DETECT PRIORITIZE ANNIHILATE

HUNTING THREATS IN THE AGE OF RELENTLESS RISK.

Orca's 2025 State of Cloud Security Report

orca SECURITY

> “Cloud security has reached a critical turning point. As organizations increasingly rely on the cloud to accelerate innovation and growth, several converging trends are reshaping the challenges security teams face—and the strategies they need to stay ahead.”

GIL GERON
CEO and Co-Founder of Orca Security

Table of Contents

Foreword

Cloud security has reached a critical turning point. As organizations increasingly rely on the cloud to accelerate innovation and growth, several converging trends are reshaping the challenges security teams face—and the strategies they need to stay ahead.

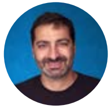
Multi-cloud adoption is now the norm, with 55% of organizations using two or more providers. While this offers greater flexibility and resiliency, it also makes it harder to maintain consistent visibility and coverage across environments. At the same time, AI adoption is increasing—84% of organizations now use AI in the cloud. But this innovation comes with new risks: 62% of organizations have at least one vulnerable AI package, and some of the most prevalent AI-related CVEs enable remote code execution.

Traditional risks haven't gone away either—they've intensified. Nearly a third of cloud assets are in a neglected state, signaling ongoing challenges with monitoring and prioritization.

As organizations store more sensitive data in the cloud, the prevalence of data exposure is rising: 38% of organizations with sensitive data in their databases also have those databases exposed to the public.

These are among the many challenges covered in this report, which highlight the Defender's Paradox in cloud security: attackers need to be right only once, defenders every time. In fact, 13% of organizations have a single cloud asset that supports more than 1,000 attack paths—underscoring the importance of comprehensive detection and effective prioritization.

This report is designed to help teams close their security gaps. Combining real-world insights compiled by the Orca Research Pod, it offers practical guidance on where to focus, what to prioritize, and how to effectively secure multi-cloud environments in the age of AI. We hope this report serves as a valuable resource for your teams.



Gil Geron
CEO and Co-Founder of Orca Security

About the Orca Research Pod

The Orca Research Pod is a group of cloud security researchers that discover and analyze cloud risks and vulnerabilities to strengthen the Orca Cloud Security Platform and promote cloud security best practices.

RESEARCH METHODOLOGY

This report was compiled by analyzing data captured from billions of cloud assets on AWS, Azure, Google Cloud, Oracle Cloud, and Alibaba Cloud and hundreds of thousands of code repositories scanned by the Orca Cloud Security Platform.

REPORT DATA SET

- Cloud workload and configuration data
- Billions of real-world production cloud assets
- Data referenced in this report was collected in 2025
- AWS, Azure, GCP, Oracle Cloud, and Alibaba Cloud environments

25+ VULNERABILITIES DISCOVERED ON AWS, AZURE, AND GOOGLE CLOUD

The Orca Research Pod has discovered more than 25 major vulnerabilities on public cloud platforms. Our expert security team discovers and analyzes cloud risks and vulnerabilities to strengthen the Orca Platform and promote best practices.

2022

+ AWS BreakingFormation
+ AWS Superglue
+ Databricks
+ Azure AutoWarp
+ Azure SynLapse
+ Azure FabriXxs
+ Azure CosMiss

2023

+ Azure Digital Twins SSRF
+ Azure Functions App SSRF
+ Azure API Management SSRF
+ Azure Machine Learning SSRF
+ Azure Storage Account Keys Exploitation
+ Azure Super FabriXss
+ 2 Azure PostMessage IFrame Vulnerabilities
+ Bad.Build Supply Chain Risk in GCP
+ 8 Cross-Site Scripting vulnerabilities on Azure HDInsight
+ Unauthenticated Access Risk to GCP Dataproc

2024

+ Sys:All GKE Loophole
+ 3 new Azure HDInsight vulnerabilities
+ System:authenticated default Google Kubernetes Engine (GKE) group
+ LeakyCLI in AWS and Google Cloud

2025

+ Privilege Escalation Vulnerability in Azure Machine Learning
+ Kubernetes CRD Abstraction Risks in kro (Kube Resource Orchestrator)

Executive Summary

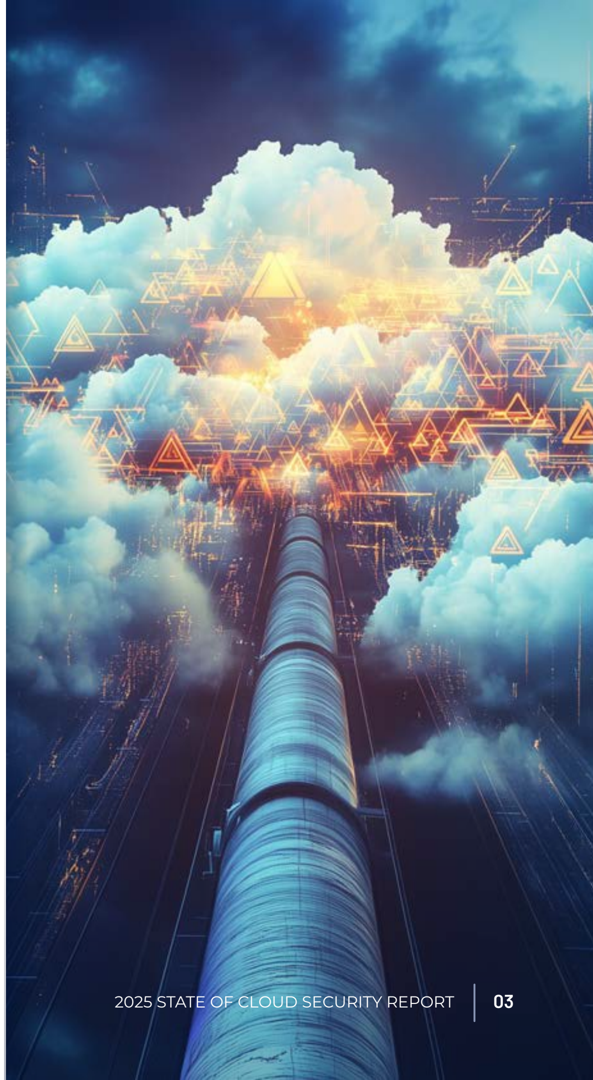
Leveraging unique insights into current and emerging cloud risks captured from the Orca Cloud Security Platform, this report reveals the most commonly found, yet dangerous, cloud security risks. Summarizing the results from our research, these are our main findings:

+ **More cloud innovation brings greater cloud risk.**
  As cloud adoption and cloud-native technologies expand, so does the volume and severity of cloud risks. Nearly a third of cloud assets are neglected today, and each asset contains on average 115 vulnerabilities. Both are two data points among many others illustrating this troubling trend.

