Brought to you by:

maxtec

# 2022 State of Public Cloud Security Report

Identifying security gaps in public cloud environments and how they can be prevented

# Contents


- Foreword ..... 3
- Executive Summary ..... 4
- About the Orca Research Pod ..... 5
- Key Findings ..... 6
  1. Your Castle in the Cloud ..... 7
  2. Upkeep and Maintenance ..... 8
  3. Castle Hygiene ..... 11
  4. Construction Mistakes ..... 13
  5. Keys to the Kingdom ..... 14
  6. Past the Gates ..... 15
  7. Protecting the Crown Jewels ..... 16
  8. Attack Paths ..... 17
  9. The Cloud Chess Pieces ..... 18
  10. Key Recommendations ..... 21
- About Orca Security ..... 22

# Foreword

In the past year, organizations have had to deal with many cybersecurity challenges. Critical and ubiquitous vulnerabilities such as Log4Shell, and to a lesser extent Spring4Shell, had security teams working around the clock. In addition to all this, teams are dealing with tremendous global unrest, heightening the chance of cyberattacks on organizations.

The Orca Research Pod has been diligently investigating cloud products and services to find unknown, zero-day vulnerabilities before malicious actors do. So far this year, Orca has announced five major vulnerabilities in Azure and AWS and worked with cloud and service providers to resolve them.

**Brought to you by:**

maxtec

Through our partnership with Orca Security, the leading agentless cloud security platform, we are delighted to share this comprehensive cloud security report with you.

We hope this report will help organizations reduce attack surfaces and strengthen cloud security postures.

We at Maxtec are available to discuss your cloud security concerns and how we can help you and your customers bolster their security in the cloud.

**Praven Pillay**
Managing Director
Maxtec

# Executive summary

All roads lead to the cloud. That is true now more than ever before. The significant advantages that the cloud brings, including increased agility, scalability, and reliability was already driving organizations towards cloud adoption. However, the global pandemic greatly accelerated this trend, with the sudden and massive move to remote work and the ensuing need to provide employees with access to business systems literally from anywhere.

**The cloud adoption trend is predicted to continue with great strides.**

Gartner predicts that worldwide spending on public cloud services will grow **20.4%** **in 2022** **to total** **$494.7 billion**

and expects it to reach nearly **$600 billion** **in 2023**[1]

**However, it is important to recognize that cloud adoption comes with new security challenges.**

Even though the cloud platform provider is responsible for securing the infrastructure, organizations are still responsible for securing the applications and services they run in the cloud. Simply deploying on-premises security solutions in the cloud may seem like an easy solution at first, but will soon come up short as organizations start to deploy more cloud-native applications and security teams struggle to keep up.

**This report assesses the different areas of public cloud security and sheds light on their current security state to help organizations better understand where their most critical security gaps are.**

The report further provides recommendations on what actions need to be taken to achieve the biggest improvements in cloud security postures.

[1]Gartner Forecast: Public Cloud Services, Worldwide, 2020-2026, 1Q22 Update

# About the Orca Research Pod

The Orca Research Pod is a group of 12 cloud security researchers with a combined experience of 79 years in cybersecurity. Our expert team discovers and analyzes cloud risks and vulnerabilities to strengthen the Orca Cloud Security Platform and promote cloud security best practices. In addition, the Orca research team discovers and helps resolve vulnerabilities in cloud provider platforms so organizations can rely on a safe infrastructure in the cloud.

## Discovered and helped resolve 5 critical vulnerabilities on AWS and Azure

### 1 AWS Superglue

Severity: Critical
Discovery date: October 4, 2021
Time to remediation: 15 days
Affected service: AWS Glue
# Potentially affected orgs: 7% of our AWS customers use AWS Glue.

### 2 Azure AutoWarp

Severity: Critical
Discovery date: December 6, 2021
Time to remediation: 4 days
Affected service: Azure Automation
# Potentially affected orgs: 54% of our Azure customers use Azure Automation

### 3 AWS BreakingFormation

Severity: Critical
Discovery date: September 9, 2021
Time to remediation: 26 hours
Affected service: AWS CloudFormation
# Potentially affected orgs: 5% of our AWS customers use AWS CloudFormation.

