tenable | Report

Tenable Cloud Risk Report 2024

Identifying blind spots, searching for context and addressing the toxic cloud trilogy

Table of contents

Introduction

Cyber exposures are business risks — wielding the power to cause liability, loss and irreparable harm. Scattered products, isolated views and disjointed teams make it difficult for organizations to hold back threats across the attack surface and identify novel blind spots. Addressing cyber exposure is particularly challenging when it comes to managing the risks inherent in the cloud. Security gaps caused by misconfigurations, risky entitlements and vulnerabilities have become the epicenter of cloud risk.

But cloud security is not a one-size-fits-all endeavor. The unique cloud environment of each organization, along with the types of data being stored, should dictate the approach used to secure cloud instances. The challenge for most organizations is having the holistic visibility needed to create context around their risk to make the best decisions about remediating vulnerabilities — and removing over-privileged access to cloud resources.

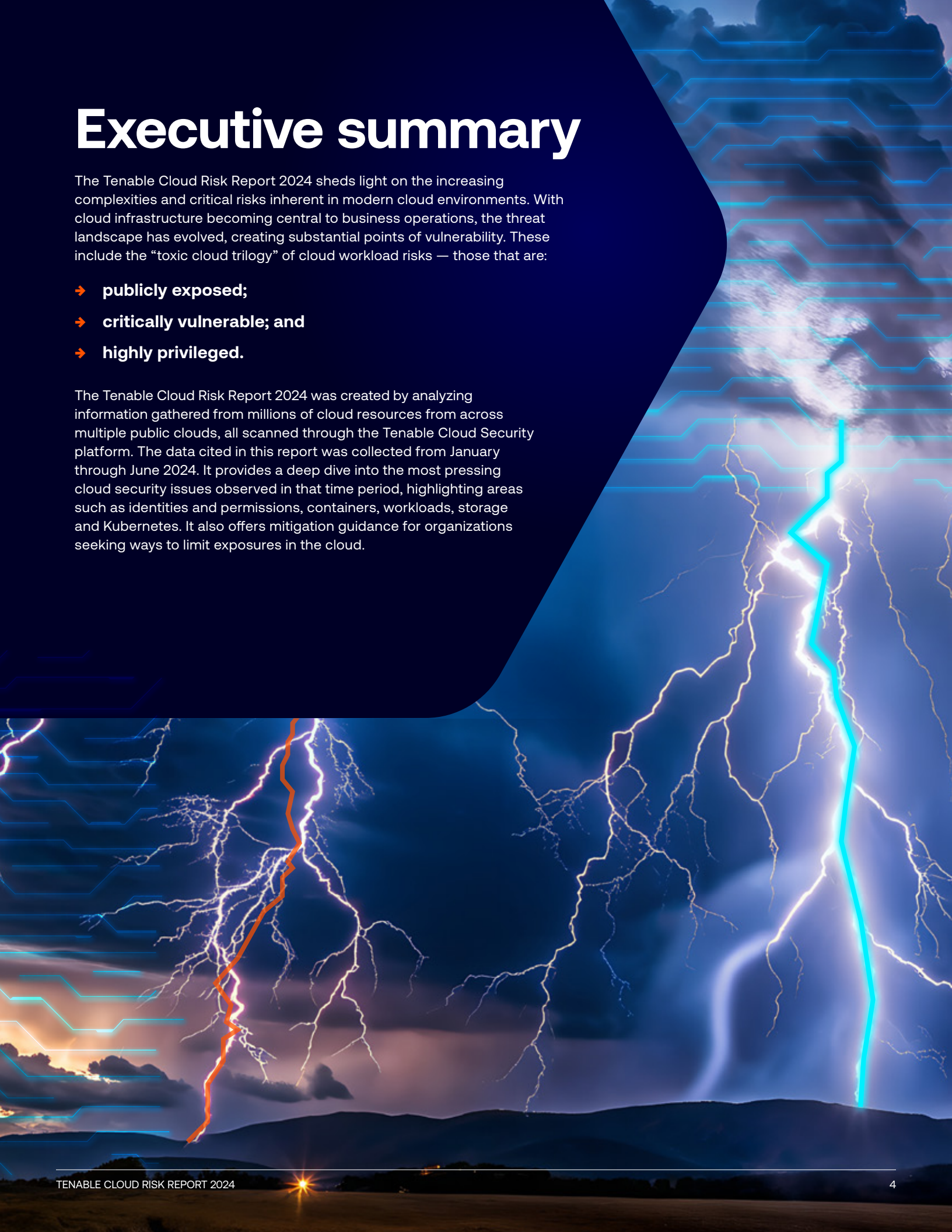
Tenable Research closely monitors cloud-based risks and delves into new trends and attack techniques as the threat landscape shifts over time, to provide customers with valuable warning signs to look for when managing their environments. This report reflects findings by our cloud researchers based on analysis of Tenable telemetry collected from January through June 2024.

Executive summary

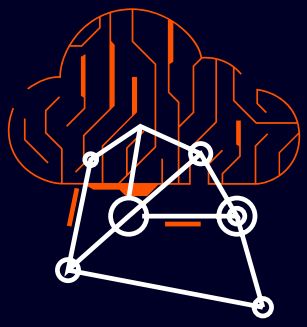
The Tenable Cloud Risk Report 2024 sheds light on the increasing complexities and critical risks inherent in modern cloud environments. With cloud infrastructure becoming central to business operations, the threat landscape has evolved, creating substantial points of vulnerability. These include the “toxic cloud trilogy” of cloud workload risks — those that are:

- **publicly exposed;**
- **critically vulnerable; and**
- **highly privileged.**

The Tenable Cloud Risk Report 2024 was created by analyzing information gathered from millions of cloud resources from across multiple public clouds, all scanned through the Tenable Cloud Security platform. The data cited in this report was collected from January through June 2024. It provides a deep dive into the most pressing cloud security issues observed in that time period, highlighting areas such as identities and permissions, containers, workloads, storage and Kubernetes. It also offers mitigation guidance for organizations seeking ways to limit exposures in the cloud.



Key findings



38% of organizations have high risk workloads

Critical exposure of cloud workloads

The report reveals that 38% of organizations have at least one cloud workload that is publicly exposed, critically vulnerable and highly privileged. This “toxic cloud trilogy” creates a high risk attack path that makes these workloads prime targets for bad actors.

84% of organizations have risky access keys

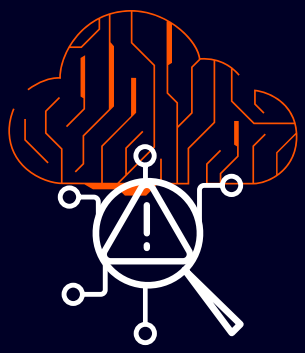
IAM and credential risks

The majority of organizations (84.2%) possess unused or longstanding access keys with critical or high severity excessive permissions, a significant security gap that poses substantial risks. Risky access keys have played major roles in numerous identity-based attacks and compromises.

23% of cloud identities have critical or high severity excessive permissions

Prevalence of excessive permissions

Analysis of Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure reveals that 23% of cloud identities, both human and non-human, have critical or high severity excessive permissions — and that in AWS alone, 35% of human identities have critical permissions. Overprivileged identities contribute significantly to breaches and compromises.



80% of workloads had an unremediated critical CVE

Unmanaged cloud vulnerabilities

Critical vulnerabilities persist: Notably, CVE-2024-21626, a severe container escape vulnerability, remained unremediated in over 80% of workloads even 40 days after its publishing. Other critical vulnerabilities, such as CVE-2024-21338 (Windows kernel), were found prevalent and requiring urgent attention.