+ **Attack surfaces are expanding—and risks are increasingly interconnected.**
  76% of organizations have at least one public-facing asset that enables lateral movement, turning a single risk into an opportunity for broader compromise. Security teams not only need to defend a growing attack surface, but increasingly interconnected risks. To illustrate, 36% of organizations have at least one cloud asset supporting more than 100 attack paths—giving attackers a direct route to endanger high-value assets.

+ **Risks span the entire application pipeline.**
  Cloud security risks aren't confined to runtime environments—they often originate earlier in the application development lifecycle. 85% of organizations have plaintext secrets embedded in their source code repositories. If a repository is exposed, attackers can extract the secrets to access systems, exfiltrate data, and more. Oversights such as these can compound risk across the cloud ecosystem.

+ **Innovation is expanding attack surfaces—and the scale of cloud risks.**
  84% of organizations are now using AI in the cloud, introducing new risks, including AI-related CVEs that enable remote code execution. Kubernetes adoption adds further complexity—93% of organizations have at least one privileged service account, increasing the potential of a breach. Combined with growing multi-cloud adoption, these trends are reshaping the nature and scale of cloud security challenges.



Key Findings

13%

of organizations have a single cloud asset responsible for creating more than 1000 attack paths.

Attack paths represent the toxic risk combinations that attackers can exploit to endanger your high-value cloud assets. When detected, attack paths help security teams prioritize risks, reduce alert fatigue, and maximize productivity.

38%

of organizations with sensitive data in their databases also have those databases exposed to the public.

The exposure of sensitive data—including PII, PHI, financial records, secrets, and more—continues to rise as organizations store more critical information in the cloud.

115

vulnerabilities on average per cloud asset.

The average number of vulnerabilities per cloud asset is significant, especially considering a broader surge in vulnerability exploitation across cloud environments.

58%

of organizations have at least one vulnerability older than 20 years.

For the first time, a majority of organizations are contending with vulnerabilities that have lingered for more than two decades.

32%

of cloud assets on average are in a neglected state.

Nearly one in three assets either run unsupported operating systems or have gone unpatched for over 180 days, providing soft targets for attackers to gain access, move laterally, and escalate attacks.

76%

of organizations have at least one cloud asset that is public-facing and enables lateral movement.

Assets exposed to the Internet and connected internally create critical pathways for attackers to escalate privileges and reach high-value targets within the environment.

85%

of organizations have plaintext secrets embedded in their source code repositories.

Secrets stored in source code pose a major risk. If repositories are exposed through breaches or misconfigurations, attackers can harvest these credentials to infiltrate systems, steal data, or move laterally.

93%

of organizations have at least one privileged Kubernetes service account.

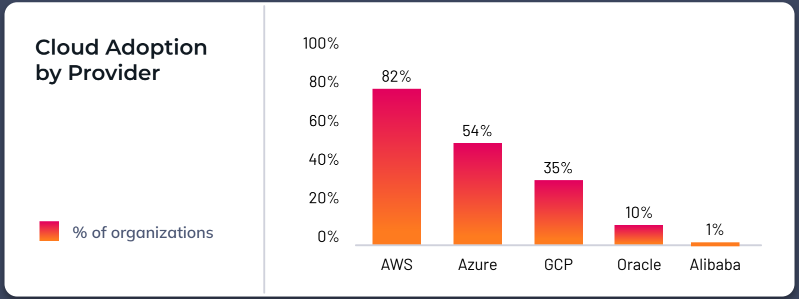
Over-privileged Kubernetes service accounts, if compromised, can be exploited to access sensitive data, escalate privileges, or disrupt workloads across the cluster.

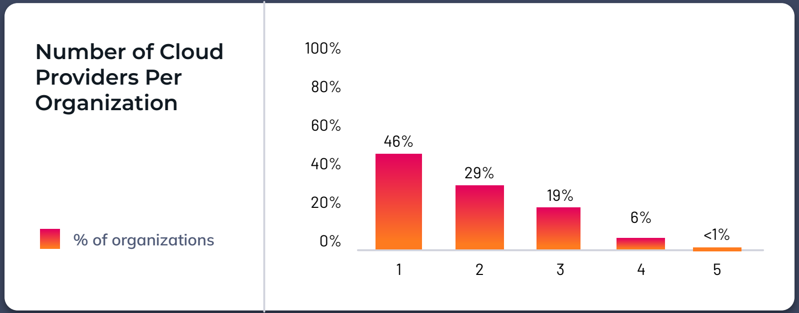
General Cloud Usage

While cloud adoption continues to accelerate, the market remains highly concentrated around AWS, Azure, and Google Cloud Platform (GCP), respectively. Each maintains significant enterprise adoption, led by AWS. Yet the percentages shown in the corresponding table also underscore the notable yet well-established trend toward multi-cloud adoption.

In fact, this year's analysis finds that most organizations are now multi-cloud by design, with **55% leveraging two or more cloud providers**. This marks a significant increase from the 12% of organizations that self-reported deploying multiple clouds in our 2024 Cloud Security Strategies Survey Report, an independent analysis conducted by Gatepoint Research.

What's driving the multi-cloud demand? Other studies point to an interest in capitalizing on provider specialization—including AI services—and building resilience against potential service disruptions and vendor lock-in.


Cloud Adoption by Provider


Number of Cloud Providers Per Organization

01

AI SECURITY

AI Security

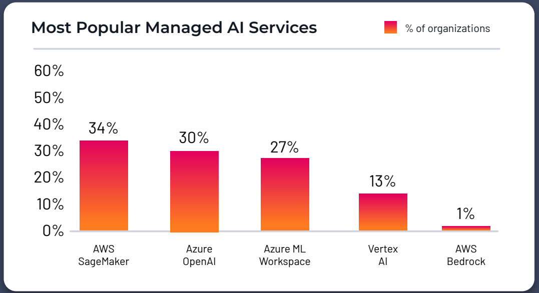
GENERAL USAGE & RELATED CVEs

Demand for cloud AI services continues to surge as organizations look to enhance innovation and operations. This year's report illustrates overall AI adoption in the cloud, the popularity of managed and unmanaged AI services, AI adoption by cloud provider, and the most popular AI packages.