### 4 Azure SynLapse

Severity: Critical
Discovery date: January 4, 2022
Time to remediation: 5 months
Affected service: Azure Synapse
# Potentially affected orgs: 13% of our Azure customers use Azure Synapse

### 5 Databricks on AWS

Severity: High
Discovery date: December 12,, 2022
Time to remediation: 3 hours
Affected service: Databricks-managed cloud storage
# Potentially affected orgs: 1% of our AWS customers use DataBricks

## Methodology

The Orca Research Pod compiled this report by analyzing data captured from billions of cloud assets on AWS, Azure and Google Cloud scanned by the Orca Cloud Security Platform.

**Report Data Set:**

- Cloud workload and configuration data
- Billions of real-world production cloud assets
- AWS, Azure and Google Cloud environments
- Collected between January 1st - July 1st, 2022

# Key Findings

This year's study shows that while many organizations list cloud security as one of their top IT priorities, there are still many basic security practices that are not being followed. In the rush to move resources to the cloud, organizations struggle to keep up with ever-expanding cloud attack surfaces and increasing multi-cloud complexity. The current shortage of cybersecurity skilled staff is further worsening the situation.

**36%**

of organizations have **unencrypted sensitive data** such as secrets and PII on their cloud assets.

**Why is this significant?**
Encrypting sensitive data greatly reduces the likelihood that it is unintentionally exposed and can nullify the impact of a breach if the encryption remains unbroken.

**78%**

of identified attack paths use **known vulnerabilities (CVEs)** as an initial access attack vector.

**Why is this significant?**
The vast majority of attacker entry points can relatively easily be prevented since these CVEs are known and the vast majority have remediations available.

**7%**

of organizations have Internet-facing **neglected assets with open ports.**

**Why is this significant?**
This is especially dangerous since attackers continually scan for open ports and known vulnerabilities and is basically a disaster waiting to happen.

The average attack path only needs

**3 steps**

to reach a crown jewel asset.

**Why is this significant?**
The root account has *complete access to all services and resources* in the account. It is extremely important that MFA is enabled since bad actors can try to obtain root credentials using brute force attacks and password spraying.

**33%**

of organizations have a cloud provider **root account without multi-factor authentication.**

**Why is this significant?**
The root account has *complete access to all services and resources* in the account. It is extremely important that MFA is enabled since bad actors can try to obtain root credentials using brute force attacks and password spraying.

**72%**

have at least one S3 Bucket that allows public READ access.

**Why is this significant?**
This is a highly exploitable misconfiguration and the cause of many data breaches. Even though by default an S3 bucket is always created as "private", misconfigurations and human error can sometimes lead them to be exposed to the public.

**12%**


have an Internet-facing workload with at least one weak or leaked password.

**Why is this significant?**
This is an easy way for attackers to gain access to your cloud environment.

**70%**

have a Kubernetes API server that is publicly accessible.

**Why is this significant?**
This leaves the Kubernetes API server exposed to reconnaissance attempts and potential zero-day attacks.

**58%**

have a serverless AWS Lambda function or Google Cloud function with unsupported runtimes

**Why is this significant?**
Unsupported runtimes means that they are no longer patched or maintained by the cloud provider, which exposes the function to multiple risks and is similar to a neglected asset.

On average, organizations take

**18 days**

to fix an 'imminent compromise' security alert.

