Guide

# 6 Common Cloud Vulnerabilities That Lead To A Data Breach

Migrating to the cloud is all about agility, flexibility and speed, but this agility and flexibility frequently comes at the expense of security, putting organizations, customers, and data at risk. As more organizations adopt multi-cloud and hybrid cloud strategies, this is adding additional challenges and threat vectors to an increasingly complex environment.

Organizations can identify potential security gaps and common mistakes by understanding the vulnerabilities of public clouds.

Here are six of the most common that security professionals currently face.

## 1 Public Exposure

It's the oldest mistake in the book— spinning-up a new cloud resource but leaving it publicly accessible and completely unsecured.

Nowadays, hackers routinely employ automated tools to scan target networks for any exposed assets, which guarantees that the unsecured public assets are discovered.

According to Gartner, over 50% of enterprises, unknowingly and mistakenly, have some IaaS storage devices, networks, applications, or APIs that are directly exposed to the public internet, which is up from 25% in 2018.

## 2 Cloud Security Misconfigurations

Despite the rapid shift to cloud, security is still a “greenfield” for many practitioners, who are unsure of which cloud configurations to select and how to do so.

Cloud security misconfigurations can come in many shapes and forms but the one thing that is constant is how ubiquitous they are. Almost any organization, security practitioner, and application can fall victim to some type of cloud security misconfiguration.

According to Gartner, through 2025, the root cause of more than 99% of cloud breaches will be preventable misconfigurations or mistakes by end users.

## 3 Excessive Permissions

A major benefit of migrating to the cloud is faster business operations. However, for such expediency, access credentials are frequently handed out unverified and in a hasty manner, and several users end up with excessive permissions for which they have no business need. The issue arises when any of those credentials fall into the wrong hands, as the attackers have widespread access to sensitive data.

According to Gartner, by 2023, 75% of cloud security failures will be the result of inadequate management of login credentials, identities, and privileges, up from 50% in 2020.

## 4 Too Many Alerts

It sounds counterintuitive, as the detection of suspicious activities is a good activity. However, these alerts may drown the recipients in too much noise instead of helping them in detecting malicious activities.

According to a study by the IT security firm Bricata, the average system operations center receives over 10,000 alerts daily, which is a large number that no individual or team can deal with. This means that security managers must sift through a sea of alerts, and false positives to find the specific alerts which are indicative of malicious activity.

## 5 Insufficient Context

One of the key challenges in cloud security is that any single alert does not provide much information or context. For example:

- Is that login in the middle of the night a hacker, or an admin working late?
- Is that first time API invocation an act of reconnaissance, or a DevOps engineer going about their business?
- Is that access to a sensitive storage bucket a new feature being released, or the last step in a data breach?

Every user activity can either be legitimate or illegitimate, and it is impossible to determine or distinguish one from the other by simply by looking at that activity.

Instead, what is required is to be able to intelligently correlate events across multiple threat surfaces, application layers, and time spans, connect event A to event B to event C, even if they are months apart, and finally identify when the system is under attack, and to block it in time.

## 6 Malicious Access

According to IBM’s 2021 report “The Cost of Data Breach”, stolen credentials are the number one cause of data breaches, accounting for one in every five breaches. Once obtained, attackers use these stolen credentials for malicious purposes by accessing the network and searching for sensitive data, then exfiltrating and selling it on the dark web.

This is an even bigger problem in cloud environments, where security managers have less visibility and control over the actions of cloud users.

# Close These Common Vulnerabilities

There are two critical factors that help address these vulnerabilities. First, understand that the cloud is not more or less secure, but different. This means that cloud native protection is critical, and defenses are required that are specifically adapted to the cloud and tailored to the unique threats faced therein. Secondly, automation is key. Easily exploitable vulnerabilities can be prevented using defensive automation procedures that automate detection when a system is attacked. Of the aforementioned vulnerabilities, four of them can be “closed” using defensive automation:

- **Publicly Exposed Assets**
  Getting in the public cloud makes it very easy to spin up new resources and to forget to secure them. Automated defensive tools can help identify publicly exposed assets and ensure that they are secured.
- **Cloud Misconfigurations**
  Ensure that the cloud environment does not fall prey to common cloud misconfigurations, as they make cloud network vulnerable to penetration and exploitation.

- **Excessive Permissions**
  Public cloud environments are notorious in granting unnecessary permissions to users who have no business need for them. Intelligent permission analysis methods and smart hardening procedures can help crack down on excessive permissions, thereby limiting the threat surface without interfering in business activities.
- **Compliance Violations**
  Cloud security is often a black box to many organizations. Therefore the first objective for organizations migrating to the cloud is to make sure that they are following the applicable national and industry standards. Defensive automation can help identify and address the compliance requirements that are not being met.

Gaining visibility into vulnerabilities and leveraging automation requires comprehensive and consistent security across public and hybrid clouds.
Learn more

## About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.