Cloud Data Security Snapshot: Current Exposure Trends

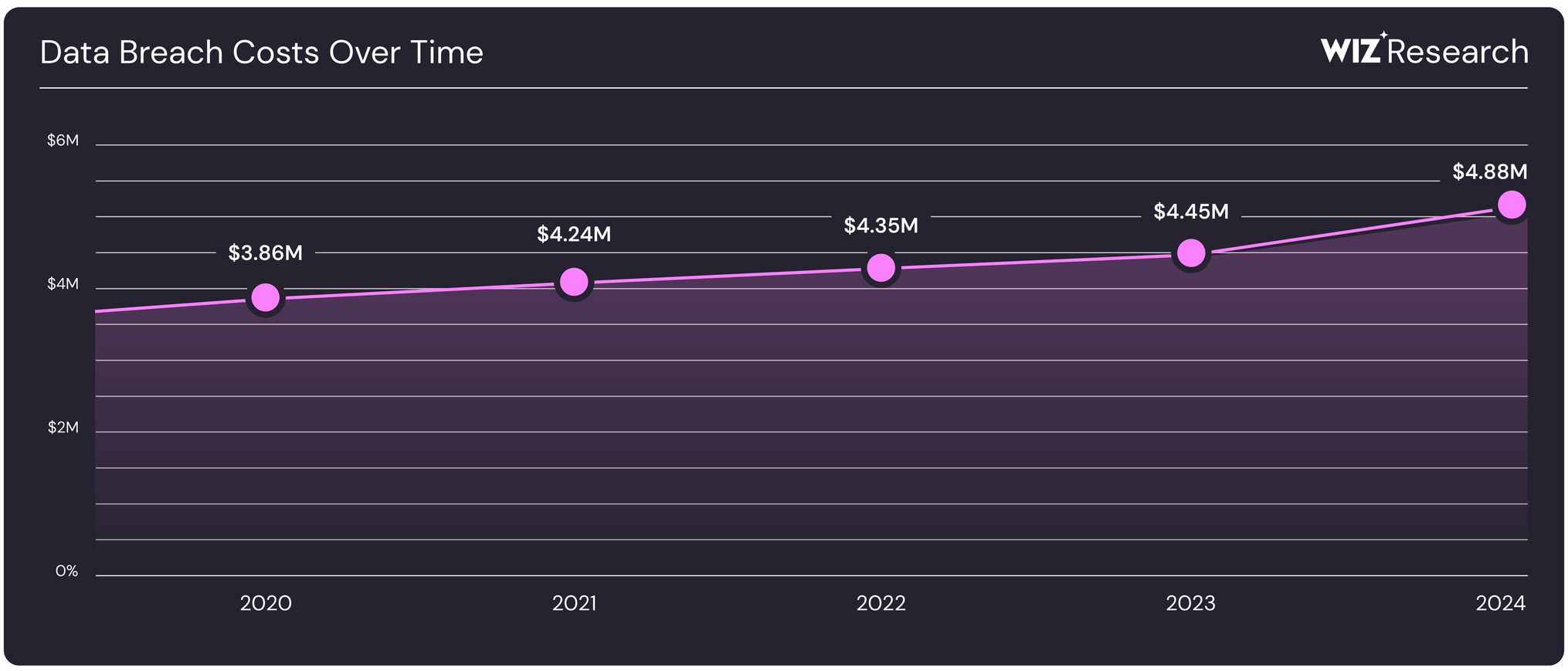
Table of Contents

OUR RESEARCH SHOWS

72% of cloud environments
have publicly exposed PaaS databases
lacking sufficient access controls

Introduction

As cloud adoption accelerates, data exposure becomes a top security (and business) priority. Misconfigurations, inadequate access controls, and high-severity vulnerabilities all place sensitive data at risk. Meanwhile, the cost of a data breach continues to grow with each passing year: In 2024, the global average cost of a breach was **$4.88M — a 10% increase from 2023** (IBM, 2024).



Source: IBM's Cost of a Data Breach Report (2020-2024)

Our intention with this report is to provide a factual, data-based assessment of the current state of customer data security posture and share real-life examples of relevant incidents that demonstrate the importance of robust security practices. This report is based on data collected and analyzed from **hundreds of thousands of cloud accounts** throughout 2024. We hope these findings will help security teams to identify and execute on opportunities to better secure their critical data.