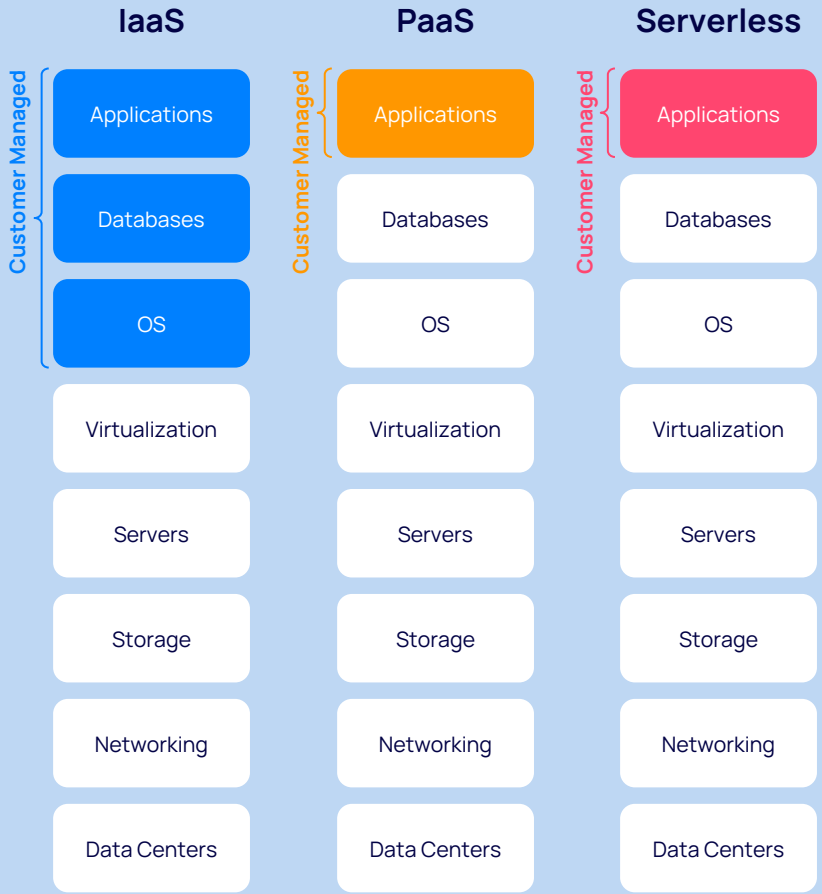
**Why is this significant?**
Imminent compromise security alerts are high priority alerts. Cloud security postures could be greatly improved by fixing issues faster

# 1

## Your Castle in the Cloud

Your cloud environment is a bit like a 'hosted castle' in the cloud. Following the shared responsibility model, the cloud platform provider gives you a plot of land to build on and surrounds it with a moat. However, you need to make sure your castle is impregnable by securing it with thick walls, a drawbridge, turrets, and a copious collection of guards.

In more specific terms, depending on the type of cloud service that is being consumed, the customer's responsibilities always include securing the applications it runs in the cloud, and in the case of IaaS, also includes any databases and operating systems used in the cloud.



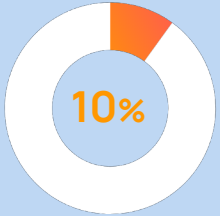
# 2
# Upkeep and Maintenance

An important part of keeping your 'castle' secure is to regularly patch, upgrade and maintain your cloud environment.

## 2.1 Vulnerabilities

With the sheer number of vulnerabilities being discovered every day, it is difficult for organizations to keep up. Many fall behind on patching newly discovered vulnerabilities, but some are also not addressing vulnerabilities that have been around for a long time.

We found that




of organizations have vulnerabilities that were disclosed **10+ years ago.**

On average, we found that Compute assets (VMs, containers and their images) have no less than **50** known vulnerabilities (CVEs) in one year.

It is important to address severe vulnerabilities as quickly as possible, since this is by far the most common initial attack vector (**78%**).

It is close to impossible for teams to fix all vulnerabilities. Therefore, it is essential to remediate strategically by understanding which vulnerabilities pose the greatest danger to the company's crown jewels and need to be **fixed first**.

## 2.2 Log4Shell

In December 2021, the cybersecurity world was rocked by the discovery of a serious zero-day vulnerability in Apache Log4j, a ubiquitous logging tool included in almost every Java application.

The vulnerability was easy to exploit, allowed unauthenticated remote code execution (RCE), and was dubbed 'Log4Shell'.

Even more unsettling was the fact that there was no patch available when the vulnerability was originally published. The open source developers hastily released several patches which in turn introduced new vulnerabilities, until the issue was finally resolved after the 4th patch.

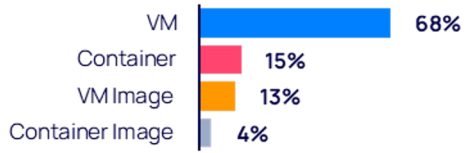
Fast forward to mid 2022. Most organizations have been frantically patching Log4j vulnerabilities in the last 6 months. However, we are still finding that Log4Shell is alive and well in many cloud environments:

Almost **5%** of workload assets still have at least one of the Log4j vulnerabilities[2] of which **10.5%** are internet-facing.

