EBOOK

CLOUD SECURITY PARTNERS

cloudsecuritypartners.com

cloud-security-partners

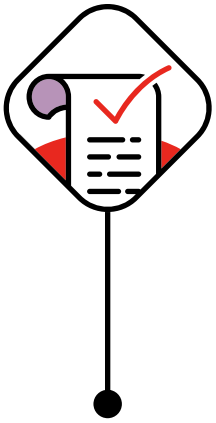
aws Top Ten Security Issues

Serious security breaches often follow the same pattern: An attacker gains a small initial foothold and moves laterally through the network, exploiting vulnerabilities to rapidly reach critical assets and take your data.

Here at **Cloud Security Partners**, we've assessed thousands of AWS accounts and seen how painfully businesses suffer from cloud breaches. We know exactly which mistakes can lead to that fast, total compromise. This eBook is a guide based on that experience, addressing the **ten most critical AWS security issues** that we consistently find, even in environments managed by experienced teams.

Whether you're just beginning your AWS security journey or maturing an existing environment, prioritizing these areas is **non-negotiable**. These are the most frequent, commonly exploited misconfigurations that you must eliminate first. Addressing them will help you reduce your risk exposure, strengthen core security controls, and improve visibility into your cloud environment.

Check to make sure you've addressed the Top 10 AWS observed security issues



Chapter 1

Enable Multi-Factor Authentication on User Accounts

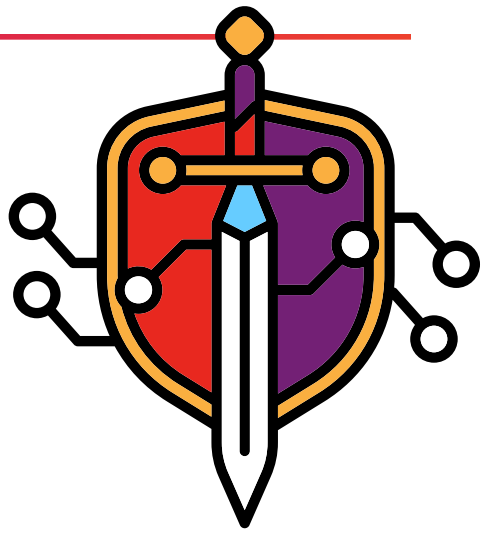
In 2025, compromised credentials were the third most common cause[1] of reported cloud security incidents.

Attackers often use techniques like credential theft or credential stuffing, using compromised credentials from other breaches, to gain access to these accounts. A successful compromise could lead to data theft or worse, control over your cloud environment.

In AWS, attackers target the root account and IAM users as the first step into your network, often using compromised credentials. Root accounts have unrestricted access to all resources, while IAM users, though typically less privileged, can still be granted broad permissions. Both use long-lived credentials, which are a significant security risk.

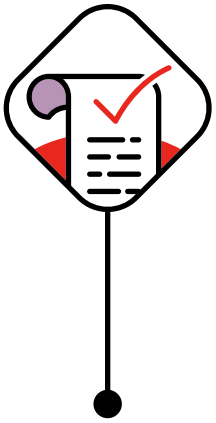
To mitigate the risk of compromised credentials, always enable Multi-Factor Authentication (MFA) for both the root accounts and all IAM users. MFA ensures that even if credentials are compromised, unauthorized access remains difficult without the additional authentication factor, significantly reducing the risk of account takeover.

AWS supports several **MFA methods**, including passkeys, hardware security keys, virtual Time-based One-Time Password (TOTP) applications, and hardware TOTP devices. We highly recommend hardware security keys for their ease of use and resistance to phishing attacks.



To further reduce your risk, avoid **IAM users** whenever possible; they should only be used for legacy purposes and emergencies. Instead, use IAM roles and identity federation for access. These are much more secure as they use short-lived tokens and are centrally managed.

1 - https://www.ibm.com/reports/data-breach



Chapter 2

Use a Federated Identity Provider

Managing individual IAM users can be a security risk.

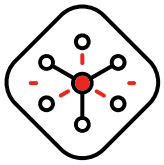
These accounts are difficult to monitor, control, and audit because they are managed directly within AWS and lack robust centralized logging and governance by default.

A far better approach is to use a Federated Identity platform. By using a platform like AWS IAM Identity Center, Azure AD, or Okta, you can manage all user identities and credentials centrally, and associate AWS permissions with those external identities.

