

HADRIAN

eBook

Top 10 Cloud Misconfiguration and How to Resolve Them



Table of contents

| | |
|--|-----------|
| Introduction | 3 |
| Common Cloud Misconfigurations | |
| Misconfiguration 1: Publicly Accessible Storage | 4 |
| Misconfiguration 2: Exposed Databases | 5 |
| Misconfiguration 3: Unrestricted Inbound Ports | 6 |
| Misconfiguration 4: Lack of Encryption | 7 |
| Misconfiguration 5: Default Credentials | 8 |
| Misconfiguration 6: Misconfigured Access Control | 9 |
| Misconfiguration 7: Unpatched Vulnerabilities | 10 |
| Misconfiguration 8: Server-Side Request Forgery | 11 |
| Misconfiguration 9: Insufficient Segmentation | 12 |
| Misconfiguration 10: Misconfigured Containers | 13 |
| The Hadrian Advantage | 14 |
| About Hadrian | 15 |

Introduction

Understanding and Addressing Cloud Misconfigurations

Cloud misconfigurations are a leading cause of security breaches, exposing sensitive data and causing compliance issues. The issue is so prevalent that almost all leading global security advisers regularly track the instances and publish annual advisories on them.

Based on the intelligence aggregated by Hadrian, we have listed the ten most common cloud misconfigurations. This e-book aims to help you understand their impact and how you can address them with the help of Hadrian's solution. Whether you are just realizing the problem, researching solutions, or evaluating vendors, this guide will provide actionable insights and expert advice.

This e-book has

Articulated the problem and impact

The ten common cloud misconfigurations and their implications

Provided an overview of solutions

Effective strategies to mitigate these issues

How Hadrian's automated risk detention and intelligent remediation services help you in this

Listed Hadrian's capabilities as your trusted cybersecurity partner

How Hadrian's expertise and tools can help safeguard your cloud interface

Misconfiguration 1: Publicly Accessible Storage

Unauthorized access to sensitive data due to misconfigured storage settings.

Issue

Cloud storage buckets (e.g., Amazon S3, Azure Blob Storage) are often incorrectly set to be publicly accessible, allowing unauthorized access to sensitive data. A Cloud Security Alliance study in 2023 revealed that 21% of publicly exposed S3 buckets contained sensitive data, and they were accessible due to misconfigured ACLs, incorrect bucket policies, or improper use of the S3 Block Public Access feature.

Impact

- ✓ Data breaches
- ✓ Exposure of sensitive information
- ✓ Compliance violations

Mitigation

- ✓ Regularly audit cloud storage permissions.
- ✓ Implement automated tools to monitor and adjust access settings.
- ✓ Educate staff on the importance of secure configuration practices.

Hadrian's Solution

Hadrian's platform continuously monitors cloud storage configurations to identify and remediate publicly accessible buckets. Hadrian platform provides instructions on how to adjust permissions and apply security best practices, ensuring that storage buckets are only accessible to authorized users.

Misconfiguration 2: Exposed Databases

Vulnerable databases due to lack of access controls.

Issue

In late 2023, Microsoft AI researchers accidentally exposed 38 TB of personal data and other sensitive information in a database due to improperly configured permissions. Databases are often left exposed to the internet without proper access controls or authentication mechanisms, making them vulnerable to unauthorized access and data breaches.

Impact

- ✓ Unauthorized data access
- ✓ Data loss
- ✓ Potential data manipulation

Mitigation

- ✓ Enforce strong authentication and access controls on all databases.
- ✓ Regularly review and update database security settings.
- ✓ Use network security groups to restrict database access to specific IP ranges.

Hadrian's Solution

Hadrian employs continuous scanning to detect exposed databases and improper access controls. By implementing robust authentication mechanisms and restricting public access, Hadrian ensures that database environments are secured against unauthorized access.

Misconfiguration 3: Unrestricted Inbound Ports

Increased risk due to permissive network traffic rules.

Issue

Inbound network traffic rules (security groups or firewall rules) are often too permissive, allowing traffic from any IP address, which increases the risk of unauthorized access and exploitation. For example, in 2017, cybercriminals exploited an SMB vulnerability on port 445 to spread the WannaCry ransomware strain.