**30%** of the Log4j vulnerabilities discovered between December 2021 - January 2022 remain unresolved, of which **6.2%** potentially expose PII.

The vast majority **(68%)** of the Log4j vulnerabilities are found on VMs. There are also still quite a few Log4j vulnerabilities found on containers and container images. Images are particularly problematic since these vulnerabilities will be reproduced each time the image is used.

**Asset Types with Log4Shell vulnerabilities**




Footnotes:
2. When we mention Log4j vulnerabilities, we are referring to the following CVEs: CVE-2021-44228, CVE-2021-4104, CVE-2021-45046, and CVE-2021-45105.

## 2.3 Neglected Assets

A neglected asset is a cloud asset that uses an unsupported operating system (such as CentOS 6, Linux 32-bit, or Windows Server 2012) or has remained unpatched for 180 days or more. Needless to say, these assets are extremely vulnerable to exploitation.

The reason why some organizations still have neglected assets is because they have old applications that don't support updated OSes.

However organizations should make it a priority to upgrade these systems since they are easy attack vectors for cyber attackers.

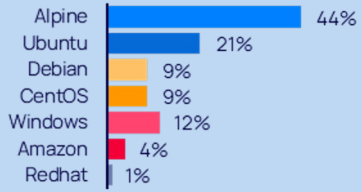
On average, organizations have **11%** of their assets in a neglected security state, and **10%** of organizations have more than **30%** of their workloads in a neglected security state.

**19%** of identified attack paths use **neglected assets** as an initial access attack vector

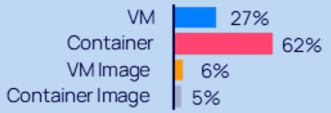
**7%** have Internet facing neglected assets with open ports 80, 443, 8080, 22, 3389 or 5900. This is especially dangerous since attackers continually scan for open ports and known vulnerabilities. The equivalent of this is basically leaving the front door open and then having a safe inside your house with a broken lock.

Out of all neglected assets, the majority are **containers** and nearly half are running unsupported versions of **Alpine OS.**

**OSes on Neglected assets**




**Asset Types of Neglected assets**




Neglected assets are the **weakest links** in your cloud environment. If you cannot patch or upgrade these systems, if possible try to segment them from other assets to prevent exposing the rest of your environment.

# 3
# Castle Hygiene

By adhering to cloud hygiene best practices and applying these consistently across the board, the chance of a damaging cloud breach is significantly reduced. Below we have highlighted some less than desirable practices that were present in environments.

## 3.1 Unused Credentials

Unused IAM users and roles provide additional attack vectors for malicious actors. It is good practice to regularly clean up and remove any unused IAM users and roles to reduce your attack surface.

Out of all scanned organizations with AWS environments, **76%** had credentials that had not been used for 90+ days.

## 3.2 Multi-Factor Authentication (MFA)

To prevent account hijacking, it is always recommended to use multi-factor authentication (MFA).

**33%** have an AWS cloud provider root account without MFA. This is very risky since the root user account is the most privileged user in the cloud account.

Nearly **half** of AWS environments have at least one role that allows cross-account access without external ID or MFA, not only increasing the chance of unauthorized access, but also widening the scope of user access that could be compromised.

**58%** have MFA disabled for at least one privileged user in Azure.

It is highly recommended that you conduct cloud security audits at least twice a year to ensure basic cloud security hygiene is being followed and the attack surface is minimized.

## 3.3 Principle of Least Privilege (PoLP)

The principle of least privilege (PoLP) is the practice of limiting users' access rights to only that which is strictly required to do their jobs.

**44%** of environments have at least one privileged identity access management (IAM) role. If an attacker gets hold of privileged IAM credentials, they not only gain access to the system, but can also remain undetected. By activating privileged access only for the duration it is needed, the attack surface can be greatly reduced.

**71%** use the default service account in Google Cloud. This is not recommended because this account gives you Editor permissions by default, not aligning to PoLP.

**42%** of the scanned cloud estates granted administrative permissions to more than 50% of the organization's users

**41%** of organizations have a role that can be assumed by an external identity which could be exploited by malicious actors to compromise your cloud resources. It is recommended to always use external IDs and/or MFA while granting access to external identities.

