 3rd party software they are running for you, in your cloud environment. How can you protect your environment from software you are not even aware of?

Let's look at selected examples of this use case:

1. **OMIGOD: Azure customers are unknowingly exposed due a "secretly" installed agent.**
   The Open Management Infrastructure (OMI) agent is an open source project. This agent is embedded in many popular Microsoft Azure services without the customer's knowledge, for example, when you set up a Linux virtual machine in you cloud.

   The Wiz Research Team discovered a chain of 4 critical/high vulnerabilities in OMI, dubbed as OMIGOD. Unless a patch is applied, attackers can easily exploit these vulnerabilities to escalate to root privileges and remotely execute malicious code (for instance, encrypting files for ransom). However, since most customers were not aware they were running an OMI agent, they did not apply the patch. In a sample of Azure tenants we analyzed, over 65% were unknowingly at risk. The magnitude of the risk, along with the lack of awareness to this silently installed agent, led Microsoft to develop an auto-update mechanism that patched the vulnerability on Azure services' machines.
2. **Log4Shell: Customers struggle to identify a highly popular compromised logging app in their cloud environment.**
   Log4Shell (CVE-2021-44228), published in December 2021, is a critical unauthenticated Remote Code Execution (RCE) vulnerability in a highly popular Java library, Log4j. A day after the vulnerability was published it had already been exploited in the wild. According to Wiz and EY research more than 93% of enterprise cloud environments were vulnerable to the Log4j vulnerabilities. This vulnerability demonstrates how one critical vulnerability in a single library immediately and directly puts thousands of products and dozens of cloud services at risk.

   The first step for security teams is to identify all applications using Log4j running across their environments. In order to get full coverage, it is important to scan all workloads, including VMs running legacy apps, containers running on Kubernetes or other orchestration platforms, and even serverless code running on cloud functions. Since Log4j can be deployed as a package or embedded into the app itself, the scanner must support both.

Cloud-native threat actors

This report focuses on the high-impact security risks in enterprise cloud environments, as determined through our research and experience over the past year. We've selected the most significant and innovative risks to ensure that you are well informed and can effectively incorporate them into your 2023 cloud security plan.

As more organizations move to the cloud, attackers shift their focus to target cloud accounts and workloads. They take advantage of the fact that many cloud environments lack proper security due to knowledge gaps. Our research shows that 70% of cloud resources are not protected by endpoint protection products, and the average enterprise environment has ~40 malware instances. There are two malicious actors that highlighted the growing trend of utilizing cloud-based technology for malicious purposes:

- TeamTNT attacked exposed Docker APIs to run their harmful code with elevated privileges on targeted systems. They have a track record of targeting cloud instances and containers using Docker, Kubernetes, or AWS workloads that have been improperly configured and are publicly accessible on the Internet. They leverage their access to install cryptocurrency miners on compromised workloads. Also, according to vx-underground, ransomware groups have since adopted some of TeamTNT's tools for their own uses.
- The Nobelium APT group continued its focus on cloud-based targets. As reported by Microsoft, Nobelium targeted cloud service providers (CSPs) and managed service providers (MSPs) that held privileged access, using their environments as a stepping stone to reach downstream customers. The group displayed a deep understanding of Azure services and environments, employing tactics like ROADTools and AADInternals to enumerate Azure AD users, creating service principal credentials for persistence, and utilizing Azure RunCommand and Azure admin-on-behalf-of (AOBO) to access on-premises environments from the cloud. This demonstration of Nobelium's cloud-native capabilities highlights the evolving nature of threat actors and the importance of staying up-to-date with the latest tactics and techniques to defend against them.

API security

Application Programming Interfaces (APIs) are crucial in modern software development and cloud environments. They allow different software applications to communicate and exchange data, making it easier for developers to build and integrate new features. However, as the use of APIs has skyrocketed with cloud adoption, so does the risk of security breaches, which can compromise sensitive information and harm businesses. Therefore, it is vital to understand the basics of API security and the measures organizations can take to protect their data and applications and minimize those risks.

As technology and the threat landscape evolve, new API security vulnerabilities are being discovered. According to OWASP and its API Security Top 10 2019 list, APIs are exposed to a wide range of security threats. Some examples include:

- Broken Object Level Authorization (BOLA) - an API does not properly restrict access to sensitive objects, allowing unauthorized users to access or modify data.
- Broken Function Level Authorization (BFLA) -an API does not properly restrict access to sensitive functions, allowing unauthorized users to access or modify data.
- Server-Side Request Forgery (SSRF) - an API accepts unsanitized user input, allowing attackers to request internal systems or resources not intended for public access.
- Insufficient Logging and Monitoring - an API does not have adequate logging and monitoring mechanisms, making it difficult to detect and respond to security incidents.
- Insufficient Security Configuration - an API is not configured with appropriate security measures, such as encryption, strong authentication, and access controls.
- Misconfigured Cross-Origin Resource Sharing (CORS) - an API allows cross-origin requests from untrusted sources, making it easier for attackers to execute cross-site scripting (XSS) attacks.