What are access keys?

Access keys are credentials, typically longstanding, that organizations use to grant programmatic access to resources in their cloud environment. Some cloud providers discourage their use — and good alternatives are available.

74% of organizations have publicly exposed storage

Cloud storage risks

A significant 74% of organizations have publicly exposed storage assets, including those in which sensitive data resides. This exposure, often due to unnecessary and/or excessive permissions, has been linked to increased ransomware attacks. Visibility and insight into data stored in the cloud is key to contextualizing and prioritizing cloud risk — and knowing when public exposure is not benign.

78% of organizations have publicly accessible Kubernetes API servers

Kubernetes security challenges

A troubling 78% of organizations have publicly accessible Kubernetes API servers, 41% of which allow inbound internet access. Additionally, 58% of organizations have cluster-admin role bindings — which means that certain users have unrestricted control over all the Kubernetes environments — and 44% run containers in privileged mode; both these permissions configurations amplify security risks.

Let's take a deeper look at each of the key findings.

Critical exposure of cloud workloads

Many of the breaches reported worldwide in 2024 were the result of one-day vulnerabilities exploited on exposed workloads. Of these, some of the most dangerous breaches involved lateral movement through use of the privileges of the compromised workloads.

Securing cloud workloads is about much more than scanning for vulnerabilities. Assessing a workload's risk level and potential vulnerability impact requires taking into account three major attack vectors:

- **Is the machine accessible via the network?**
  Machines with public IP exposure are more likely to be targeted.
- **Does the machine have critical vulnerabilities?**
  Machines with vulnerabilities can be compromised by attackers.
- **Is the machine's attached identity highly privileged?**
  Highly privileged machines, if compromised, have a much greater potential effect on the organization than those with fewer privileges.

Of course, context is key in these instances, and a data security posture management (DSPM) solution can help identify the level of sensitivity around the data in these workloads. But a workload that is highly privileged, publicly exposed and has critical vulnerabilities creates a "toxic cloud trilogy" of combined risk that makes an especially compelling attack path for bad actors. How many workloads with a trilogy of toxic combinations do organizations typically have?

Percentage of organizations (AWS/GCP) with vulnerable exposed privileged instances

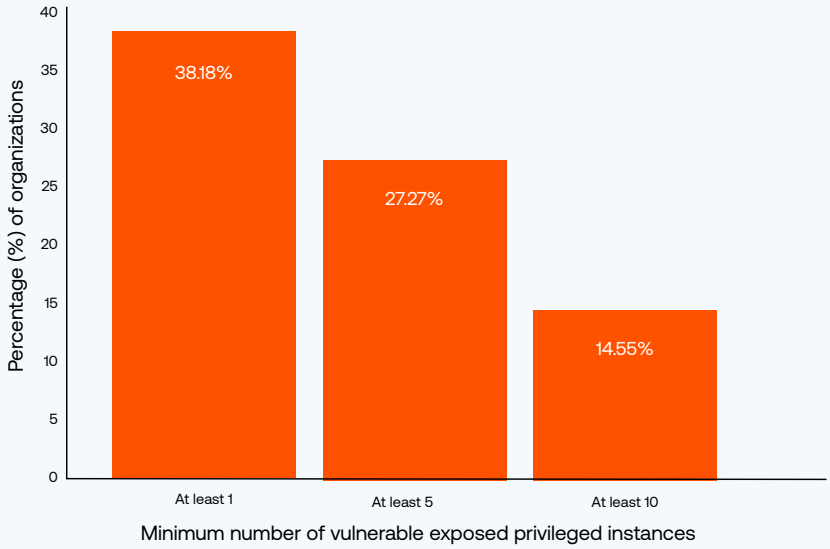


Figure — 38% of organizations had at least one workload in AWS or GCP environments with the toxic cloud trilogy of a critical vulnerability, public exposure and highly privileged permissions; many organizations had multiple workloads with such toxic trilogies (Microsoft Azure workloads were not included in this analysis)

38% of organizations have at least one workload that is publicly exposed, critically vulnerable and highly privileged — the toxic cloud trilogy.

What is the implication of 38% of organizations having workloads with a toxic cloud trilogy? Without being too dramatic, it means more than one-third of organizations could potentially land in tomorrow's headlines. The irony is, so much of this kind of risk is preventable. Toxic combinations involving even one or two risk factors have enormous security implications for an organization — let alone three.

When looking at the sources of toxic cloud trilogies across all workloads and cloud providers, we found excessive permissions surfaced as the greatest offender, with 50% of all workloads overprivileged. This aggregated view includes data from AWS, Microsoft Azure and GCP environments.

But do not let the lower numbers in the chart suggest small risk! Production workloads across the board are at much risk, with 30% suffering vulnerabilities, 16% inflicted with CVEs combined with excessive privileges and 1% bearing the burden of a toxic cloud trilogy. What dangers lie in 1%? Recall that a toxic combination is tantamount to a path leading a bad actor to high-value resources.

A major challenge in cloud protection is understanding which security gaps to prioritize for remediation — making insight into toxic combinations essential. A CVE, even one flagged as critical, doesn't necessarily convey a workload's risk level; the absence of fuller risk insight can lead to control gaps or time spent unnecessarily by security teams addressing low-risk findings.

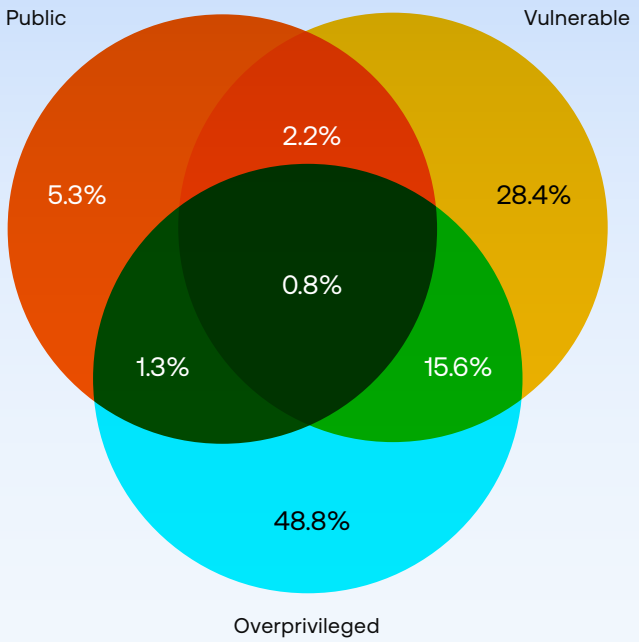


Figure — Aggregated findings (in percentages %) across the cloud providers observed show workloads are plagued by over-privilege, vulnerabilities, and toxic duos and trilogies

IAM and credentials in danger

It's well understood today that identity is the cloud's perimeter, making identity and access management key to reining in cloud risk. Indeed, a plethora of identity-based attacks have made recent headlines, including:

- MGM Resorts — An Okta social engineering breach involved lateral movement to Microsoft Azure as part of the larger cyberattack by the BlackCat/ALPHV ransomware group
- Microsoft — Midnight Blizzard a Russian state-sponsored actor also known as NOBELIUM, hacked the tech giant's corporate email systems
- Scattered Spider — Continued attacks by these threat actors, which use dedicated attack tools for cloud environments to gain initial access, and leverage BlackCat/ALPHV ransomware alongside their usual tactics, techniques and procedures (TTPs)
- Fbot — Python-based malware that targets web servers, cloud services and software-as-a-service, and achieves persistency and propagates on AWS via AWS IAM users

Core to IAM risks are access keys and their assigned permissions; combined, they are literally the keys to the kingdom of cloud-stored data.