## 3.4 Remediation Time

Attack surfaces can be greatly reduced by remediating known risks as fast as possible. On average, organizations take **18 days** to fix an 'imminent compromise' alert. Authentication issues are the quickest to be remediated, with on average 6 days to fix. Neglected assets and lateral movement are the alerts that take longest to fix, with an average of 27 and 47 days per alert.

**# Days to remediate 'Imminent Compromise' alerts:**

- Authentication **6 days**
- Data at risk **13 days**
- Network misconfigurations **25 days**
- Malicious activity **7 days**
- IAM misconfigurations **22 days**
- Neglected assets **27 days**
- Best practices **13 days**
- Vulnerabilities **23 days**
- Lateral movement **47 days**

Note that it is not the remediation time of *all* vulnerabilities that is important, but the remediation time of those vulnerabilities that pose the biggest danger to your organization. These are not identified by just looking at the CVSS score, but by understanding which risk combinations are a direct path to your critical assets.

# 4

# Construction Mistakes

No matter how much training is provided or how well-intentioned the IT professional is, to some degree, human error is unavoidable. In fact, Gartner predicts that through 2025, more than 99% of cloud breaches will originate from preventable misconfigurations or mistakes by end users[3]. Here we have listed the top three cloud misconfigurations that we see in our scanned environments.

## 4.1 Top Misconfiguration #1: AWS KMS Key Misconfigurations

The AWS Key Management Service (KMS) allows administrators to create, delete and control keys that encrypt data stored in AWS databases and products.

- **8%** have configured a KMS key with public access policy. This is particularly dangerous since it creates an easy attack vector for a malicious party.
- **99%** use at least one default KMS key. It is always recommended to use customer-managed CMKs instead of AWS-managed.
- **80%** have KMS rotation disabled. It is better to enable rotation for all of the KMS master keys to reduce the chance of an attacker using CMKs without your knowledge.

## 4.2 Top Misconfiguration #2: Policy and Access Misconfigurations

- **80%** have a user with an inline policy and **49%** have a group with an inline policy. It is highly recommended to use IAM Groups to manage permissions instead of using inline or directly attached policies, since this reduces the possibility that a user or group inadvertently receives or retains excessive privileges.
- **79%** have at least one access key older than 90 days. It is best practice to configure access keys older than 90 days to be rotated, to limit the time a compromised set of IAM access keys could potentially provide access to your AWS account.
- **51%** have a Google Storage bucket without uniform bucket-level access. If access levels are not set uniformly, this means that an attacker could move laterally and obtain a higher access level.

## 4.3 Top Misconfiguration #3: Database Misconfigurations

- **75%** have AWS MultiAZ disabled. When Multi-AZ is enabled and the primary node goes offline, it will automatically fail over to one of the read replicas, avoiding system downtime.
- **77%** have at least one RDS database instance using default ports and **42%** of these are Internet-facing. It is best practice to change the ports of your RDS databases since if a potential attacker does not know which ports you are using, it makes reconnaissance attempts much harder.
- **42%** of Google Cloud environments don't use automated backups

Footnotes: 3. Gartner 2021 Hype Cycle for Cloud Security

# 5
# Keys to the Kingdom

The keys to the cloud kingdom are found in so-called 'secrets' that are used to authenticate and access systems, including passwords, keys, APIs, and tokens.

It is of the utmost importance that these secrets are kept safe since they are the keys that provide access to your cloud resources.

**18%** have at least one Internet-facing workload with a weak or leaked password

**43%** have at least one clear-text password in the shell history of an Internet-facing Linux workload. On a compromised system, malicious actors will search the bash history file for credentials and other exploitable information.

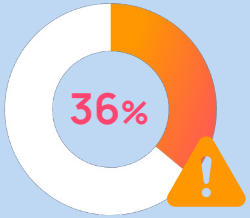
**56%** of organizations on AWS **11%** of organizations on Azure **55%** of organizations on GCP have sensitive keys on their system. This is not good practice since if a malicious actor obtains access to these keys, they can be used to access sensitive resources and perform unauthorized operations.