Executive Summary

Our findings reveal that:

1. **54% of cloud environments have exposed VMs containing sensitive information** like credit card details and phone numbers, increasing the risk of privacy violations and regulatory non-compliance.
2. **12% of cloud environments have publicly exposed containers with high or critical severity vulnerabilities and known exploits.**
3. **4% of cloud environments have misconfigured HTTP/S application endpoints that expose sensitive data.**
4. **1% of cloud environments have storage buckets that allow for admin-level lateral movement, and 3% of service accounts with access to sensitive data are accessible by all users.**

These findings spotlight security blind spots that involve toxic combinations: public exposure and sensitive data, excessive access and lateral movement potential. They reinforce the need for tighter access policies, continuous monitoring, and data-aware risk remediation.

Key Findings:

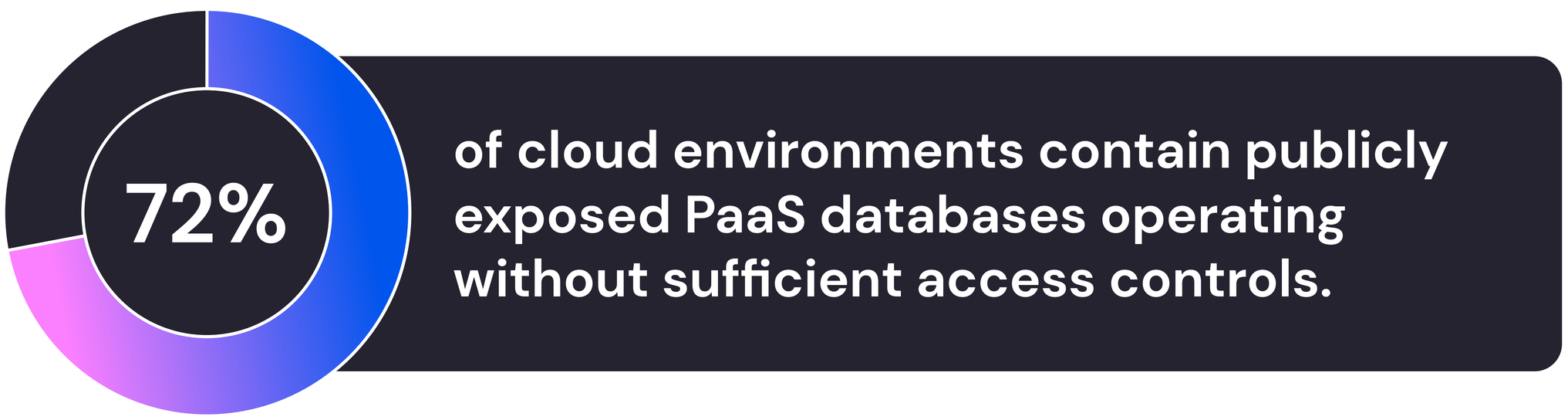
1 Many Cloud Environments Lack Context-Aware Access Controls.

While public cloud buckets are common in modern architectures (e.g., to host public assets or content delivery), elevated risks arise when public access intersects with sensitive data—a toxic combination that elevates breach risk.

Our research found that:

- Publicly accessible cloud storage buckets are widespread, but without proper context (e.g., containing personal or confidential data), public access alone is not inherently risky.
- **22%** of cloud environments have buckets that allow write access for all users, increasing the threat of unauthorized data modification or ransomware.
- **72%** of environments have publicly exposed PaaS databases lacking sufficient access controls—a much more pressing risk given the likelihood of sensitive data in these databases.

For a real-world example of the perils of misconfigurations, look no further than a recent breach involving an exposed Microsoft server (Wiz, 2023): 38 terabytes of sensitive data were accidentally exposed due to misconfigurations, demonstrating the potential scale and impact of improperly secured cloud storage.