84% of organizations have unused or longstanding access keys with critical or high severity excessive permissions.

How we define permissions severity

The permissions severity levels (critical, high, medium or low) referred to in this report are as assessed by the Tenable Cloud Security platform. The solution derives the risk severity level for each permission in a manner specific to the logic of each cloud provider. It calculates permissions severity based on a combination of parameters, including the category of the actions within the permission, such as data access, privilege escalation or infrastructure modifications, in conjunction with other factors such as credentials, exposure, sensitivity, multi-factor authentication (MFA) configuration and more.

Identities and permanent credentials risk

Credential compromise is one of the most known attack vectors in cloud environments — yet the risk continues to plague organizations. Breaches involving stolen or compromised credentials take the most time — a whopping 292 days[1] — to identify and contain, making preempting such risk essential.

Credentials are the authentication and authorization data used by organizations to grant identities, such AWS IAM users or GCP service accounts, access to their cloud resources. Credentials can take various forms; they are often access keys, which can be long-lasting or temporary in duration. Assigned access keys typically remain valid until rotated or permissions expire. Security best practice calls for avoiding the use of longstanding access keys yet their use prevails — likely in the name of speedy development.

Given the significant — and entirely avoidable — associated risk, we chose to analyze active and unrotated keys. Strikingly, we found that 43% of all AWS IAM users have excessive permissions on unused keys, and 26% of all GCP users have excessive permissions on unrotated keys, in the cloud environments observed.

Specifically, the research reveals that 16% of AWS IAM users and 12% of GCP service account users have access keys of critical or high permissions severity that are inactive — a security gap perhaps somewhat understandable as organizations may not have tools for accurately identifying inactive use. We also found a notable incidence of similarly high risk unrotated access keys — 16% of GCP accounts and 12% of AWS IAM. Such lack of rotation is counter to security best practices.

AWS IAM user key risks - by excessive permissions severity

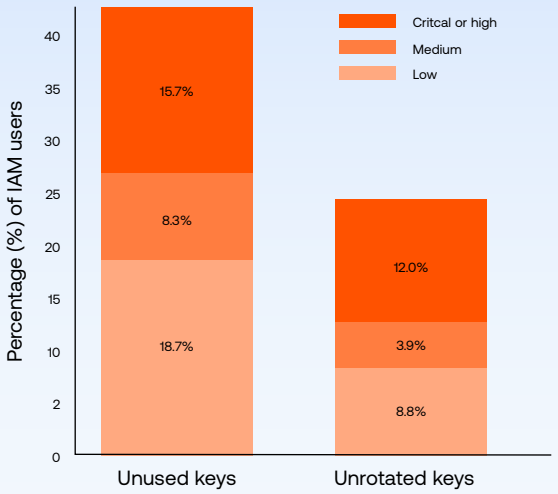


Figure — Among AWS IAM users, 16% have critical or high severity excessive permissions attached to access keys they are not using and 12% to access keys not being rotated

GCP service account access key risks - by excessive permissions severity

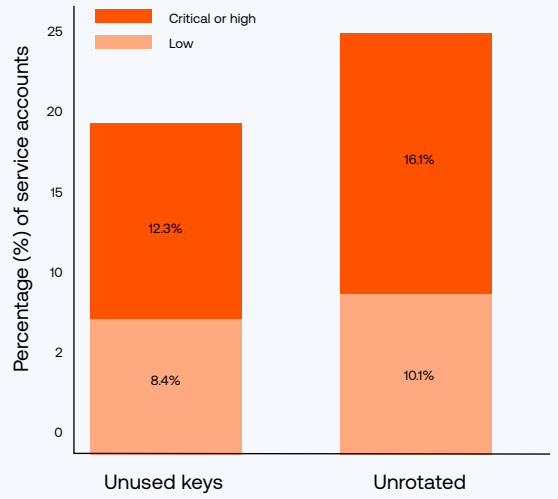


Figure — Among GCP service accounts, 12% have critical or high severity excessive permissions attached to access keys they are not using and 16% to access keys not being rotated

[1] Cost of a Data Breach Report 2024, published by IBM, based on research by Ponemon Institute, July 30, 2024

Our research found that more than eight in 10 organizations (84%) possess unused or longstanding access keys with critical or high risk permissions — a significant security issue. The persistence of these keys, especially with high privileges, is a known, reported, major factor in numerous identity-based attacks and compromises.

According to the shared responsibility model, the organization is responsible for key rotation. Cloud providers advise adhering to a timely credential rotation schedule — security best practice calls for a cadence of every three months — and removing unused keys, especially highly privileged ones. Organizations can also reduce risk by using Just-in-Time access mechanisms to enforce time-bound permissions and automated removal upon expiration.

Percentage of organizations with critical/high risk unused and/or unrotated keys

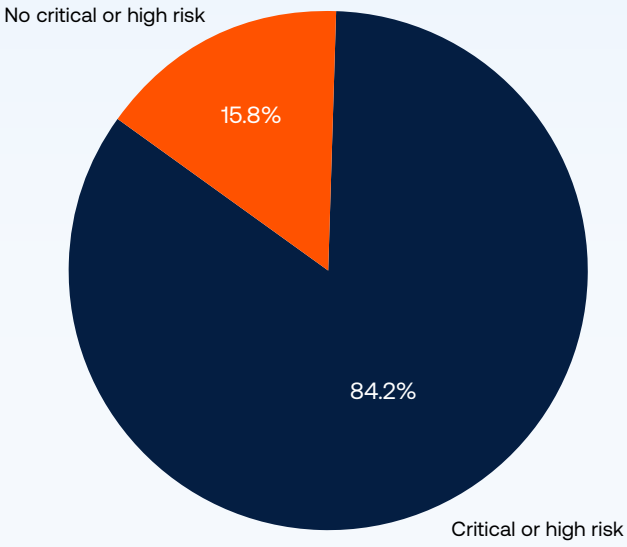


Figure — The vast majority of organizations, 84%, have critical or high-risk unused and/or unrotated keys

Excessive permissions in human and non-human identities

As noted, identities and permissions are among the cloud's greatest risks and among the greatest sources of frustration for cloud security professionals, who find themselves hampered by visibility and entitlements management issues[2].

Our research revealed extensive instances of — and issues with — excessive permissions in both human and non-human identities. Overprivileged human identities are the key impact factor in identity-based attacks (Okta, Scattered Spider). Overprivileged non-human identities are the key impact factor in breaches based on application vulnerabilities, such as the 2024 Cloudflare breach. While they differ, these risks are ultimately part of the same IAM system.