Impact

- ✓ Unauthorized access
- ✓ Potential exploitation of vulnerabilities
- ✓ Potential data manipulation

Mitigation

- ✓ Regularly review and update inbound network traffic rules.
- ✓ Implement least privilege access for network traffic.
- ✓ Use automated tools to monitor and enforce network security policies.

Hadrian's Solution

Hadrian's platform audits inbound network traffic rules in depth by performing regular port scans. The platform allows you to configure workflows that generate alerts if an unexpected open port is detected, preventing unauthorized users from exploiting them.

Misconfiguration 4: Lack of Encryption

Vulnerable data due to unencrypted storage and transmission.

Issue

Data at rest and in transit is often not encrypted, leaving it vulnerable to interception and unauthorized access. In fact, research released by Enterprise Strategy Group in 2023 revealed that a lack of encryption remained the top reason for data loss for 33% of the surveyed organizations.

Impact

- ✓ Data breaches
- ✓ Loss of confidentiality
- ✓ Compliance issues

Mitigation

- ✓ Encrypt data at rest using strong encryption algorithms.
- ✓ Implement TLS/SSL for data in transit.
- ✓ Regularly audit encryption settings and update protocols as needed.

Hadrian's Solution

Hadrian detects encryption in transit by analyzing the SSL/TLS versions/ciphers during the initial handshake. By implementing strong encryption protocols and continuously monitoring encryption settings, Hadrian proactively mitigates the threat of unauthorized access and breaches.

Misconfiguration 5: Default Credentials

Vulnerability due to unchanged default usernames and passwords.

Issue

Default usernames and passwords are often not changed, leaving cloud resources vulnerable to brute force attacks. According to LastPass, more than 80% of confirmed breaches are related to stolen, weak, or reused passwords.

Impact

- ✓ Unauthorized access
- ✓ Potential for complete system compromise

Mitigation

- ✓ Change default credentials immediately upon setup.
- ✓ Implement strong password policies and use unique passwords.
- ✓ Use automated tools to monitor for and replace weak or default credentials.

Hadrian's Solution

Hadrian's platform automatically detects the usage of default and easily guessable credentials on a variety of login forms. By enforcing password policies and monitoring for weak credentials, Hadrian ensures that all cloud resources are secure from brute force attacks.

Misconfiguration 6: Misconfigured Access Control

Excessive privileges due to poorly configured access controls.

Issue

Access control policies are often overly permissive or incorrectly configured, granting excessive privileges to users and services. According to OWASP, in 90% of the applications they examined, they found some form of misconfiguration.

Impact

- ✓ Unauthorized actions
- ✓ Privilege escalation
- ✓ Potential data breaches

Mitigation

- ✓ Implement least privilege access for all users and services.
- ✓ Regularly review and update access control policies.
- ✓ Use automated tools to enforce and monitor access controls.

Hadrian's Solution

Hadrian's platform continuously audits access control policies to ensure they follow the principle of least privilege. By automatically adjusting policies and enforcing strict access controls, Hadrian minimizes the risk of unauthorized actions and data breaches.

Misconfiguration 7: Unpatched Vulnerabilities

Security risks due to outdated patches and updates.

Issue

Failure to apply security patches and updates to cloud services and virtual machines leaves systems vulnerable to exploitation of known vulnerabilities. A study by the Ponemon Institute noted that 60% of data breach victims cite an unpatched vulnerability.

Impact

- ✓ Exploitation of known vulnerabilities
- ✓ Security breaches
- ✓ System compromises

Mitigation

- ✓ Regularly apply security patches and updates to all systems.
- ✓ Use automated tools to monitor for and apply patches.
- ✓ Maintain an inventory of all systems and their patch status.

Hadrian's Solution

Hadrian's platform continuously monitors for unpatched vulnerabilities and alerts the client about the necessary updates and patches. Whenever a new exploit is discovered Hadrian automatically scans organizations assets for the new vulnerability. By maintaining up-to-date systems, Hadrian ensures that vulnerabilities are addressed promptly, reducing the risk of exploitation.

Misconfiguration 8: Server-Side Request Forgery

Increased risk due to Server-Side Request Forgery (SSRF) vulnerabilities in cloud environments.