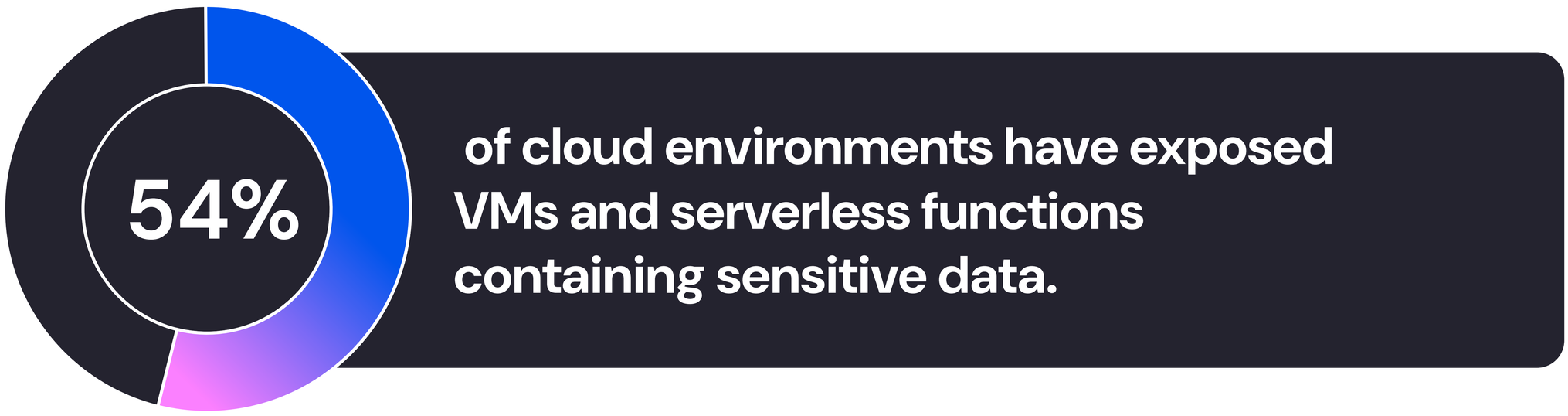
2 54% of Environments Have Exposed Cloud Assets with Sensitive Data.

Misconfigured assets are not just accessible—they often hold sensitive data, making the prospect of unauthorized access a particularly concerning one:

- **54%** of cloud environments have exposed VMs and serverless instances granting access to sensitive data, presenting a significant entry point for attackers.
- **29%** of cloud environments have exposed assets containing personal information, heightening the stakes for privacy violations and identity theft.
- **35%** of cloud environments have VMs or serverless instances that both expose sensitive data and are vulnerable to high or critical severity threats.

This combination of exposed sensitive data and critical vulnerabilities creates a perfect storm for potential breaches, offering attackers both valuable targets and the means to exploit them.

A high level of exposure intensifies the risk of identity theft, reputational damage, and failure to meet compliance mandates. Take the recent Dell (Business Insider, 2024) and Ticketmaster (Framework Security, 2024) security incidents as examples. In both cases, the sensitive information of more than 40 million customers was compromised.