Permissions severity of human and non-human identities — AWS

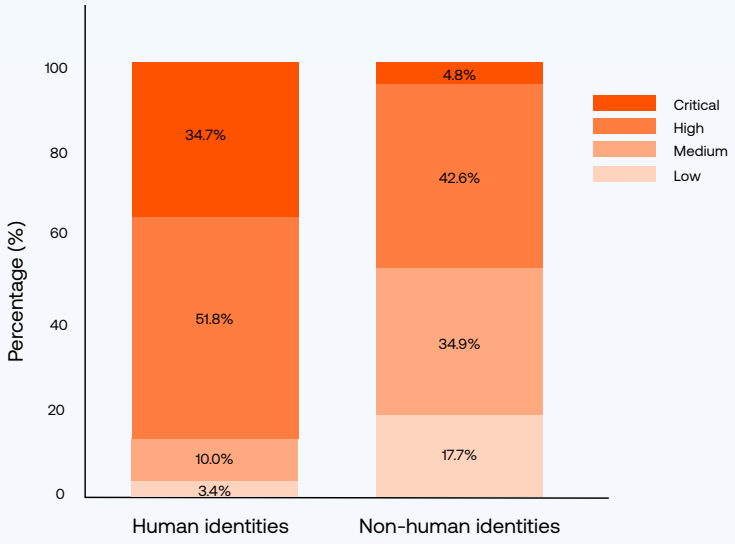


Figure — A significantly higher percentage of critical permissions in AWS are granted to human identities (35%) than non-human identities (5%) — and a stunningly high percentage of critical or high permissions, combined, are granted to human identities (87%)

When examining human and non-human identities in AWS, GCP and Microsoft Azure environments, we found that 23% have critical or high severity excessive permissions.

When looking specifically at AWS environments, we found permissions of considerably high risk among human identities: 87% have critical or high severity excessive permissions, and 35% have critical severity excessive permissions.

[2] Cloud Security Outlook 2024, Tenable

AWS IAM role risks — excessive permissions of human and non-human identities

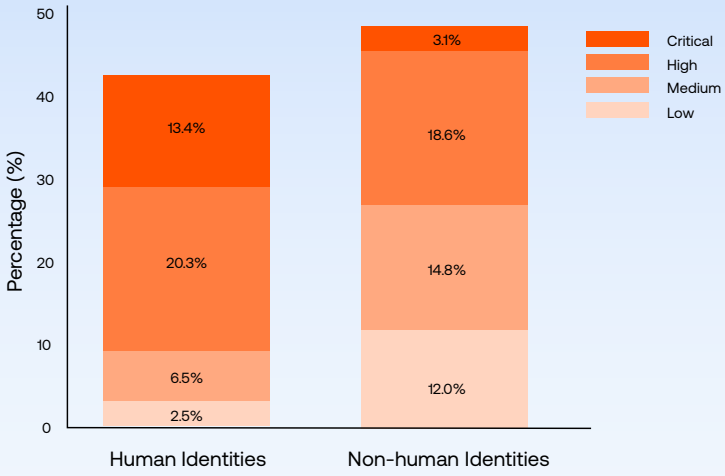


Figure — A significantly higher percentage of critical or high severity excessive permissions in AWS are granted to human identities (34%) than non-human identities (22%)

Our findings also showed that human identities are more commonly granted administrator privileges than non-human identities. This distinction may reflect developer use of programmatic templates with pre-scoped permissions for IAM roles to define access for non-human identities. It may also indicate increased awareness, with teams outside of security moving toward least privilege access.

The complexity of cloud-native architectures, with tens of thousands of permissions, policies and roles, creates huge difficulties for organizations. It forces them to determine which permissions have been granted, detect when they are excessive and their potential risk exposure — and understand the least privilege access actually needed to get the job done. By performing deep risk analysis — that relates to each cloud infrastructure and its respective permissions model — on millions of real-world cloud assets, we were able to surface and pinpoint permissions excess and severity level.

Unmanaged cloud vulnerabilities

Cloud vulnerabilities are weaknesses or flaws in software that an organization has installed in its cloud environment that attackers can exploit to gain unauthorized access, steal sensitive data or disrupt services. These vulnerabilities represent significant risk factors in cloud infrastructure. Despite this, organizations often struggle to prioritize and manage cloud vulnerabilities effectively. Addressing vulnerabilities is crucial for maintaining the security and integrity of cloud environments.

We identified top cloud vulnerabilities by factoring in three parameters:

- **Severity**: A vulnerability's Tenable Vulnerability Priority Rating (VPR) score, which is a dynamic companion to the data provided by the vulnerability's CVSS score. VPR scoring values range from 0.1-10.0, with a higher value representing a greater likelihood of exploit.
- **Ubiquity**: The commonness of a vulnerability in the cloud environments we observed.
- **Likelihood of exploitation**: The existence of a publicly available PoC reporting exploitation of a vulnerability, as observed in the wild.

Severe vulnerabilities remain prevalent and unremediated, including one that appears in 80% of workloads, in the cloud environments observed.

Risk trends of the top cloud vulnerabilities

Applying the parameters described above, we identified the four most critical cloud vulnerabilities:

CVE ID	VPR SCORE	DESCRIPTION
CVE-2024-21626	10	Vulnerability in runc where a file descriptor leak allows container escapes and host filesystem access
CVE-2024-21338	9	Windows kernel elevation of privilege vulnerability
CVE-2024-21412	8.8	Internet Shortcut files security feature bypass vulnerability
CVE-2024-21339	8.4	Windows kernel elevation of privilege vulnerability

We provide here the findings and details for the top two critical vulnerabilities:

CVE-2024-21626 — Container escape in runc

CVE-2024-21626, which has a VPR score of 10 and a PoC on Github, was found in more than 200,000 workloads in the cloud environments observed — and was still unremediated in more than 80% of them 40 days after publishing. (It is possible that, in environments in which the vulnerability could not be exploited, the decision to not remediate was intentional.)

Description: runc is a CLI tool for spawning and running containers on Linux according to the OCI specification. In runc 1.1.11 and earlier, due to an internal file descriptor leak, an attacker could cause a newly spawned container process to have a working directory in the host filesystem namespace, allowing for a container escape by giving access to the host filesystem. The same attack could be used by a malicious image to allow a container process to gain access to the host filesystem through runc run.

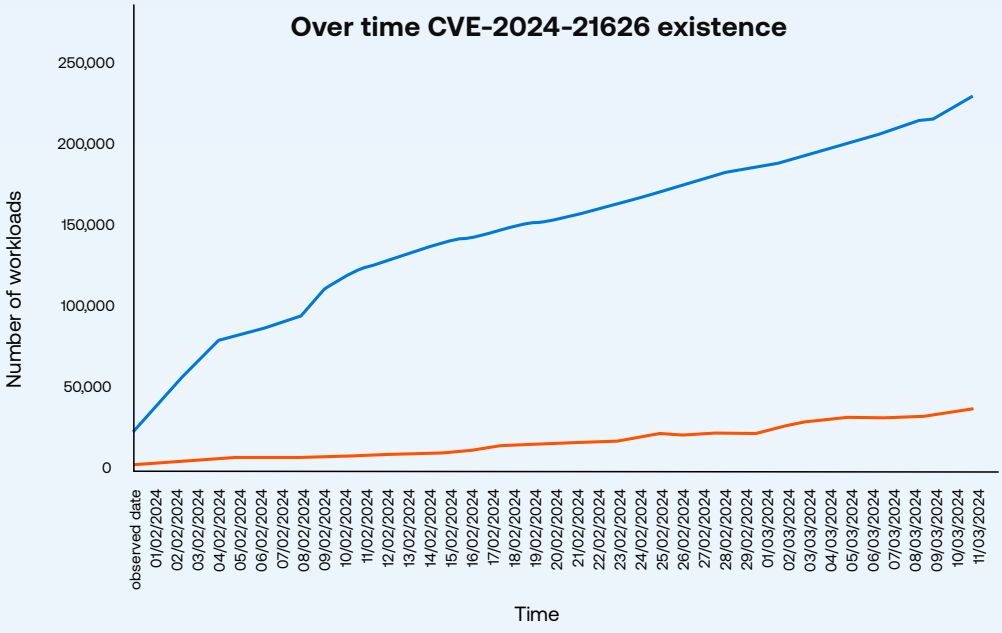


Figure — CVE-2024-21626, a top critical vulnerability affecting a CLI tool, was found in more than 200,000 workloads — and unremediated in more than 80% of them (February 1 to March 11, 2024)

CVE-2024-21338 — Windows kernel elevation of privilege vulnerability

CVE-2024-21338, which has a VPR score of 9, was found in slightly fewer than 300,000 workloads in the cloud environments observed — and was still unremediated one month after publishing.