**21%** have at least one Internet-facing workload with a non-corporate authentication key. Illegitimately added keys usually have non-corporate usernames and email addresses and should therefore be checked and removed.

# 6

# Navigating Past the Gates

Lateral movement is a technique that attackers use to move from one asset to another to reach their end target. The more lateral movement possibility in the environment, the easier the attacker will be able to get to the organization's crown jewels.




of organizations are prone to lateral movement, which means they are exposed to at least one of these risks:

**Insecure Private Key:** If private keys are discovered they can be used together with the public key for lateral movement.

**Group Policy Preferences with cpassword:** Cpasswords are encrypted using a weak encryption algorithm that can easily be decrypted. Once decrypted, the cpassword can be used for lateral movement.

Sensitive **AWS keys,** Azure keys or GCP credentials on system: If these keys or credentials are obtained by a malicious actor, they can be used to access sensitive resources and perform unauthorized operations.

**Password in shell history:** On a compromised system, malicious actors will search the bash history file for credentials and other exploitable information.

**IAM Privilege Escalation:** An attacker with this permission can escalate their privileges by creating or updating an inline policy for a role that they have access to.

# 7

# Protecting the Crown Jewels

A company's crown jewels are its most valuable assets, such as PII, customer and prospect databases, employee and HR information, corporate financials, intellectual property, and production servers. Much like the royal guards who are tasked with protecting a king or queen, the CIO or CISO are tasked with protecting the company's crown jewels.

The company's crown jewels should be protected using the highest security standards and receive the highest priority when deciding which risks need to be remediated first.

**36%**

of organizations have **unencrypted sensitive data** such as secrets and PII in files, storage buckets, containers, and serverless environments. Encrypting sensitive data greatly reduces the likelihood that it is unintentionally exposed and can nullify the impact of a breach if the encryption remains unbroken.

**35%**

have at least one Internet facing workload with sensitive information in a Git Repository. Cybercriminals can easily extract this information and use it to compromise your systems.

**6%**

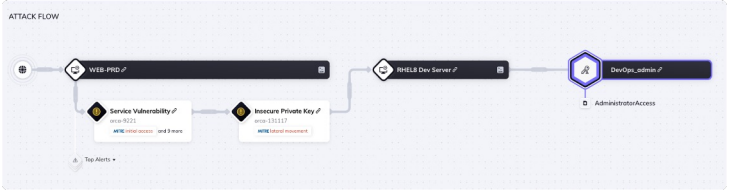
of the unresolved Log4j vulnerabilities discovered between December 2021 - January 2022 potentially expose PII.

# 8 Attack Paths

An attack path is the route that an attacker takes - or could take - to reach their target, with the goal of confidential data exfiltration, holding the organization to ransom, or selling PII. En route to the company's crown jewels, attackers take advantage of weaknesses in the environment to gain access to specific assets and move laterally from one to the other.

## 8.1 Steps in the attack path

The average attack path only needs **3 steps to reach crown jewels**. This means that an attacker only needs to find 3 connected and exploitable weaknesses in a cloud environment to exfiltrate data or hold an organization to ransom.

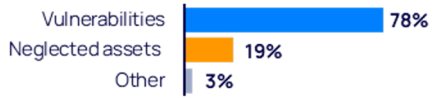



For example, in the attack path above, the initial attack vector is

1. an EC2 instance with a service vulnerability that allows asset compromise. On this asset, there is also
2. an insecure private key that enables access to the asset 'Dev Server', that could be exploited by an attacker to move laterally. Once the attacker gains access to the 'Dev Server' asset, they
3. can obtain an admin role that allows administrator access to the entire account.

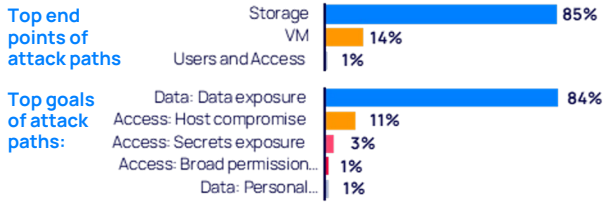
## 8.2 Top initial attack vectors

The vast majority of attacks start by exploiting a vulnerability. Neglected assets account for nearly one fifth of initial attack vectors.