Federated identities significantly improve the security of your IAM:

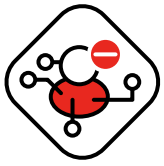
Temporary Credentials

They use short-lived temporary credentials for authentication, which drastically reduces the risk of long-lived, high-privilege keys being leaked or compromised.



Centralized Control

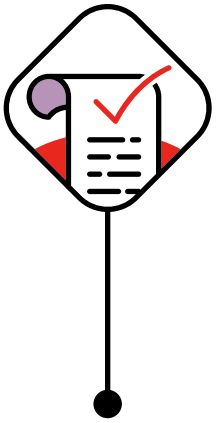
They simplify access management, centralize monitoring, and enable you to use conditional access policies to restrict authentication further.



Streamlined Offboarding

Federation ensures that access is consistently and promptly revoked across all services the moment a user leaves your organization.

Migrating away from manually managed IAM users to a robust Federated Identity Provider is the critical first step to properly setting up access controls within your environment.



Chapter 3

Enable Amazon GuardDuty

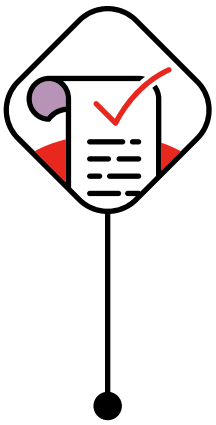
The best defense is GOOD monitoring.

Proactively monitoring your environment for breaches is the most important way to prevent catastrophic security incidents.

AWS GuardDuty is a threat detection service that monitors your AWS environment for malicious activity and unauthorized behavior. It analyzes data from many sources, like AWS CloudTrail, VPC Flow Logs, DNS logs, and threat intelligence feeds to proactively detect and alert on potential security threats.

Many organizations make the mistake of leaving GuardDuty disabled in certain regions, which can leave major blind spots in your monitoring strategy. Since GuardDuty is often the only continuous monitoring strategy in place, it is vital that it is properly enabled and configured, and that alerts are investigated and addressed promptly.

GuardDuty should be enabled in **every** region where you have resources. Results from GuardDuty should be forwarded to an external S3 bucket for extended retention, and integration with an SIEM for further analysis. You should also create a plan for addressing new alerts to ensure timely investigation and response.



Chapter 4

Enhance Logging and Monitoring

Logs are the **most important** way to diagnose and remediate incidents after they occur. Many companies ignore their logs until they need them during an incident.

The main logging and monitoring tools to enable within an AWS environment are:

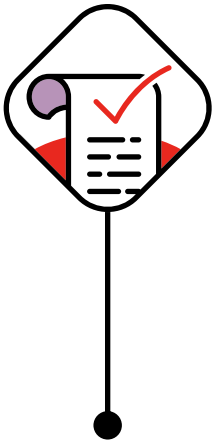
- **CloudTrail:** CloudTrail is a logging service that tracks all user-initiated events and API calls, and can help understand an attacker's path through your environment.
  - **Log file** validation should be turned on when enabling CloudTrail.
  - **Data Event** logging should also be enabled, to add an additional layer of logging.
- **CloudWatch:** CloudWatch sets up alarms and metrics for various security-related events, helping you proactively monitor for security incidents.
- **Config:** AWS Config tracks configuration changes to your environment. Enabling it will allow you to do historical analyses after an incident to determine what misconfigurations were in place.

A robust logging strategy should prioritize visibility and searchability.

Visibility comes from enabling monitoring on all resources, in all regions, and on all accounts.

Searchability comes from collecting all logs and metrics in one central place, such as a secure, centralized S3 bucket, or, preferably, an SIEM.

To enhance monitoring, forward all logs to an external SIEM such as **Amazon Security Lake** or **Splunk**. This will help do further analysis and correlation for rapid investigation in the future.



Chapter 5

Eliminate Overly Permissive IAM Policies

Always design your infrastructure with **defense-in-depth** as the standard.

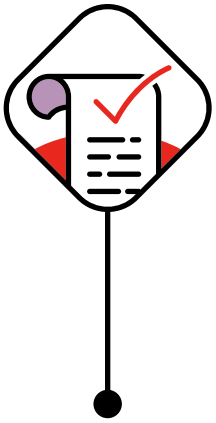
The foundational rule is the Principle of Least Privilege:

If an IAM entity does not need a particular permission, **remove that permission** from the IAM policy. Attaching unrelated permissions to an IAM policy drastically increases your security risk should that IAM entity be breached.