Description: Windows kernel elevation of privilege vulnerability, with insufficient access control. The vulnerability was discovered in an in-the-wild, admin-to-kernel exploit for a zero-day vulnerability in the appid.sys AppLocker driver. The exploitation activity was orchestrated by the North Korea-based Lazarus Group, with the end goal of establishing a kernel read/write primitive.

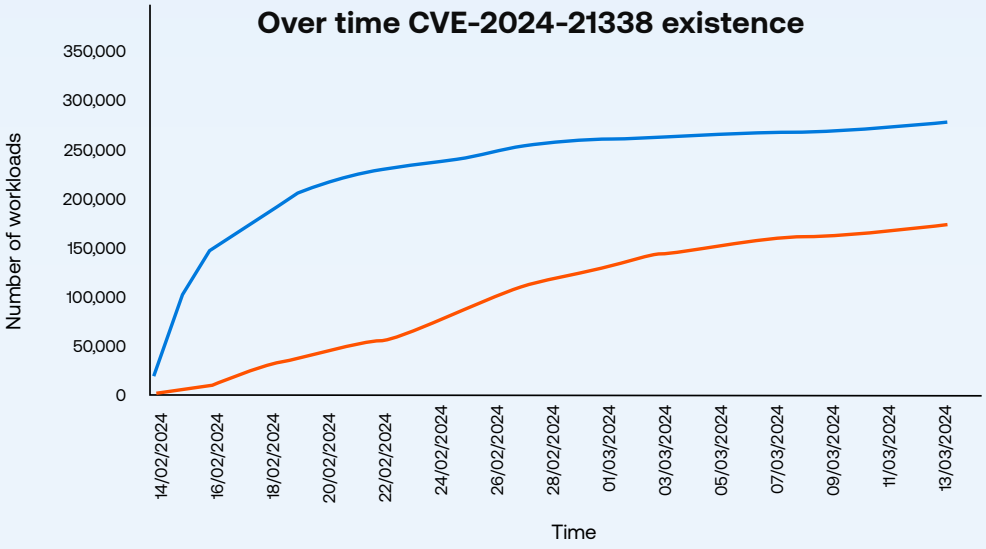


Figure — CVE-2024-21338, a top critical vulnerability involving Windows kernel privilege elevation with insufficient access control, was found in slightly fewer than 300,000 workloads (February 14 to March 13, 2024)

Vulnerability fatigue can — and must — be overcome. A list of CVEs floods the senses and wits but doesn't serve to inform risk-based decision making. An examined, contextual approach to vulnerabilities helps surface the vulnerabilities that matter the most. It's worth mentioning that vulnerability scanning that bridges between public, private and hybrid cloud environments adds context for accurately determining and unifying management of the most critical vulnerabilities in need of attention.

Cloud storage at risk

It's a basic cloud fact: As organizations ramp up their use of cloud-native applications so, too, does the amount of sensitive data they store there increase — including customer and employee information and business IP. Hackers are motivated to get at such cloud-stored data.

The first half of 2024, the period of our research, coincided with many public reports of ransomware attacks targeting cloud storage. Public cloud storage assets were the most accessible targets reported, particularly those with excessive access privileges. Much of the exposure facilitating these breaches was unnecessary and could have been prevented.

74% of organizations have publicly exposed storage assets.

Public assets

Public assets are entities in the cloud environment that are exposed to external networks so they can be accessed outside the organization. Examples include databases, web applications and websites, email servers and other online services. A public asset is not a misconfiguration unto itself, as some assets are intentionally and legitimately exposed.

Examining which assets are public shines a light on the typical perimeter of a cloud-based environment. Also, the stakes are high — almost every organization with public assets is at risk if an asset is configured as external when it shouldn't be.

To secure their cloud, it is imperative that organizations examine whether an asset truly needs to be public and, if so, that they downgrade the permissions to the minimum necessary and carry out timely patches.

96% of organizations have public cloud assets.

Top 10 public facing assets — % of organizations

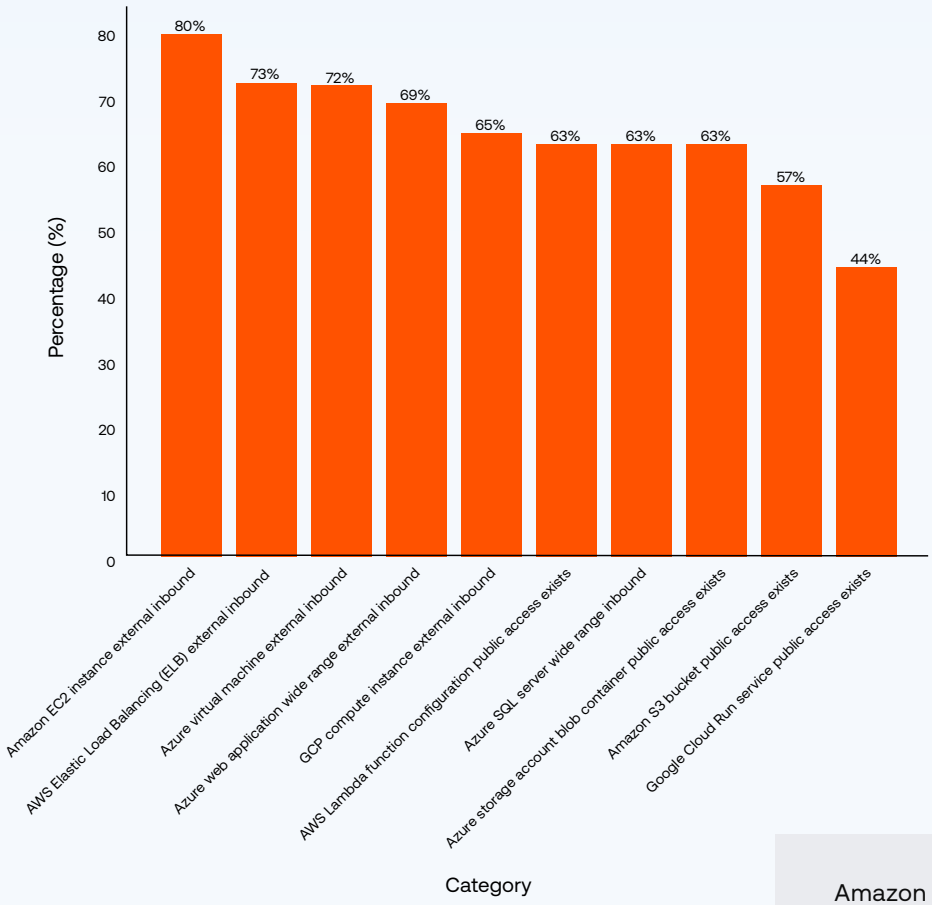
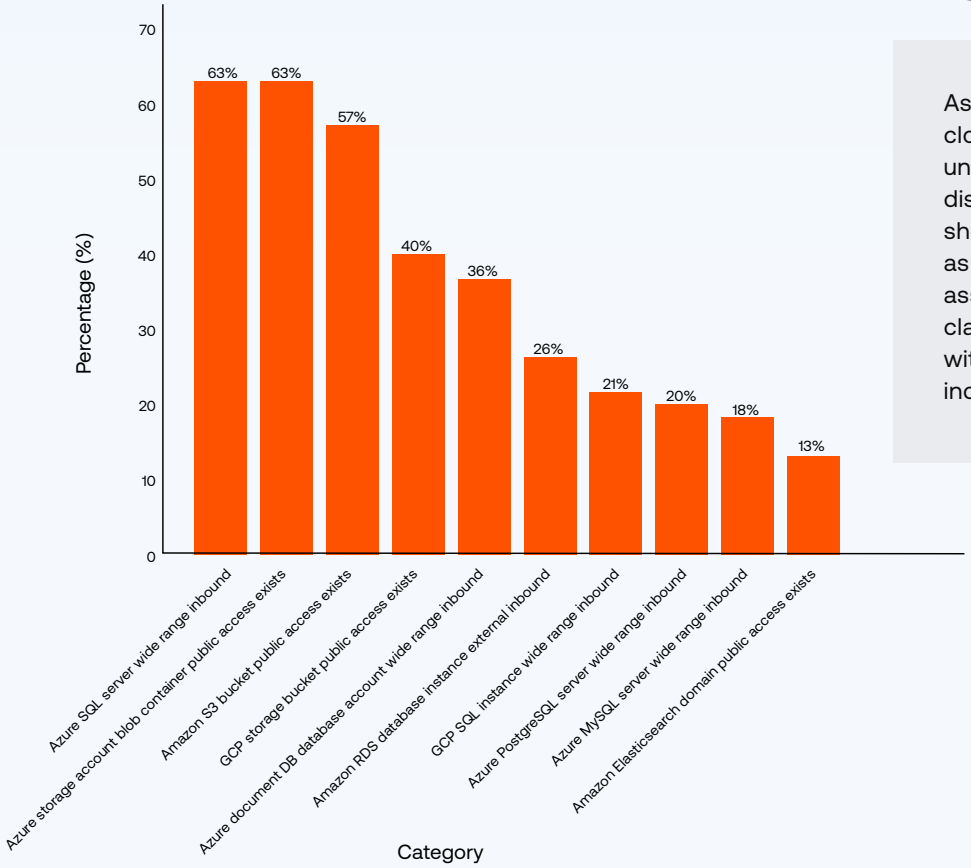