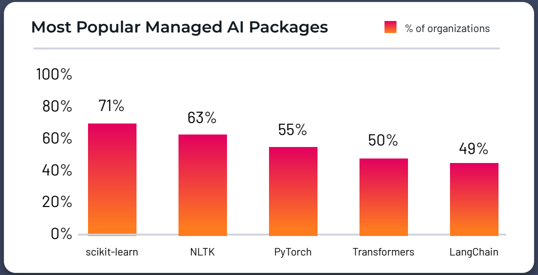
Readers of our 2024 State of AI Security Report understand the related cloud risks of AI adoption, a reality that prevails today. In fact, **62% of organizations have at least one vulnerable AI package in their cloud environment**.

The data below lists the most prevalent CVEs associated with AI packages deployed in cloud environments. Two of them, **CVE-2024-39705** and **CVE-2025-32434**, can allow remote code execution and await NVD enrichment at the time of this writing. This points to the need for better detection, prioritization, and remediation of AI-related vulnerabilities.

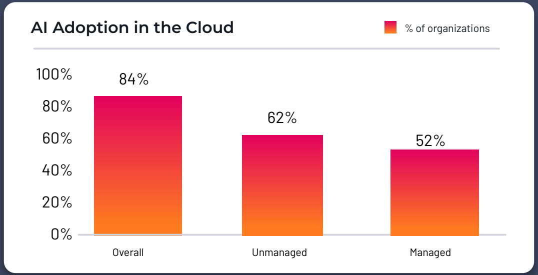
AI PACKAGE	TOP CVE	% OF ORGS USING AI PACKAGE W/ CVE
scikit-learn	CVE-2024-5206	82
NLTK	CVE-2024-39705	72
PyTorch	CVE-2025-2953	59
PyTorch	CVE-2025-3730	59
PyTorch	CVE-2025-32434	57



Most Popular Managed AI Services



Most Popular Managed AI Packages



AI Adoption in the Cloud

02

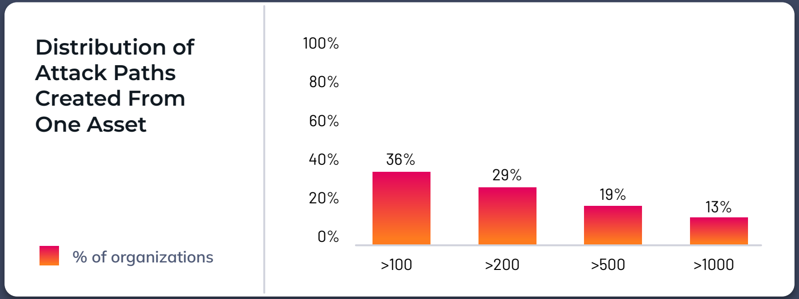
ATTACK PATHS

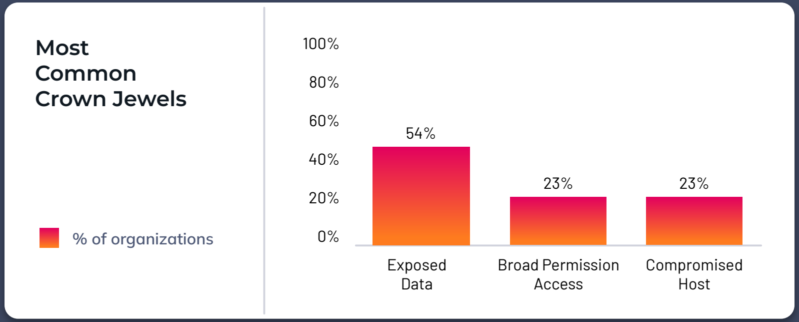
Attack Paths

Attack paths represent the toxic risk combinations that attackers can exploit to endanger your high-value cloud assets (i.e., crown jewels). Attack paths reveal how seemingly isolated risks—like an exposed storage bucket or an over-permissioned identity—can be chained together to exploit resources such as sensitive data, admin-level IAM roles, or critical infrastructure components. They enable security teams to prioritize the risks that matter most, reducing alert fatigue while maximizing resource efficiency and productivity.

The corresponding graphs reveal the most common crown jewels in cloud environments, as well as the distribution of organizations that have a cloud asset supporting more than 100 attack paths. The latter represents a key asset for security teams to prioritize for remediation, since remediating its associated risks can not only break an attack path, but many of them.

Thirteen percent of organizations have a cloud asset responsible for creating more than 1000 attack paths, with the most toxic asset in our dataset responsible for **165,142** attack paths.


Distribution of Attack Paths Created From One Asset


Most Common Crown Jewels

03

DATA EXPOSURE

Data Exposure

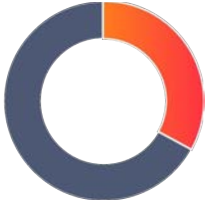
THE BURDEN OF SENSITIVE DATA

Sensitive data—which includes PII, PHI, API keys, financial information, secrets, and more—pose a significant risk when publicly exposed, increasing the likelihood of unauthorized access, data theft, compliance violations, and other severe security incidents.

According to our analysis, sensitive data exposure is prevalent across storage buckets, databases, and cloud functions. While the reasons may vary, multiple studies show that organizations are not just storing more data in the cloud, but *sensitive data*.

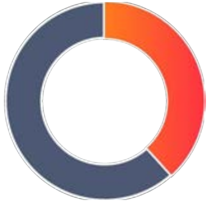
This naturally follows the continued increase in cloud adoption and cloud-native applications. Through 2026, Gartner predicts that 70% of organizations will increase their cloud spending with specialty cloud providers to support their business needs.

The growth of cloud data and storage expands the attack surface for organizations and makes it more attractive to attackers. Threat actors prize sensitive data, especially at a time when the demand for data continues to increase amid AI innovation. It underscores a troubling trend that calls for more attention on data security.



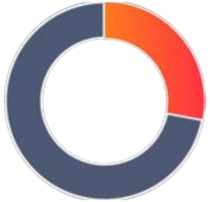
33%

of organizations with publicly exposed storage buckets have sensitive data in them.