Importantly, wildcard (*) policies must be avoided, as they grant access to all resources within an environment.

To enforce this, leverage **AWS IAM Access Analyzer** to quickly audit all current IAM policies to find which ones are outdated, overpermissioned, or simply obsolete. Use this tool to identify which policies need to be rewritten and to remove any that are unused.

Crucially, analyze cross-account roles, which allow users from another AWS account to access your resources. These can often be over-permissioned, especially when granted to external accounts not under your direct control.



Chapter 6

Audit for Public Data Exposure

A **2024 study**[2] found that nearly **23%** of cloud security incidents were caused by cloud misconfigurations. Within these cloud misconfigurations, publicly exposed data is one of the most common causes of breaches. Attackers actively seek out misconfigured resources using automated tools to access exposed data, and potentially using this foothold to go deeper into your environment.

While **S3 exposure** is the most commonly known attack, there are a **few other** common misconfigurations.

Focus on these four areas when auditing for public data exposure:

S3 Buckets

- **Ensure** that public read/write is not enabled for any S3 buckets unless there is a specific, documented need.
- **Use** the S3 Block Public Access feature to enforce restrictions centrally and prevent accidental data exposure.

Databases (Redshift, RDS, etc.)

- **Verify** that database instances are deployed in a private subnet and are not accessible from the public internet.

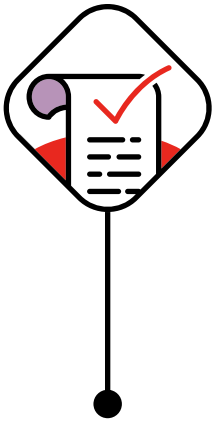
SNS/ SQS

- **Make** sure **Simple Notification Service (SNS)** topics and **Simple Queue Service (SQS)** queues are not exposed to public or overly broad principals. Permissions should be restricted only to roles and users that require access.

EKS (Elastic Kubernetes Service)

- **Confirm** that the EKS control plane is not exposed to the public internet.

2 - https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics



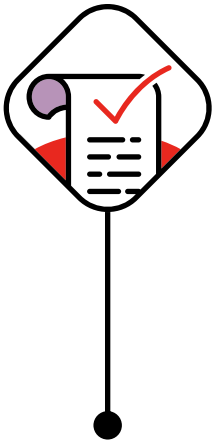
Chapter 7

Enable Network Segmentation

When architecting your cloud infrastructure, your threat model must account for the possibility of any single resource being breached. Implementing the rest of your infrastructure with **defense-in-depth** measures to limit the extent of this breach will significantly mitigate the impact of any future incidents.

Workload and **network** isolation are two such key tools to limit the blast radius of a breach. Segregating workloads and ensuring that components only communicate where necessary prevents attackers from pivoting deeper into your environment. If two workloads do not need to interact, enforce technical controls to block any unnecessary communication between them.

When designing your cloud environment, model how each resource will communicate with every other resource. Based on this network model, use **Virtual Private Clouds (VPC)**, **private subnets**, **Network Access Control Lists (NACL)**, and **security groups** to isolate resources from one another.

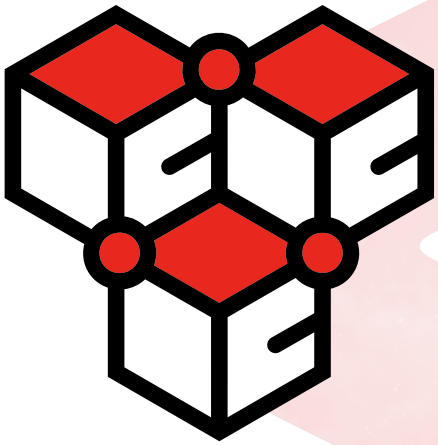


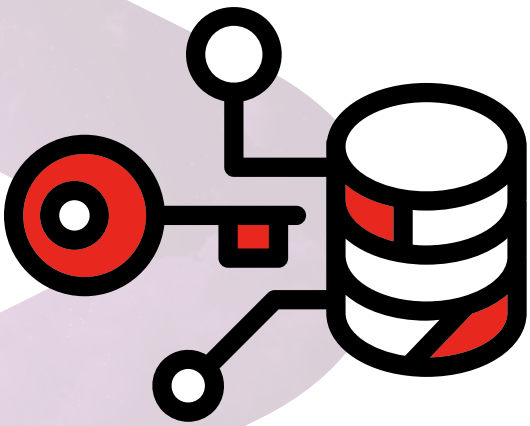
Chapter 8

Set up Appropriate Encryption

Encryption is another powerful defense-in-depth measure that significantly helps mitigate the risk of an unauthorized data breach. This is only true, however, if encryption is **properly enabled** across your environment.