Figure — Top 10 public cloud assets of organizations across cloud providers, with externally facing Amazon EC2 instances open to internal traffic leading the pack at 80%

Amazon EC2 is the most commonly used cloud service so it is not surprising that such instances are the most public facing by far.

Top 10 public facing storage assets — % of organizations



As mentioned, intentionally exposed cloud assets are benign and understanding risk will enable you to discern between public assets that should and should not be configured as such. In the case of cloud storage assets, it is important to discover and classify whether sensitive data resides within and identify risky combinations including through custom prioritization.

Figure — Top 10 public cloud storage assets of organizations across cloud providers, with both Microsoft Azure SQL server and Microsoft Azure storage account blob container leading at 63%

Exposed storage

Just as access keys, combined with excessive permissions, create the literal keys to the cloud kingdom, public-facing buckets combined with excessive permissions are a straight path to the data stored within. Overcoming this acute cloud risk requires understanding where sensitive data resides, who can access it and how it has been used. Integrating data in a cloud security strategy provides context for understanding and prioritizing risk in storage buckets that are overprivileged, publicly exposed and/or both.

29% of organizations have buckets, public and private, with overprivileged access.

39% of organizations have public buckets.

6% of organizations have public buckets with overprivileged access.

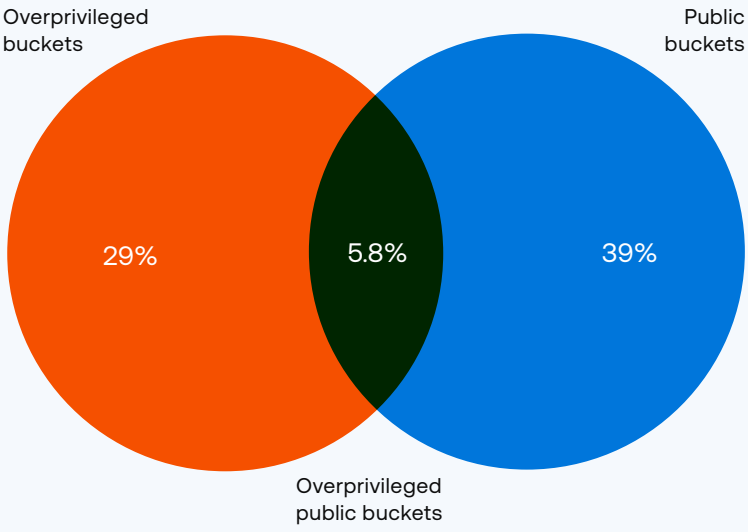


Figure – Percentage (%) of organizations with exposed storage buckets

Kubernetes security challenges — who's at the helm?

As containerized application adoption rises, with Kubernetes serving as the primary orchestrator and manager, new security challenges are emerging that require expertise and a deep insight into Kubernetes-related complexities.

In short, Kubernetes has made it to cybersecurity, big time! It has become an attractive attack target, with malicious actors primarily looking to mine cryptocurrencies and shift their efforts to the cloud. At high risk are publicly accessible clusters that grant anonymous access with elevated privileges and clusters hosting vulnerable applications. Due to the seriousness and complexity of this trilogy of factors, we focused our analysis on Kubernetes-specific configurations that expose clusters to such risks.

Our research found key Kubernetes-related risks in organizations' cloud environments.

78% of organizations have publicly accessible Kubernetes API servers.

44% of organizations have containers running as privileged.

Public Kubernetes API server

The Kubernetes API enables querying and manipulation of the state of API objects within Kubernetes. For most managed Kubernetes providers, to enable the Kubernetes API server to serve its critical role as the main gateway into the cluster, the default configuration exposes the server to the internet. It is not surprising, then, that 78% of organizations were found to have Kubernetes API servers that are publicly accessible.

This configured internet exposure makes the Kubernetes API server an attractive target for attackers. Malicious scanners continuously scan the internet for exposed clusters. Any misconfigurations or vulnerabilities detected by this scanning can lead to further malicious exploitation in the environment.

Public exposure of Kubernetes clusters through inbound internet access is also a risk, if potentially a lesser one. The finding that 41% of Kubernetes clusters allow inbound internet access indicates outside exposure, whose risk can be lowered by applying firewall or security group rules that isolate the clusters. If such security practices are not applied, or not applied correctly, these exposed workloads can be dangerous.