38%

organizations with sensitive data in their databases also have those databases exposed to the public.

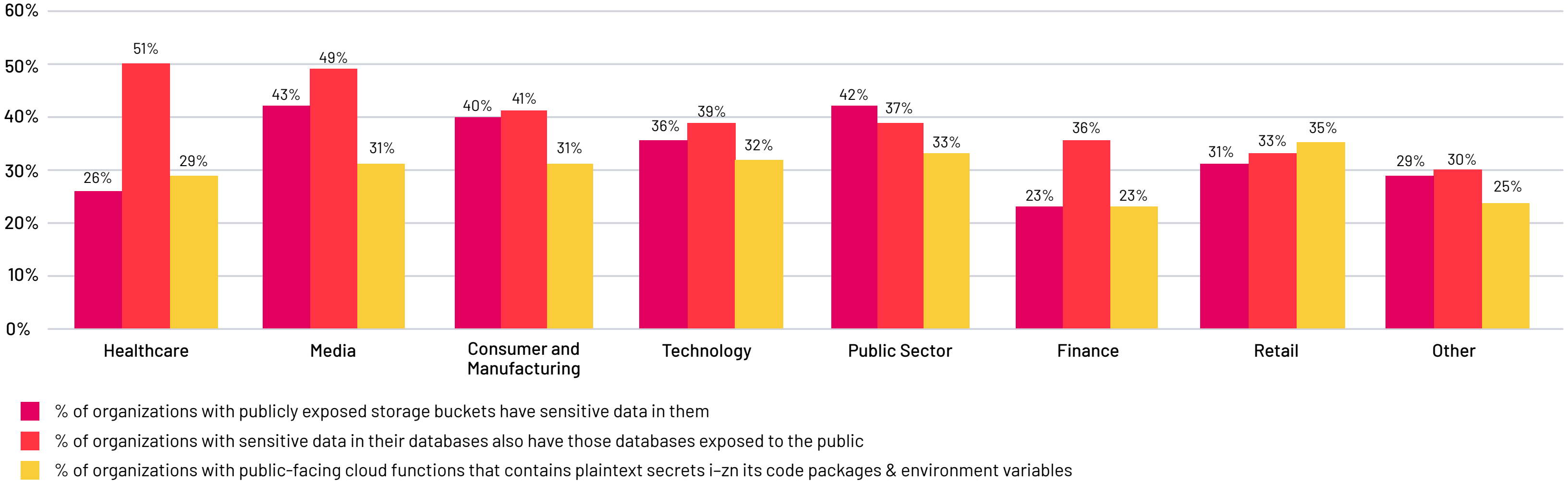


28%

of organizations with cloud functions have publicly accessible functions with plaintext secrets in the function's code package and environment variables.

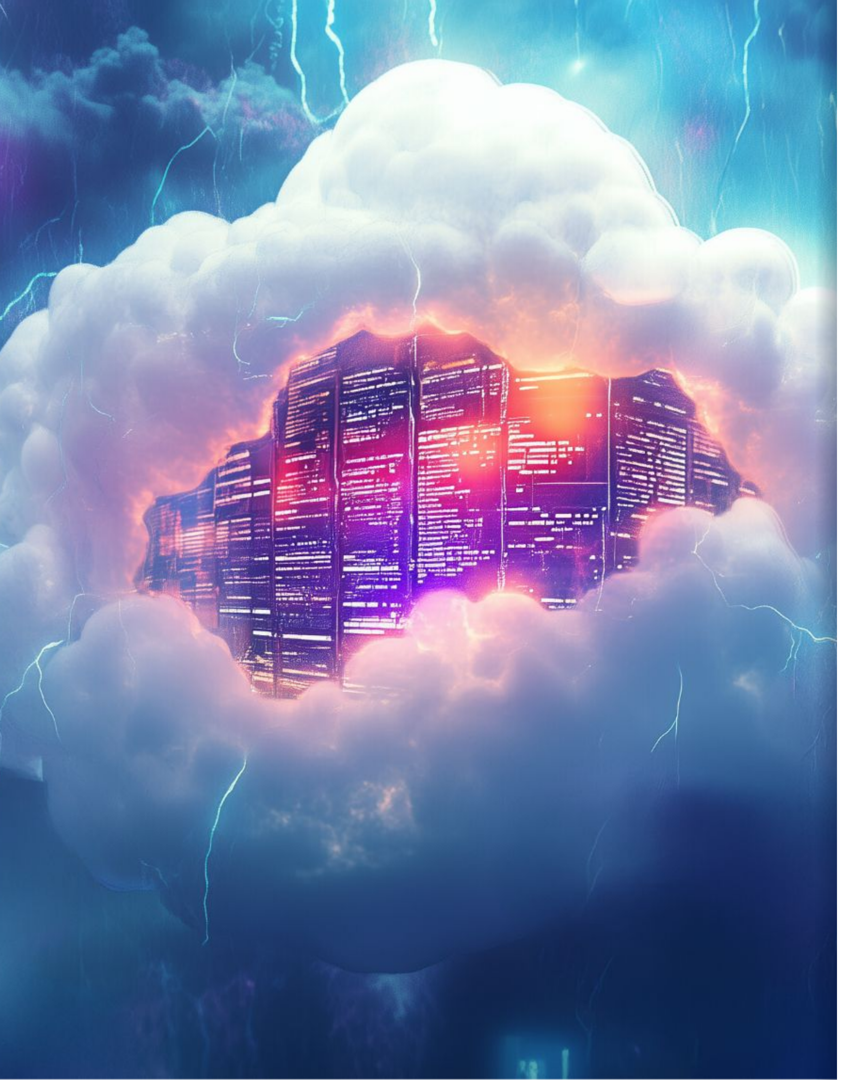
THE BURDEN OF SENSITIVE DATA

Healthcare is the industry most susceptible to sensitive data exposure for databases—an alarming fact for organizations. The Health Insurance Portability and Accountability Act (HIPAA), for example, regulates the privacy of protected health information (PHI) in the US, and can impose fines up to $1.5 million (USD) for violations depending on culpability. Yet the risk appears to affect a significant proportion of organizations across all industries.