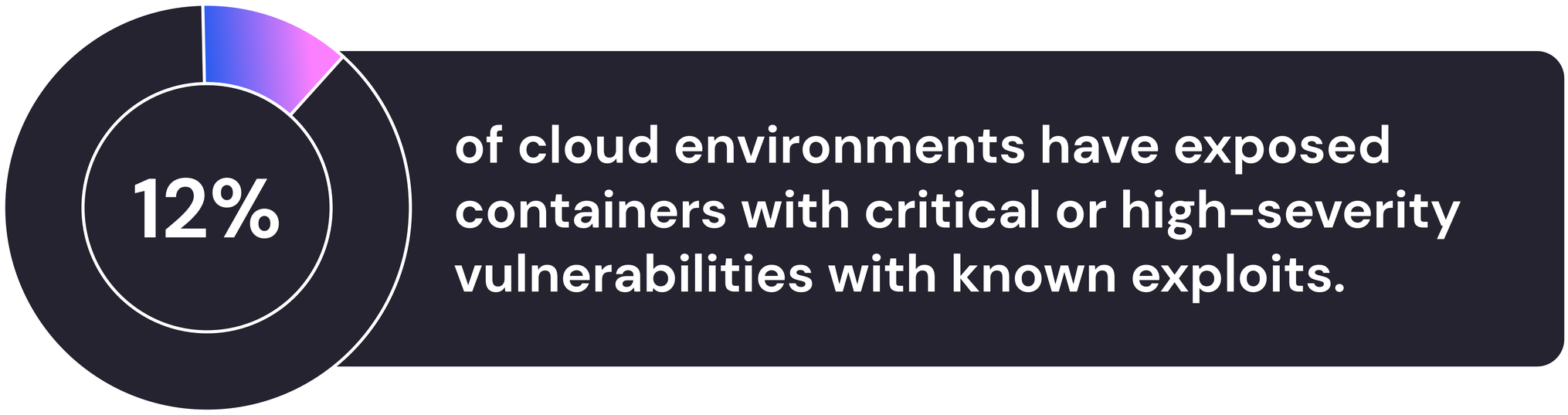


3 Containers and Application Endpoints Remain Key Targets with High-Severity Vulnerabilities.

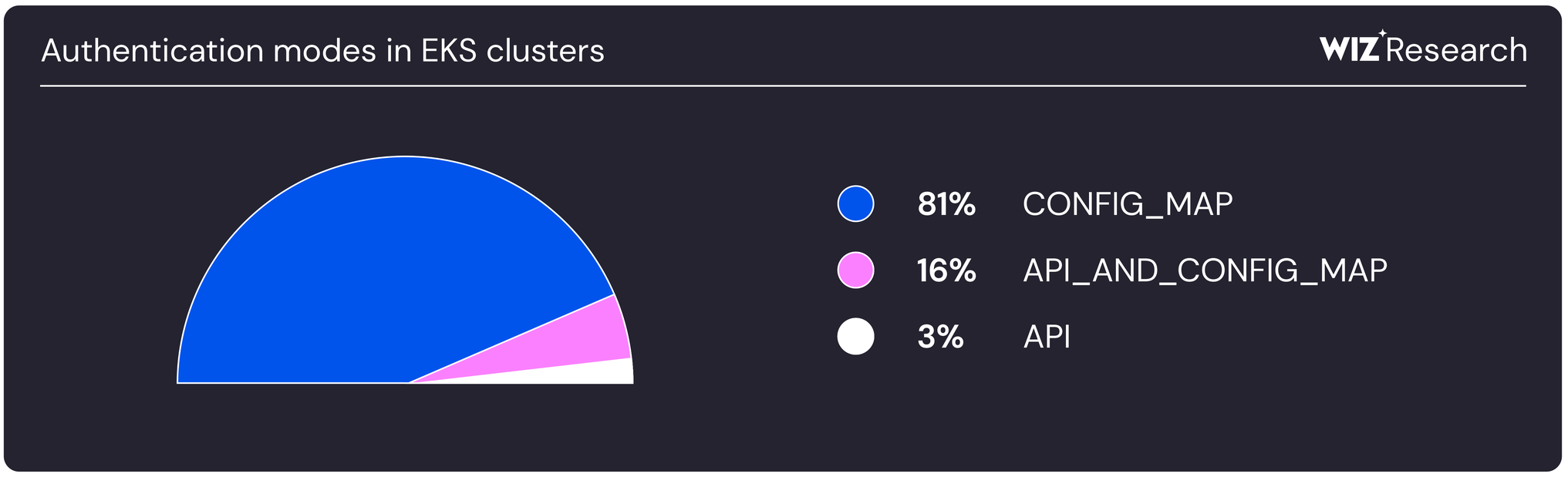
Containers, which are integral to cloud-native architecture, are also often vulnerable:

- **12%** of cloud environments have publicly exposed containers containing high- or critical-severity vulnerabilities with known exploits.
- **4%** have misconfigured HTTP/S application endpoints that expose sensitive data. While this may seem like a small number, it represents a substantial attack surface—especially given the frequency and scale of modern web app deployments.

Even a single misconfigured container or endpoint can act as a gateway for attackers, putting entire systems and sensitive data at risk. The presence of known exploits significantly lowers the barrier to entry, making these vulnerabilities especially dangerous and important to address.



A recent Wiz Research report on Kubernetes (Wiz, 2025) illustrates how configuration drift can silently expand the attack surface. Alarmingly, **81%** of clusters still rely solely on the outdated CONFIG_MAP method to store sensitive configuration data—a practice AWS and other cloud providers discourage due to its lack of encryption and access controls. This misconfiguration puts secrets like API keys and database credentials at risk of exposure, especially when paired with other container vulnerabilities.



4 Weak Access Controls are a Hidden Pathway to Privilege Escalation and Lateral Movement.

Once attackers infiltrate a cloud environment, weak access controls allow them to move laterally and escalate privileges:

- **1%** of cloud environments allow lateral movement to admin roles, enabling attackers to expand access within the cloud environment. This small but critical percentage represents a potential pathway for attackers to gain extensive control over cloud resources.
- **3%** of cloud environments have service accounts that are accessible to all users and contain sensitive data, inviting unauthorized access and privilege escalation.