APIs in the cloud

APIs have become integral to modern technology and are increasingly becoming a common target for attackers to facilitate data breaches. The security of APIs in cloud environments is becoming increasingly important as more organizations move their applications and data to these environments. Unfortunately, misconfigured cloud APIs are also exposed to the various security risks we described above. Here are examples of data breaches in 2022 that involved API security failures:

- January 2022: An insurance company reported a breach of 1.8 million user accounts due to a vulnerability in a web service application that inadvertently allowed access to protected parts of the application. The root cause in this case was a BFLA. In the same month, a digital scheduling platform had a security breach that exposed Personally Identifiable Information (PII) for 3.7 million user accounts.

The vulnerability exploited in this case was a BOLA vulnerability, and specifically a misconfuguration of an AWS S3 bucket.

- February 2022: A large online marketing platform experienced a breach that exposed PII for 7 million customer accounts. The culprit was a misconfigured, unencrypted S3 bucket containing PII.
- July 2022: A major social media platform reported an API breach from late 2021 into 2022. It exposed the PII of at least 5.4 million user accounts. The vulnerable API allowed users to retrieve data related to other users, mistakenly revealing PII. Some of this data was put on sale, and some of it was allegedly published for free.
- September 2022: An international telco company reported a breach in 10 million accounts, with an ensuing $1 million extortion demand from the attacker. The vulnerability was a BFLA in the form of an unsecured public API.

It's important to note that while API vulnerabilities were a significant factor of these breaches, the issue is not with the API itself but with how it is implemented and secured. These examples demonstrate the importance of implementing secure API practices and ensuring that sensitive data is appropriately secured. Companies can take measures to prevent API breaches by following best practices for API security, such as:

- Encrypting data in transit and at rest
- Implementing robust authentication and access controls
- Enforcing user input validation
- Using API keys and tokens
- And monitoring API usage for suspicious activity

Wiz Research 2022 recap

Here are the latest cloud vulnerabilities found and reported by our Wiz research team:

- **AttachMe** - critical OCI vulnerability allows unauthorized access to cloud storage volumes
- **ExtraReplica** - a cross-account database vulnerability in Azure PostgreSQL
- **Hell's Keychain** - Supply-chain vulnerability in IBM Cloud Databases for PostgreSQL

AttachMe

A vulnerability in Oracle Cloud infrastructure has been discovered that allows unauthorized access to data stored in the cloud. This vulnerability affects the "AttachMe" feature in the Oracle Cloud and allows malicious actors to access cloud-based data volumes that are not intended for them. Which could lead to data breaches and other security incidents. Oracle has issued a patch for this vulnerability and recommends that users update their systems as soon as possible to prevent unauthorized access.

ExtraReplica

A vulnerability has been discovered in the Azure PostgreSQL service offered by Microsoft. This vulnerability, known as the "ExtraReplica" cross-account database vulnerability, allows unauthorized access to database systems stored in the Azure cloud. It can result in sensitive data being stolen or altered without the knowledge of the database owner. Microsoft has issued a patch to fix this vulnerability and advises users to update their systems as soon as possible to prevent unauthorized access to their data.

Hell's Keychain

A vulnerability called "Hell's Keychain" has been discovered in IBM Cloud Database for PostgreSQL. This vulnerability allows attackers to steal sensitive data by exploiting the supply chain of third-party software used in the IBM Cloud. It can result in unauthorized access to sensitive data stored in cloud-based databases. IBM has issued a patch to fix the vulnerability and advises users to update their systems to prevent such attacks. The company also recommends following best practices for secure supply chain management to minimize the risk of similar attacks in the future.

Your cloud security checklist for 2023

To significantly enhance your cloud security in 2023, consider these recommendations:

- Boost your insight into your entire cloud infrastructure, including virtual machines, containers, serverless computing, and platform-as-a-service offerings. Keeping an up-to-date inventory of your cloud assets can help you quickly identify and address vulnerabilities.
- Ensure logging and monitoring are in place for your cloud environment so you can detect the presence of malware and other suspicious activity.
- Minimize your cloud environment's exposure to the internet by identifying unnecessarily exposed resources and closing any unintentional lateral movements paths.
- Limit third-party access to your cloud environment by thoroughly reviewing any vendors that require access to your data and ensuring they only have the minimum access necessary.
- Adopt a "shift-left" security strategy by integrating your security policies into your continuous integration and deployment pipelines, allowing you to resolve security issues before they make it into production.

About Wiz Research

We are a team of seasoned cybersecurity professionals with over a decade of experience. We work tirelessly to identify potential security risks within cloud service providers (CSPs). We assist our clients in identifying and mitigating these issues and occasionally uncover vulnerabilities within these platforms. In 2022, we contributed to uncovering dozens of new cloud risks and resolving security vulnerabilities across multiple AWS, Azure, and Google Cloud services. Our Wiz Threat Center also closely monitors emerging cloud security threats and provides ongoing monitoring.

For any inquiries regarding our research, kindly contact us at research@wiz.io.