04

VULNERABILITIES



Vulnerabilities

4.1 VULNERABILITIES - A TIMELESS CHALLENGE

Vulnerabilities predate the cloud as a top concern for security leaders and teams. Yet, year-after-year, they sustain their relevance—with this year no exception. Our analysis shows that the average cloud asset carries a significant number of vulnerabilities that security teams must contend with.

In fact, cloud assets on average have 115 vulnerabilities. This represents a significant number when we consider that vulnerability exploitation continues to increase.

According to VulnCheck, the number of CVEs exploited and publicly disclosed rose 20% YoY in 2024, totaling 768 CVEs. Findings from the 2025 Data Breach Investigations Report also show an increase in vulnerability exploitation (34%), making it the second most popular initial access vector for breaches and partly responsible for one-fifth of the data breaches publicly disclosed in 2024.

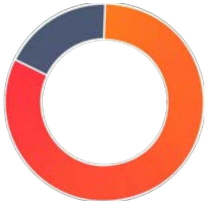
115 The average number of vulnerabilities per cloud asset

4.2 UNPATCHED WEB SERVICES

Web services are applications that are able to send or receive communication over a network, whether internal or the public Internet. They provide a way to communicate, connect, and use an application over a network. Unpatched services, with known vulnerabilities and bugs, can be one of the main attack vectors into your system. Malicious actors can exploit an unpatched vulnerability or bug to cause service downtime or a denial of service. In some cases, unauthorized remote access may also be a possibility.

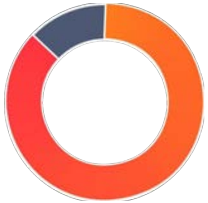
According to our analysis, nearly eight in every 10 organizations have at least one unpatched web service. This remains notable in light of an October 2024 joint Cybersecurity Announcement (CSA) by the FBI, NSA, CNMF, and NCSC-UK. The CSA cautioned organizations about APT29—an Advanced Persistent Threat (APT) tied to the Russian Federation’s Foreign Intelligence Service (SVR)—targeting software vulnerabilities to gain initial access, escalate privileges, move laterally, persist in environments, and exfiltrate data.

Targets specified in the CSA included technology companies, which can fuel supply chain attacks. Notably, a significant majority of technology companies in our analysis have at least one unpatched web service, along with healthcare organizations, which also remains a popular target among threat actors. Security teams should ensure that all components of a web service, including the web server and third-party libraries, are up-to-date.



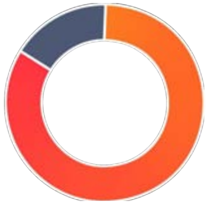
82%

of organizations have at least one unpatched web service.



87%

of healthcare organizations have at least one unpatched web service.



84%

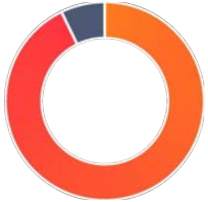
of technology organizations have at least one unpatched web service.

4.3 OLD, BUT STILL RELEVANT

There's a familiar saying: problems don't go away by themselves. And that's especially true when it comes to vulnerabilities. In 2024, we saw a slight but important increase in the number of organizations with vulnerabilities at least 10–20 years old. This year marked the first time in our analysis that a majority of organizations are now dealing with a vulnerability at least two decades old. While these risks aren't new, they deserve attention considering that they're often well-documented and widely exploited by attackers.

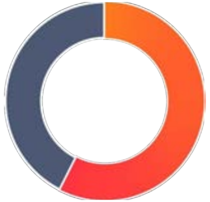
Also notable, most organizations in our dataset still have at least one asset vulnerable to Spring4Shell and Log4Shell, both zero-day vulnerabilities reported in 2022 and 2021, respectively. Additionally, nearly a third of cloud assets vulnerable to Log4Shell are public-facing, providing attackers direct access from the Internet.

Clearly, these findings signal the critical need for better patch management, especially in the context of sophisticated threat groups targeting the least path of resistance to a compromise.



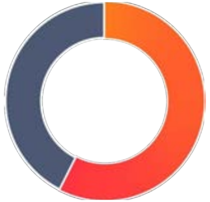
93%

of organizations have at least one vulnerability older than 10 years, **+2% YoY**.



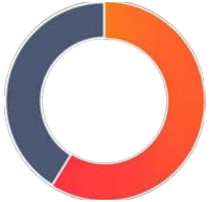
58%

of organizations have at least one vulnerability older than 20 years, **+12% YoY**.



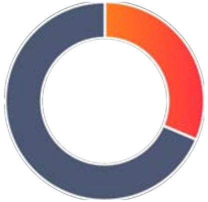
58%

of organizations have at least one asset vulnerable to Spring4Shell.



59%

of organizations have at least one asset vulnerable to Log4Shell.



32%

of cloud assets vulnerable to Log4Shell are public facing.

05

NEGLECTED ASSETS

Neglected Assets

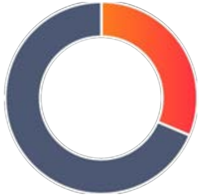
NEGLECTED BY DEFENDERS, BELOVED BY ATTACKERS

Neglected assets are a prime example of the Defender's Paradox, which says that defenders have to be right every time when securing their environments, while attackers need only to be right once when attempting to exploit it.

A neglected asset is a cloud asset that uses an unsupported operating system or has remained unpatched for 180 days or more. As applications and operating systems reach EOL, vendors stop offering support, causing security and stability to decrease over time.

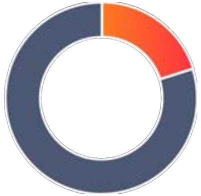
Neglected assets are a soft target for attackers, which explains why attackers commonly exploit them to gain initial access. Recall the reference to APT29 from the previous chapter. A well-documented TTP (techniques, tactics, and procedures) of the infamous threat group is to target neglected assets, which remain unmonitored and often unpatched.

Based on our analysis, **nearly a third of cloud assets are neglected (32%)**, leaving them susceptible to exploitation as they expand organizations' attack surfaces. The most neglected asset type is virtual machines (95% of organizations have at least one), while the most neglected operating system (OS) distribution is Ubuntu (88% of organizations have at least one instance). Additionally, our findings show that more than a fifth of organizations are neglecting at least 40% of their cloud assets.



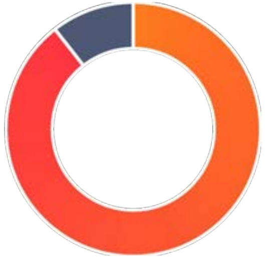
32%

of cloud assets are in a neglected state on average.