## 8.3 Top end targets and goals

The vast majority of attack paths end with a storage asset, indicating that the end goal is to steal data. The top goal of an attack path in by far the most cases is Data exposure of sensitive information such as financial data or other confidential information, although only 1% actually have obtaining PII as their top goal.



# 9

# The Cloud Chess Pieces

The cloud environment contains many different asset types and services, ranging from VMs and containers to databases and secrets. The largest asset category **(23%)** is the network category, which includes security groups, firewalls, network roles, and assets that are run in a closed network in the cloud. After network assets, storage and databases are the most deployed assets in the cloud.

## 9.1 Storage

Examples of cloud storage services are AWS Simple Storage Services (S3) Buckets, Azure Blob storage, and Google Storage buckets. It is recommended to encrypt stored data and to perform regular backups to protect against ransomware attacks. Since storage assets often include business critical or confidential data, it is also important that they are securely configured. Unfortunately we find that all too often preventable storage misconfigurations are leaving the door open to data exfiltration and ransom requests:

- **72%** of AWS environments have at least one S3 Bucket that allows public READ access. Even if an S3 Bucket does not contain sensitive data, it is still good practice to keep all S3 buckets at their default "private" setting, since another team member may inadvertently save sensitive data in the bucket without realizing that it is set to allow public READ access.
- **42%** of organizations using Azure have at least one public blob container. However, only 2.5% of the Azure Blob Storage assets are publicly exposed. Note that unauthorized access on Azure blobs is much harder to accomplish than on S3 buckets, because you need to know the unique storage account name, the name of the blob itself before you can even attempt access.
- **39%** of Google Cloud environments have at least one publicly-accessible Google storage bucket. Similar to publicly-exposed S3 buckets, this means that it will be easy for an attacker to access the data.

## 9.2 Databases

Since database assets often include business critical and/or confidential data, it is important that cloud administrators deploy a robust database protection strategy against unwanted access and data breaches. Below we have listed areas where databases should be configured more securely:

- **60%** are not encrypting database instance snapshots, which means that they are easily readable by a potential attacker
- **67%** only require a password and username for database access without using IAM authentication, making them vulnerable to brute-force and dictionary attacks.
- **2%** are using the default AWS user name for their Amazon Relational Database Service (RDS). By using the default username, a potential attacker only needs to guess the password, which can be done with a brute force attack or password spraying
- **73%** do not use logging services for their databases. It is recommended to enable logging for security and troubleshooting purposes.

## 9.3 VMs

Virtual Machines (VM) are a compute resource that mimic physical machines by running a separate system with their own OS and applications. For VM security, it is important to know what is running on your VM instances (OS, software, etc) and that they are free of risks. It is also important to ensure that VM images are regularly checked for risks. Since images are used to create new VMs, any risks will automatically be duplicated when they are copied to create new VMs

**71%**

of Google Cloud environments have a VM instance using the default service account, which an attacker can use to move laterally across compute engine instances

**23%**

have at least one Internet facing EC2 Instance that has full Access to S3. This is very dangerous since if the EC2 is compromised, all the S3 buckets will be exposed to the attacker

**23%**

have at least one EC2 Instance with Administrator Privileges. This means that if the EC2 is compromised, it can potentially lead to full account takeover.

**32%**

have at least one Internet Facing GCP Compute Engine Instance with Broad Storage Read Permission, which does not adhere to the least-privilege principle.

## 9.4 Containers

Containers package applications and their dependencies and run them in isolated environments. Unlike VMs, containers usually do not contain an entire operating system and are therefore more lightweight, use fewer resources, and allow for greater application modularity. For this reason, containers are rapidly gaining popularity.

- **16%** of the containers are in a neglected state, which means that they use an unsupported operating system or have remained unpatched for 180 days or more
- **84%** have at least one container with the critical Open SSL infinite loop DoS vulnerability (CVE-2022-0778)
- **28%** have at least one container with the Spring4Shell RCE vulnerability (CVE-2022-22965 RCE)
- **17%** have at least one container with the critical Samba RCE vulnerability (CVE-2021-44142)

## 9.5 Kubernetes

Kubernetes is an open source system for automating the deployment, scaling, and management of containerized applications. Kubernetes usage is growing fast, with **56%** of the organizations using Kubernetes.