Again, don't let these small percentages fool you; they can still represent significant security risks. In large-scale cloud environments, even a seemingly small percentage can translate to numerous potential entry points for attackers. Moreover, the high-privilege nature of these issues means that exploiting just one could lead to catastrophic breaches, potentially compromising entire systems or exposing vast amounts of sensitive data across an organization.

For example, in the case of the 2023 MOVEit Transfer breach (Wiz, 2023), attackers exploited a vulnerability in the file transfer system, which allowed them to initially gain unauthorized access through SQL injection. After compromising the system, they conducted reconnaissance to identify valuable targets and then used stolen credentials to move laterally across networks, accessing sensitive data undetected. This resulted in the exposure of data from numerous organizations, with an estimated 40 million records compromised.

How Wiz Can Help

Wiz offers critical DSPM capabilities to help organizations discover sensitive data, manage permissions, and identify attack paths within their cloud infrastructure.

Agentless Scanning:
Wiz examines public and private storage, hosted databases, and NoSQL platforms like Amazon DynamoDB without requiring agents. It identifies sensitive data such as PCI, PII, PHI, and user-defined categories, helping uncover unique business risks.

Rich Context:
Wiz's Security Graph connects data vulnerabilities to broader cloud risks, such as public exposure or misconfigurations. Uncovering these attack paths enables remediation that focuses on high-priority threats posing the greatest danger to sensitive data.

Comprehensive Access Control Visibility:
Wiz maps out 'who has access to what' across your cloud environment, identifying overprivileged accounts, unused permissions, and potential access paths that could lead to lateral movement or privilege escalation. The result is tighter security controls and reduced attack surfaces.

Developer Love:
The Wiz CLI and integration with CI/CD environments helps Wiz prevent data exposure by identifying risks earlier in the development lifecycle so teams can block risky deployments and refine compliance policies.

Customization and Flexibility:
Organizations can set tailored policies to identify sensitive data in code repositories, IDEs, or specific directories—auditing or blocking findings as needed. Custom classifiers also allow businesses to detect entity types unique to their operations.

> "A major concern for us is customer data security. We can't have any personal information on the platform to adhere to GDPR. With Wiz's DSPM, we can easily detect personal information and stay compliant."
>
> **Anthony Lewkowicz, CISO, Valiuz**

Read full story

Conclusion

High exposure rates of storage buckets, containers, and VMs elevate the risk of data breaches, compliance violations, and reputational harm. To effectively manage data security posture, focus on minimizing your attack surface and addressing key vulnerabilities:

1. **Secure Storage Configurations:** Misconfigured storage assets are alarmingly common and a major driver of data exposure. Implement strict access controls to prevent unauthorized access and establish clear policies to limit permissions and restrict access to cloud storage buckets.
2. **Protect Sensitive Data:** This simple mandate lies at the core of a strong DSPM strategy. Ensure sensitive information is not stored in exposed assets and actively address vulnerabilities to maintain regulatory compliance and protect privacy.
3. **Harden Cloud-Native Applications:** As container adoption accelerates, organizations must proactively prepare for exploitation risks. Enforce regular patching, deploy robust endpoint security, and monitor exposed assets continuously. Use solutions that can identify when VMs or containers store sensitive data to reduce potential exposure.
4. **Enforce Least Privilege Access:** Effective access control is critical to preventing lateral movement and privilege escalation. Identify and eliminate overprivileged accounts, enforce role-based access policies, and maintain continuous visibility across your cloud environment.

References

1. IBM. (2024). Cost of a Data Breach Report 2024. link
2. IBM. (2023). IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. IBM Newsroom. link
3. IBM. (2022). Cost of a Data Breach Report 2022. Key4Biz. link
4. IBM. (2021). Cost of a Data Breach Hits Record High During Pandemic. IBM Newsroom. link
5. IBM. (2020). Cost of a Data Breach Report 2020. DataEndure. link
6. Wiz. (2023). 38 Terabytes of Private Data Accidentally Exposed by Microsoft AI Researchers. link
7. Business Insider. (2024). Dell Data Breach 2024: What to Know as 49 Million Customers Feel Impacts. link
8. Framework Security. (2024). Ticketmaster Breach: A Deep Dive into the May 2024 Cyberattack. link
9. Wiz. (2025). Securing the Container Frontier: Kubernetes Trends Report 2025. link
10. Wiz. (2023). MOVEit Transfer Vulnerability CVE-2023-34362. link