+20%

of organizations are neglecting at least 40% of their cloud assets.



89%

of organizations have at least one neglected cloud asset that is internet-facing, **+7% YoY.**

Equally troubling, our analysis finds that nearly nine in every 10 organizations have a neglected asset accessible from the Internet. These assets are often spun up for temporary use and are never secured or turned down. When publicly exposed, they become prime targets for attackers.

Industries particularly susceptible to public-facing neglected assets include:

CONSUMER & MANUFACTURING	TECHNOLOGY	PUBLIC SECTOR
97%	94%	92%

The prevalence of neglected assets has increased YoY, with nearly every organization and industry affected. This troubling trend is likely to continue as more cloud assets meet the criteria of “neglected” (i.e., unsupported OS or unpatched for a 180 days or more).

06

IDENTITY & ACCESS

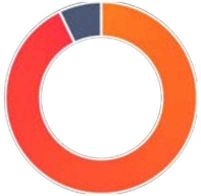
Identity & Access

6.1 LATERAL MOVEMENT

Considering the “soft targets” explored in the previous chapter, it’s important to look at other ways attackers can gain unauthorized access and move within cloud environments—and execute more ambitious, malicious, and impactful campaigns.

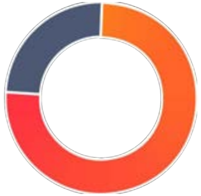
Lateral movement—when attackers leverage a cloud asset to exploit another—represents a key risk that has increased YoY. Lateral movement often allows attackers to escalate privileges, access sensitive data, and compromise high-value assets deeper in the environment.

Cloud assets that enable lateral movement are risky in their own right, yet this risk magnifies when those assets are publicly accessible.



95%

organizations have at least one cloud asset that enables lateral movement, **+5% YoY.**



76%

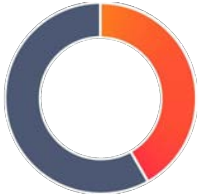
of organizations have at least one cloud asset that is public-facing and enables lateral movement, **+4% YoY.**

6.2 CLOUD FUNCTIONS

The adoption of serverless architectures, including cloud functions, continues to increase. Forrester notes growing adoption of "serverless-first" approaches, as many organizations want cloud services without the burden of Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS) deployments.

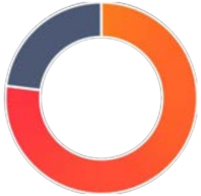
Serverless computing still presents risks, however. Cloud functions configured to allow public access can lead to unauthorized access and potential data breaches, service disruptions, or unauthorized resource consumption.

Additionally, cloud functions granted administrative privileges can perform wide-ranging actions across cloud resources. If attackers compromise the function, they can access sensitive data, further escalate privileges, and perform other malicious actions



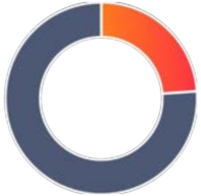
42%

of organizations have at least one Lambda function that lacks any policies restricting public access, **+12% YoY.**



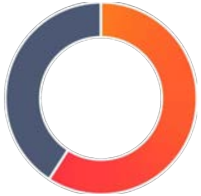
77%

of organizations have Lambda functions exposing secrets like API keys or access information.



24%

of organizations have Lambda functions with admin permissions, **+5% YoY.**



59%

of GCP functions are public and have invoker rights.

6.3 NON-HUMAN IDENTITIES

Non-human identities (NHIs) refer to digital identities assigned to machines, services, and automated processes—not human users. These can include service accounts, workload identities, cloud functions, and more. Our analysis finds that **NHIs outnumber their human counterparts by an average of 50:1.** NHIs play an important role in cloud and Kubernetes environments, powering critical applications and efficient operations by enabling digital identities to gain the cloud access and permissions they need.

Yet NHIs, when left unsecured, can dramatically increase cloud risks. This is especially true when users grant NHIs more permissions than they need. If attackers compromise the NHI, this can lead to unauthorized access, lateral movement, data loss, and other severe security incidents, whether in cloud or Kubernetes environments.

78%

of organizations have at least one IAM role that hasn't been used for 90+ days, **+6% YoY.**

77%

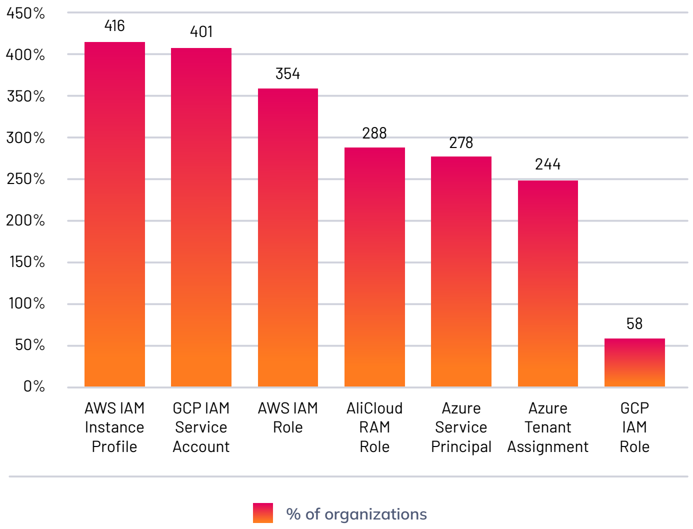
of organizations with AWS have at least one service account with permissions across two or more accounts.

12%

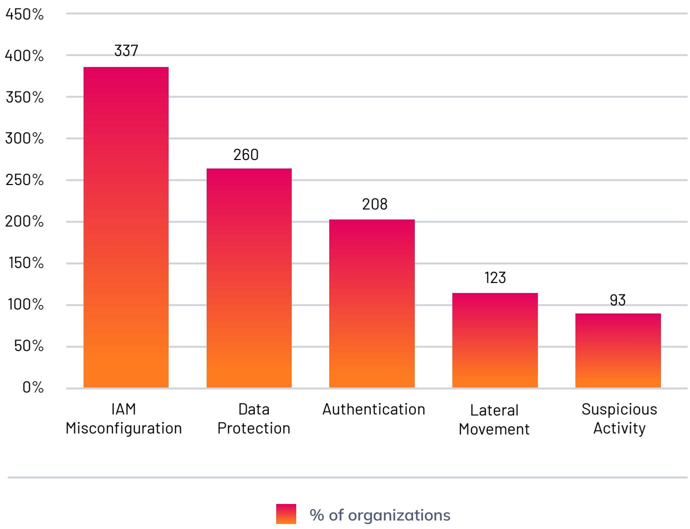
of organizations have at least one permissive role attached to more than 50 instances.