**62%** of containers are being orchestrated by an outdated version of Kubernetes.

**70%** have a Kubernetes API server that is publicly accessible. This leaves the Kubernetes API server exposed to reconnaissance attempts and potentially zero-day attacks.

**30%** have a controller of pods with a role that allows the creation or modification of other pods. This can allow an attacker to gain an initial foothold and facilitate lateral movement by an attacker

Kubernetes was designed with functionality in mind, not security, therefore it is very important to apply the principle of least privilege on K8s and ask questions such as: Does this cluster have to be accessible from the broad Internet? Does this controller need a broad set of permissions? It is important to ask these questions when creating the resources, since fixing these issues after deployment is much more complicated.

## 9.6 Serverless

In serverless architectures, all of the microservices are provided and managed by cloud providers. The advantage of this is that developers do not need to worry about purchasing, provisioning, and managing backend servers. However, this does not mean that organizations are no longer responsible for the security of their serverless functions.

**69%** have at least one serverless function exposing secrets in the environment variable. This means that there are keys, authorization tokens, or passwords that can be exploited by malicious actors.

**37%** have at least one serverless function with admin privileges. In accordance with the Principle of Least Privilege (PoLP), it is recommended to only provide functions with the permissions that are required to perform their tasks.

**58%** have an AWS Lambda function or Google Cloud outdated function with unsupported runtimes, which is similar to using an unsupported OS on a VM. Unsupported runtimes means that they are no longer patched or maintained by the cloud provider, which exposes the function to multiple risks.

# 10

# Key Recommendations

Based on our findings, we have summarized key recommendations for organizations wishing to reduce their cloud attack surface and harden their environments:

### Identify your crown jewels:

The first step in your cloud security strategy should be to identify which of your cloud assets are business critical and/or contain sensitive data. These are your 'crown jewels' and should always be protected by the highest security standards. Any threats that endanger these assets should always be addressed above all others.

1

### Patch, patch, patch:

Whenever possible, systems with known vulnerabilities should be patched. Since it is impossible to patch *all* vulnerabilities, it is important to understand which vulnerabilities enable dangerous attack paths and make sure those are patched first.

2

### Maintain a cloud asset inventory:

You can only patch a vulnerability if you know it exists. The Log4j vulnerability highlighted the importance of knowing which cloud assets you have and what they contain, so that teams can quickly patch and mitigate zero-day threats if necessary.

3

### Adhere to the Principle of Least Privilege:

Ensure that administrator privileges are only given to those who really need them, and that regular users don't have the power to escalate their own privileges or create new accounts.

4

### Encrypt sensitive data and keys:

Use encryption for critical assets to limit the impact of potential data and key exposure.

5

### Apply MFA and strong password management:

Always implement Multi-Factor Authentication (MFA) where possible, use strong, unique passwords (including uppercase and lowercase letters, numbers, special characters, and no dictionary words), and rotate passwords frequently.

6

### Perform regular audits:

Perform cloud configuration audits at least twice a year to ensure best practices are followed and cloud misconfigurations are addressed.

7

### Eliminate unused assets:

Make sure that any users, files or systems that are no longer being used are deleted.

8

### Utilize checklists:

To minimize human error, use checklists when creating and configuring cloud assets and resources, as well as onboarding and offboarding users.

9

### Perform backups:

Regularly backup critical data and store offline if possible. This minimizes the impact of a potential ransomware attack since systems can be restored without having to pay the ransom.

10

### Secure templates and images:

Ensure that Infrastructure as Code (IaC) templates and container images are checked for misconfigurations and other risks to prevent repeatedly copying weaknesses into production.

11

# About Orca Security & Maxtec

**For more information:**
www.maxtec.co.za

As the exclusive distributor for Orca Security in Southern Africa, Maxtec is delighted to share the Orca's State of Public Security Cloud report with you.  As cloud adoption continues to accelerate in our region, we hope this report will help you to reduce attack surfaces and strengthen cloud security postures.

Orca's agentless platform connects to your environment in minutes and provides 100% visibility of all your assets, automatically including new assets as they are added. Orca detects and prioritizes cloud risks across every layer of your cloud estate, including vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and overly permissive identities.