Issue

Server-Side Request Forgery (SSRF) vulnerabilities allow attackers to make requests from the server to internal or external services, potentially bypassing firewall rules and accessing sensitive information. In cloud environments, the impact of SSRF vulnerabilities is magnified due to the interconnected nature of services and resources.

Impact

- ✓ Unauthorized access to internal services
- ✓ Potential data breaches and exposure of sensitive information
- ✓ Compromise of cloud resources

Mitigation

- ✓ Validate and sanitize all user inputs to prevent malicious requests.
- ✓ Implement whitelisting to restrict external requests to trusted URLs.
- ✓ Use network segmentation and firewall rules to limit access to sensitive resources.
- ✓ Regularly review and update security policies and configurations.

Hadrian's Solution

Hadrian's platform natively detects SSRF vulnerabilities and identifies their presence in cloud environments. By proactively scanning for these issues, Hadrian significantly reduces the risk of exploitation.

Misconfiguration 9: Insufficient Segmentation

Increased risk due to lack of network segmentation.

Issue

Lack of proper network segmentation allows unrestricted lateral movement within the cloud environment, increasing the risk of widespread compromise following an initial breach.

Impact

- ✓ Widespread compromise
- ✓ Increased risk of data breaches

Mitigation

- ✓ Implement network segmentation to isolate different parts of the cloud environment.
- ✓ Use security groups to enforce segmentation policies.
- ✓ Regularly review and update network segmentation settings.

Hadrian's Solution

Hadrian's platform identifies links between different assets within cloud environments. Understanding the connection between different infrastructure elements the blast impact of an attack can be determined and minimized. Utilizing Hadrian can mitigate the risk of lateral movement and widespread compromise.

Misconfiguration 10: Misconfigured Containers

Vulnerable containers due to improper configuration.

Issue

Containers are often misconfigured, leading to issues such as running containers with root privileges or exposing sensitive data. For example, the keys and tokens for 190,000 accounts lost from Docker Hub as a result of an attacker exploiting weak security configurations in cloud storage.

Impact

- ✓ Container escapes
- ✓ Unauthorized access
- ✓ Potential data breaches




Mitigation

- ✓ Avoid running containers with root privileges.
- ✓ Secure sensitive data within containers.
- ✓ Use automated tools to monitor and enforce container security best practices.

Hadrian's Solution

Hadrian's platform continuously monitors and offers the strongest and apt container configurations to our clients. By identifying poor practises and insecure container environmets, Hadrian enables containers to be proactively secured against vulnerabilities.

The Hadrian Advantage

| Automated Risk Detection  | Comprehensive Cloud Visibility  | Intelligent Remediation  |
|---|--|---|
| <p>Hadrian's event-driven platform continuously monitors your cloud environments for changes in exposure levels.</p> <p>Hadrian utilizes in-house modules developed by our top security researchers to detect cloud misconfigurations and exposed secrets in real-time.</p> <p>This proactive approach ensures that potential security issues are identified and addressed immediately, minimizing the window of vulnerability.</p> | <p>Hadrian's probes are designed to scan various applications and infrastructure components across different cloud environments with ease.</p> <p>Hadrian provides a unified view of all assets by mapping out the entire cloud environment, including hybrid and multi-cloud setups.</p> <p>This comprehensive visibility allows your security teams to identify and manage risks more effectively, even in highly complex and distributed cloud architectures.</p> | <p>Hadrian's platform uses sophisticated risk assessment modules to prioritize security threats based on their potential business impact and likelihood of exploitation.</p> <p>Hadrian generates detailed, actionable recommendations to guide remediation efforts, ensuring that the most critical issues are addressed first.</p> <p>Additionally, Hadrian verifies the success of remediation actions, assuring that vulnerabilities have been effectively mitigated.</p> |

About Hadrian

Hadrian provides the hacker perspective, revealing the targets and methods that could be used in a real-world data breach. Hadrian's continuous and comprehensive testing discovers and validates risks completely autonomously.

Hadrian's platform combines attack surface discovery, automated penetration testing, and threat exposure management technologies in a cloud-based and agentless platform. The cutting-edge technology is constantly updated and improved by Hadrian's in-house hacker team.

Trusted by market leaders