Interestingly, our analysis also uncovers the average age of NHIs by type, with several surpassing the one-year mark. We also see the average remediation days for NHI-related assets, a measure that tracks the life of specific cloud alerts from open to close. Here, we see that IAM misconfiguration alerts associated with NHIs take the longest to remediate, followed by data protection and authentication.

Average Age of NHI by Type



Average Remediation Days for NHI-related Risks

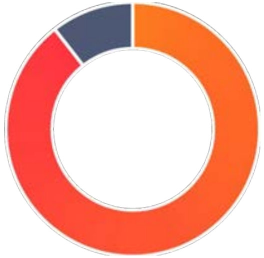


6.4 UNUSED IAM USERS

User credentials are considered unused if they remain active but unused for more than 90 days. While seemingly harmless, it can dramatically increase the attack surface and provide attackers opportunities for unauthorized or backdoor access, lateral movement, and more.

This year's findings, compared to last year's, show a moderate, yet notable increase in unused user credentials. This occurs when access keys or passwords associated with an IAM user remain active despite not being used in over three months. Stale user credentials increase the attack surface. If compromised, they may provide silent backdoor access—especially if not closely monitored.

Organizations should implement automated inactivity detection for unused users, enforce credential rotation policies, and disable or delete unused credentials after a defined threshold (e.g., 60–90 days).



89%

of organizations have IAM user credentials that haven't been used for 90+ days, **+7% YoY.**

07

APPLICATION SECURITY

Application Security

7.1 SECRETS EXPOSURE

According to Verizon Data Breach Investigation Report, stolen credentials is the top cause of data breaches for cloud-native applications, contributing to nearly nine out of every 10. Secrets encompass more than just user credentials (e.g., OAuth tokens, access keys), and attackers often find and exploit them via code repositories. In fact, past studies by our researchers found that attackers can find and steal exposed secrets from GitHub in two minutes. That's far less than the median time of 94 days it takes to remediate leaked secrets on a GitHub repository, according to Verizon's findings.

This all underscores the importance of scanning code repositories for exposed secrets. Secrets detection can help organizations find and remediate exposed secrets before code is built and shipped to production environments.

85%

of organizations have plaintext secrets embedded in their source code repositories.

If the repository is exposed (public or breached), attackers can extract these secrets and use them to access systems, exfiltrate data, or escalate privileges.

36%

of these plaintext secrets are active and stored in the current main branch.

Active secrets in the main branch are immediately usable by attackers, enabling real-time exploitation such as unauthorized API calls, infrastructure access, or data theft.

58%

of these plaintext secrets are saved in Git history, with 14% of those secrets still valid.

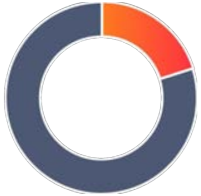
Even if removed from the latest code, secrets in Git history can be easily discovered using public tools. If just a small percentage remain valid, attackers can still exploit them to compromise systems, access data, or pivot deeper into infrastructure.

7.2 MISCONFIGURATIONS - IAC

Infrastructure-as-Code (IaC) misconfigurations are a common and critical source of production risks. A simple misconfiguration in one IaC artifact, when reused for multiple projects, can quickly propagate into hundreds or thousands of risks in runtime. A recent survey by the Enterprise Strategy Group found that two-thirds of organizations report an increase in IaC misconfigurations.

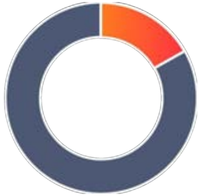
Our analysis identified a variety of IaC misconfigurations. Among them, we find that **one-fifth of organizations have created an IaC misconfiguration that allows cross-account access for an IAM role without requiring MFA or an external ID**. This can lead to unauthorized access; third parties need only to guess the correct Amazon Resource Name (ARN) to assume the cross-account role. Additionally, we find that **17% of organizations have at least one IaC artifact that configures S3 storage buckets to grant GET (read) access to anyone on the Internet**. This can expose sensitive data and result in data breaches, compliance violations, and other severe security incidents.

We also uncovered the popularity of IaC artifacts by type, with most organizations using Dockerfile (74%), Terraform (65%), Docker Compose (63%), and Kubernetes Manifest (47%).



20%

of organizations have created an IaC misconfiguration that allows Cross-Account Access for IAM Role Without External ID or MFA.



17%

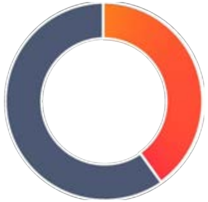
organizations have a IaC artifact that configures S3 buckets to grant public GET.

7.2 MISCONFIGURATIONS - SCM

Source Code Management (SCM) platforms such as GitHub and GitLab are crucial technologies for developers, giving them a collaborative solution to centrally store, manage, and track changes to source code. Despite their advantages for development, SCM solutions present significant security risks if not properly configured at the organization, account, and repository levels.

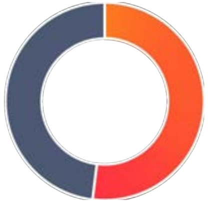
Our analysis identified numerous high-severity misconfigurations. Among them, four in every ten organizations have a GitHub Actions configuration that allows workflows to approve pull requests, enabling attackers to bypass code reviews and inject malicious code into the software supply chain and ultimately into production. More than half of SCMs at the organizational level are not configured to create a Git Ignore file for each new repository, allowing developers to commit secrets, configuration files containing sensitive data, and local system files that shouldn't be a part of a repository.

SCM Posture Management (SCM-PM) capabilities enable organizations to detect and remediate misconfigurations and security risks across their SCM organizations, accounts, and repositories.



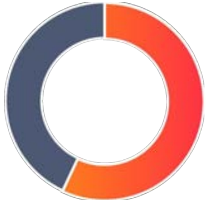
40%

of organizations have GitHub Actions configured to allow workflows to approve pull requests.