Distribution of organizations with public clusters

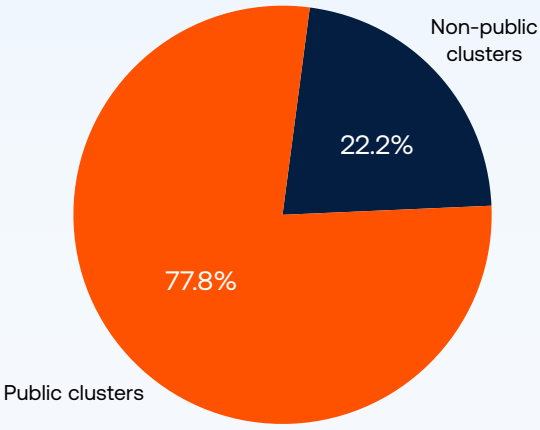


Figure — 78% of organizations have public clusters

Distribution of public/non public clusters

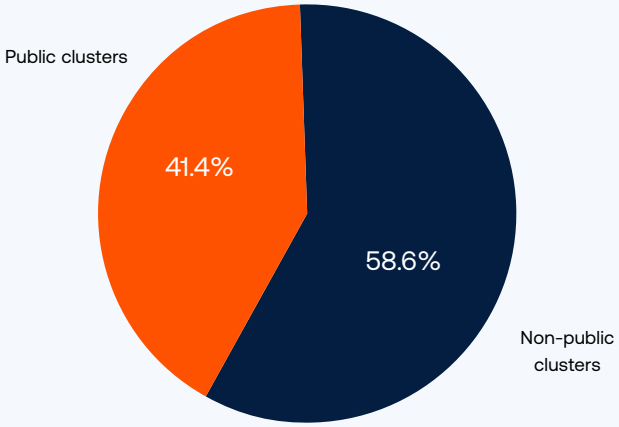


Figure — 41% of Kubernetes clusters, across all cloud providers, allow inbound internet access

Kubelet server with anonymous access enabled

Kubelet is a crucial component in Kubernetes, serving as the primary node agent and handling containers throughout their lifecycle. By default, the configuration for most major cloud providers allows anonymous access to Kubelet, effectively allowing anyone to authenticate as the anonymous user (the anonymous-auth flag is set to true). When used with a publicly accessible cluster, this configuration becomes a toxic combination, with increased risk of being compromised. Assigning elevated privileges to `system:anonymous` user significantly amplifies the risk, potentially leading to malicious activities such as cryptojacking within the cluster.

We flag this as a key finding because it is well recognized today that anonymous access is extremely dangerous, a cloud security no-no, as it allows anyone, without authentication, to interact with the containers — yet 3% of organizations are still allowing it.

3% of organizations have containers that allow anonymous access.

Distribution of organizations with anonymous access enabled Kubelet servers

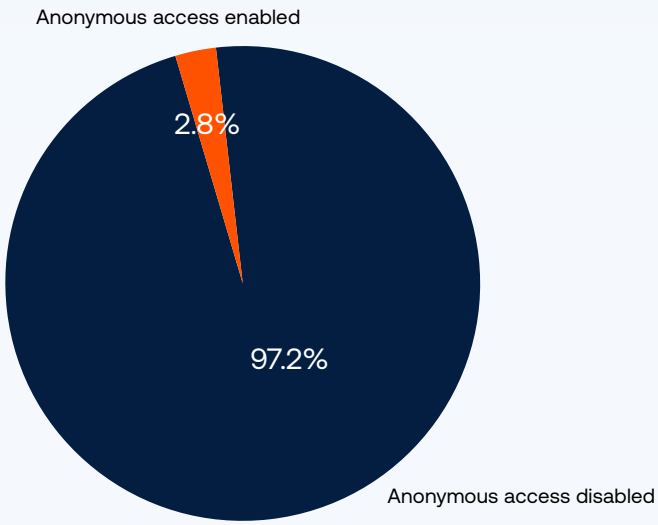


Figure — 3% of organizations globally have containers enabled for anonymous access

Of the containers enabled for anonymous access, GCP had the highest instance (4.4%), followed by Microsoft Azure (1.2%) and AWS (0.6%). This finding may reflect Google's inherent association with Kubernetes and the aim to make cloud-based container deployments accessible. It goes without saying that to eliminate the unnecessary risk of containers that are both exposed and overprivileged organizations need to be able to understand when anonymous access has been enabled and when a container's permissions are elevated.

Overprivileged cluster-admin role

The cluster-admin role-based access control (RBAC) role grants extensive privileges within the environment. When used in a ClusterRoleBinding, the role grants full control over every resource in the cluster. Such unfettered access poses high risk so this superuser role should be reserved for essential tasks only. Access by an attacker to such privileged roles amplifies the risk of data breaches and unauthorized access. Alternatives to this broad, cluster-level role include roles that limit access by namespace, granular access controls using an Open Policy Agent (OPA) or, if available, pod-level security controls.

58% of organizations have cluster-admin role bindings in their environments.

Distribution of organizations with over-privileged cluster-admin roles

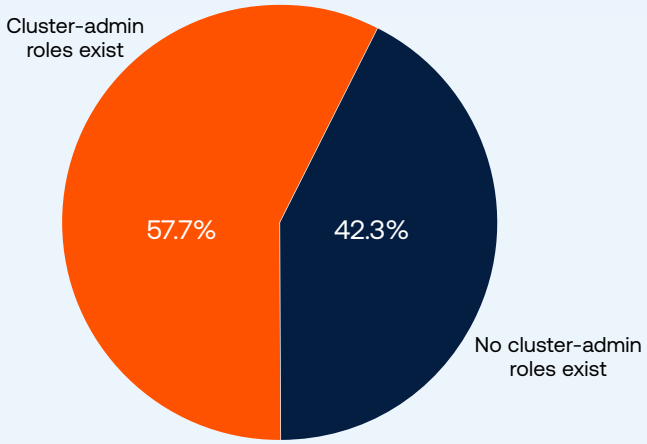


Figure — 58% of organizations overall have cluster-admin role bindings

Of the nearly 60% of organizations that have cluster-admin role bindings, usage by cloud provider is fairly similar (AWS, 67%; Microsoft Azure, 57%; GCP, 71%; note: some organizations have multiple cloud providers so the values do not add up to 100%). To limit risk, organizations should review cluster-admin role bindings, check if they are used and need the cluster-admin role, eliminate those that do not and, where possible, bind users to a lower privileged role. They should enhance security practices by using finer-grained alternatives such as those cited above.

Container running as privileged

Running a container in privileged mode grants access to the host's resources and kernel capabilities. Since attackers can exploit such access, running privileged containers is strongly discouraged by multiple standards, including CIS benchmarks, NIST and CISA.

44% of organizations have containers running as privileged.

Distribution of organizations with containers running as privileged

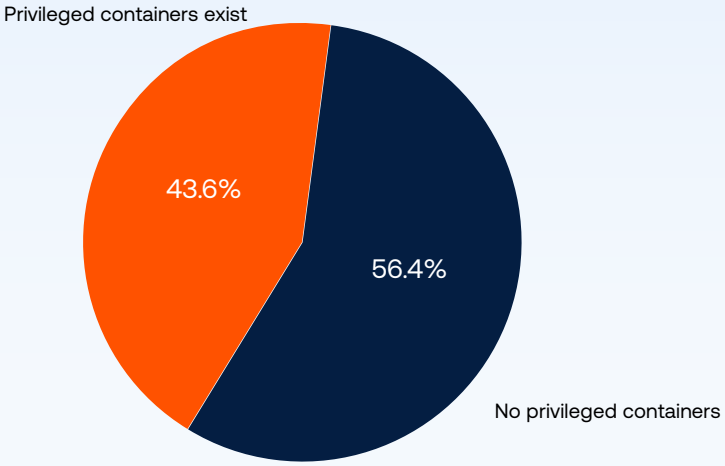


Figure — 44% of organizations have containers running as privileged

Approximately half of organizations using GCP (52%) and AWS (48%) are running privileged containers; about a third (31%) of Azure users are doing the same. This may be because GCP and AWS are the deployment platforms preferred by developers, leading to more unmonitored environments, with fewer controls, whereas Azure, popular among enterprises, is a more controlled environment overall, including robust container management tools.