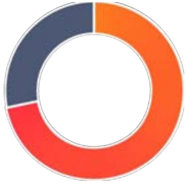
52%

of organizations have a configuration that does not create a Git Ignore File (.gitignore) for each repository.



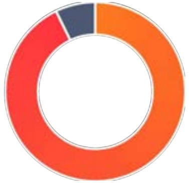
57%

of organizations have an organization configuration that does not restrict default repository member permissions.



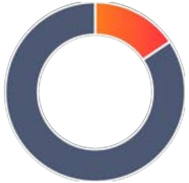
72%

of organizations have at least one package with a severe vulnerability (CVSS > 7) in a code repository, **+10% YoY.**



97%

of organizations have at least one vulnerable package in a code repository that is fixable.



16%

of all vulnerable packages detected have a CVE with a CVSS score of 9 or greater. Of these CVEs, **95% are fixable.**

7.3 VULNERABILITIES

Vulnerabilities often find their way into the software development lifecycle (SDLC) through open-source and third-party software components, as well as risks introduced into first-party codebases. According to our analysis, more than seven in every 10 organizations have severe vulnerabilities in code repositories such as GitHub, GitLab, Azure DevOps, or Bitbucket.

This represents a notable increase YoY and highlights a persistent problem for organizations. If severe vulnerabilities make it to production environments and become reachable by attackers, they can result in severe security incidents, including data breaches.

Notably, the industries most affected by severe vulnerabilities in code repositories include:

RETAIL	CONSUMER & MANUFACTURING	TECHNOLOGY
79%	67%	59%

08

KUBERNETES

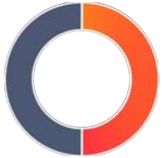
Kubernetes

KUBERNETES USAGE AND RISKS

Kubernetes (K8) plays a critical role in cloud environments because it provides the orchestration needed to deploy, scale, and manage containerized applications reliably and efficiently. It simplifies the complexity of managing infrastructure, enabling organizations to run applications consistently across cloud providers, environments, and regions—making it foundational to cloud-native development and multi-cloud strategies.

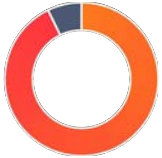
Importantly, our analysis shows that most organizations use Kubernetes in their cloud environments **(70%),** with adoption increasing significantly YoY **(15%)**. Of organizations using Kubernetes, nearly a third **(30%)** have at least one Kubernetes asset (e.g., workload, identity, configuration) that is publicly exposed. Like other cloud assets, public exposure increases the risk of unauthorized access and related security incidents.

Besides Kubernetes adoption, we also see a significant share of organizations with Kubernetes risks. One in every two K8 organizations have at least one cluster with an unsupported version of Kubernetes installed, leaving the cluster vulnerable to known exploits. Additionally, **93% of K8 organizations have an overprivileged service account**, which attackers can exploit to escalate privileges, access sensitive data, or disrupt the cluster.



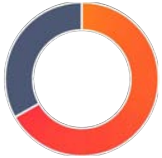
50%

of organizations have at least one cluster with an unsupported version of K8 installed.



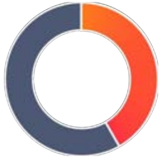
93%

of organizations have an overprivileged K8 service account.



67%

of organizations have at least one unused K8 service account.



42%

of organizations using K8s have a controller of pods with admin-like permissions, **+8% YoY**.

09

KEY RECOMMENDATIONS

Key Recommendations

Secure AI While Leveraging It to Enhance Cloud Security

Protect your environment from AI-related risks by securing models, packages, and data according to cloud security best practices. At the same time, use AI to improve security outcomes—enhancing risk discovery, remediation, least privilege enforcement, and more.

Protect High-value Assets

Secure high-value assets by prioritizing the attack paths that endanger them. Continually scan and monitor your entire cloud, identify your crown jewels, and analyze risk in context. Ensure real-time monitoring, detection, and protection for sensitive assets against sophisticated threats, such as exploits in memory—without compromising scalability or performance.

Protect Your Sensitive Data

Identify all the places your sensitive data lives in your cloud estate. Once discovered, take proper measures to secure data and ensure it meets compliance requirements. Continually monitor sensitive data for suspicious activity and quickly investigate and triage potential threats.

Prevent Workload Neglect

Maintain an up-to-date inventory of cloud workloads and continuously monitor for abandoned or compromised assets. Deploy only supported applications and operating systems with active vendor updates. Enforce security benchmarks for all configurations before deployment, and oversee infrastructure as code (IaC) to prevent unmanaged workloads.

Prioritize Patching

Patch strategically by focusing on vulnerabilities that attackers can actually reach and exploit in runtime, recognizing that not all vulnerable packages are used in production. This calls for performing Reachability Analysis on a continuous basis and prioritizing remediation efforts accordingly.

Enforce the Principle of Least Privilege (PoLP)

Grant users and NHIs only the minimum permissions needed, and scope roles tightly to specific resources and functions. Use automation and AI-driven IAM capabilities to streamline policy creation, monitor access, and enforce least privilege. Leverage Just-in-Time (JIT) Access to further optimize and secure permissions.

Unify Security Before Deployment and During Runtime

Implement pre-deployment security measures to detect issues in the development pipeline and ensure these capabilities integrate with your runtime measures. Ensure full pipeline visibility, enforce security policies to block risks before production, and trace and remediate issues from production alerts to code artifacts.

Perform Regular Audits and Leverage Continuous Monitoring

Conduct regular audits to enforce security policies and prevent misconfigurations. Continuously monitor access logs and set alerts for unusual activity to quickly detect and respond to potential threats.

About Orca Security

Orca enables organizations to make cloud security a strategic advantage. With the most comprehensive coverage and visibility across multi-cloud environments, the agentless-first Orca Platform unites teams to eliminate complexities, vulnerabilities and risks.

Backed by Temasek, CapitalG, ICONIQ Capital, Redpoint Ventures and others, Orca is trusted by hundreds of organizations, including SAP, Gannett, Autodesk, Unity, Lemonade and Digital Turbine.

To find out more,
schedule a personalized demo

> “Combining real-world insights compiled by the Orca Research Pod, [this report] offers practical guidance on where to focus, what to prioritize, and how to effectively secure multi-cloud environments in the age of AI.”

GIL GERON
CEO and Co-Founder of Orca Security