Mitigation strategies

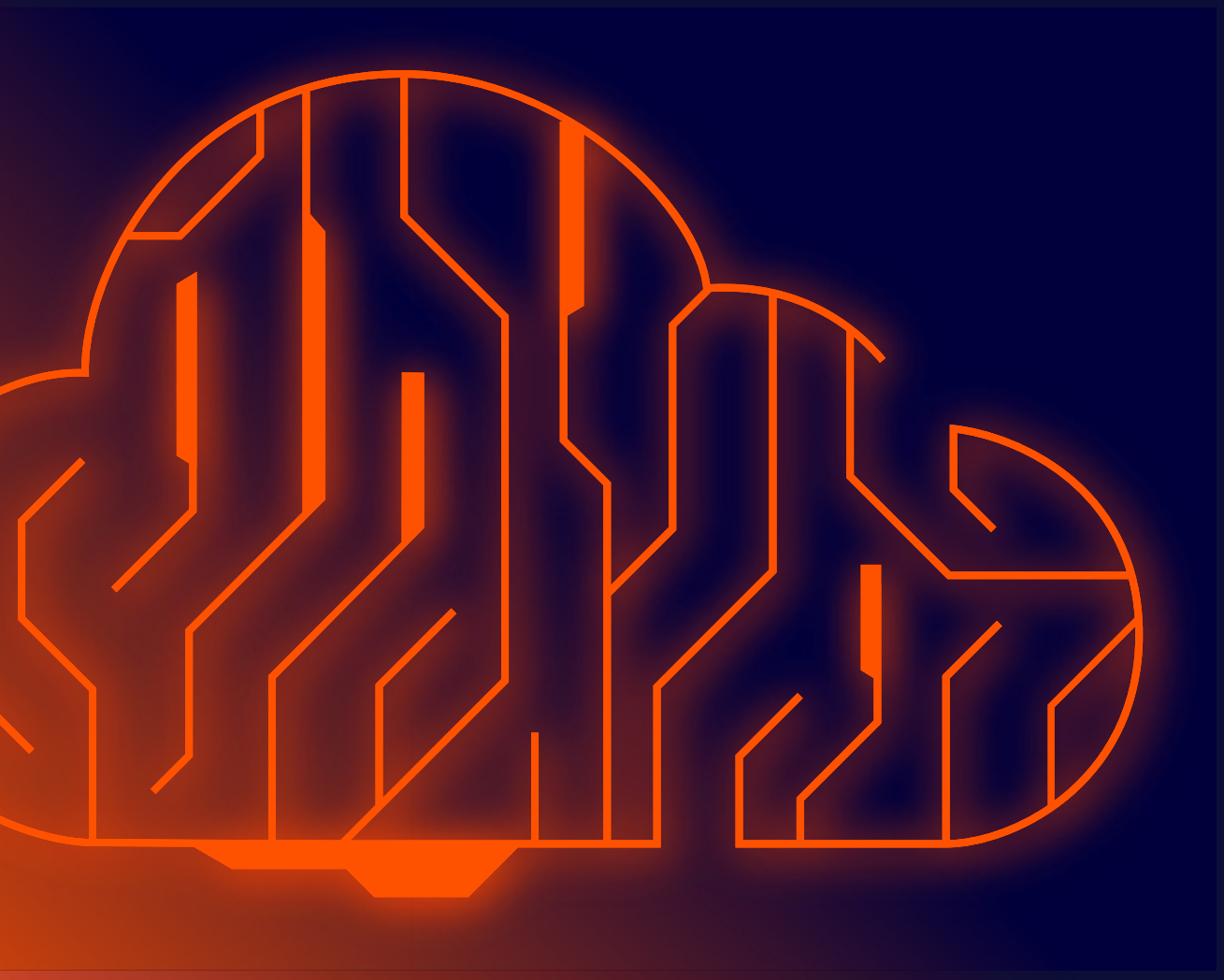
Strategies for addressing and mitigating cloud risks span an organization's security culture, technologies and practices. The report's findings point to common areas of weakness and, in some cases, vulnerability that self-perpetuates. We believe actions like those below will help organizations overcome "toxic cloud trilogies" and other security gaps, and help them deliver cloud security from a position of strength:

1. **Create a context-driven ethos**: Bring identity, vulnerability, misconfiguration and data risk information together in unified tooling, for accurate visualization, context and prioritization around cloud security risk. Not all risk is created equal — identifying toxic combinations can dramatically reduce risk.
2. **Closely manage Kubernetes/containers access**: Ensure containers are configured as privileged only when absolutely necessary. Adhere to Pod Security Standards, such as limiting privileged containers and enforcing access controls. As a principle:
   - Restrict inbound access, limit inbound access to Kubernetes API servers and ensure that Kubelet configurations disable anonymous authentication.
   - Review cluster-admin cluster role bindings, check if they are used and need the cluster-admin role; where possible, bind users to a lower privileged role.
3. **Credential and permissions management**: Regularly rotate credentials, avoid using long-lasting access keys, and implement Just-in-Time access mechanisms. Regularly audit and adjust permissions for human and non-human identities to adhere to the principle of least privilege.
4. **Prioritize vulnerabilities**: Focus remediation efforts on high-risk vulnerabilities, especially those with high VPR scores.
5. **Minimize exposure**: Review public assets to ensure such exposure is needed and doesn't compromise confidential information or critical infrastructure. Keep up with patches.

Conclusion

As cyber exposures proliferate across the enterprise, business risk has reached an untenable level. Understanding toxic cloud trilogies and other toxic combinations, including knowing what data is at risk of being breached, is key to effectively addressing the highest priority exposures. The danger is in the gaps where attackers move in, navigating nimbly between and across outdated, incomplete approaches that can't visualize or mobilize in force.

Tenable provides an actionable cloud security platform that helps enterprises rapidly expose and close priority security gaps in their cloud infrastructure caused by misconfigurations, risky entitlements and vulnerabilities. It helps organizations isolate and eradicate cloud exposures at scale for public, private and hybrid cloud environments, across infrastructure, workloads, identities and data, including through AI insights into access, resources and datasets.



Methodology

This report was created by analyzing information gathered from millions of cloud assets across multiple public clouds, all scanned through the Tenable Cloud Security platform. The data cited in this report was collected from January through June 2024.

The data set consisted of:

- Cloud workload and configuration information
- Millions of real-world cloud assets in active production
- Data from the AWS, Microsoft Azure and GCP environments of organizations

To determine which CVEs have the highest criticality, we applied our proprietary best-of-breed scoring mechanism, the Tenable Vulnerability Priority Rating (VPR), to common cloud CVEs. The Tenable VPR rates vulnerabilities based on severity level (Critical, High, Medium and Low) as determined by two components: technical impact and threat. The resulting dynamic scoring determines the likelihood of exploitation and aims to help organizations improve their remediation efficiency and effectiveness.

About Tenable Cloud Research

Tenable Cloud Research is the cloud research arm of Tenable Research. It conducts ongoing research into new attack vectors, uncovers and discloses cloud provider vulnerabilities, and applies its expertise to innovatively fortify the Tenable cloud product against emerging risks.

Recent discoveries include:

- EmojiDeploy: Smile! Your Azure Web Service Just Got RCE'd ._.
- Abusing Service Tags to Bypass Azure Firewall Rules
- FlowFixation: AWS Apache Airflow Service Takeover
- ConfusedFunction: Privilege Escalation Vulnerability
- CloudImposer: RCE Vulnerability in GCP Composer

About Tenable

Tenable is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for more than 44,000 customers around the globe. Learn more at www.tenable.com.

Contact Us

Please email us at sales@tenable.com or visit tenable.com/contact.

111324