All data must be encrypted both in transit and at rest. This includes **S3**, **Elastic Blob Store (EBS)**, **RDS**, **Redshift**, and **your backup** and **archive storage**. When encrypting, use **Customer-Managed Keys (CMK)**.





Customer-Managed Keys via **AWS Key Management Service (KMS)** allow you to manage your own encryption within your AWS environment. This is a much more granular way to enable encryption and **should be preferred** over Amazon-managed keys when possible.

When implementing encryption, ensure that you follow proper Key Management Service practices. **Routinely** rotate your keys to maintain cryptographic hygiene and ensure that all relevant services are configured to use CMKs.

Chapter 9

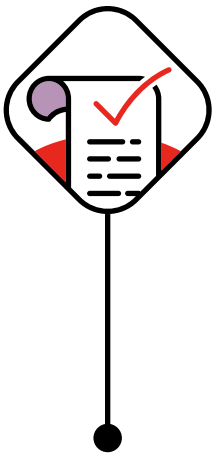
Enable Patch Management

Easier and better patch management is one of the **major benefits** of using the cloud compared to traditional infrastructure. Applying patches on traditional infrastructure can be error-prone, difficult to audit, and often result in inconsistent environments. The superior cloud-native approach is to use **immutable infrastructure principles** instead.

Immutable infrastructure is enabled by building and maintaining **golden images** (pre-patched, pre-hardened system templates).

Instead of patching running instances in place, you simply **replace** them with a new, compliant golden image. This helps ensure that patches are consistently applied and that all deployed resources are compliant with baseline configurations.

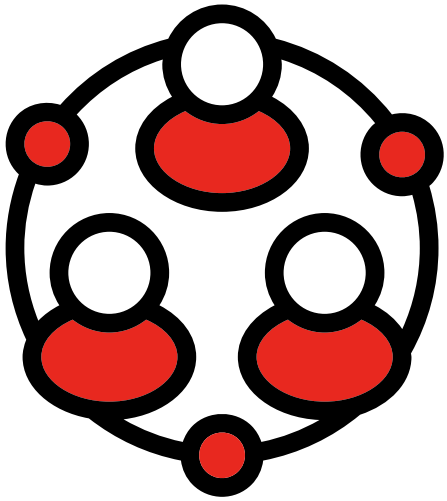
To build and maintain golden images, security scanning **must** be built into your **CI/CD workflow**. Scan all new containers and source code before deploying them. When a new image is released, tag and version the image to ensure traceability and rollback capability.

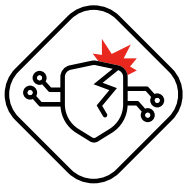


Chapter 10

Apply Policies Consistently Across Organization

Many companies struggle with **cloud bloat**, a situation where the sheer volume of resources and cloud accounts under management makes manually applying consistent security controls **nearly impossible.**



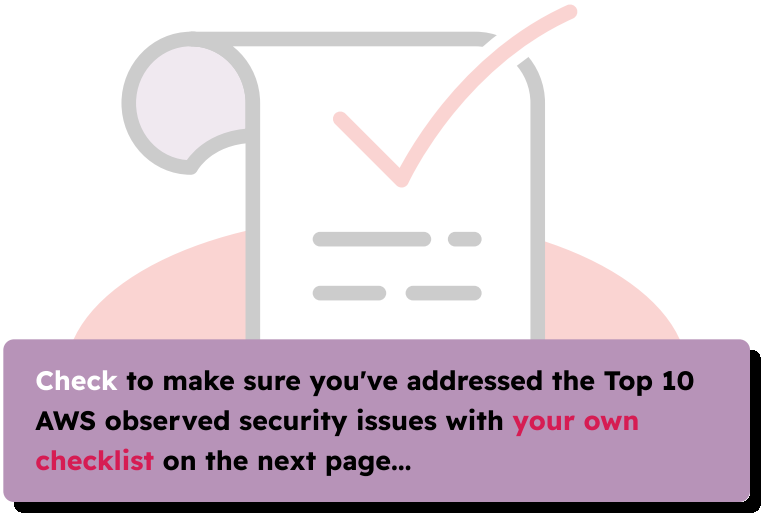


Inconsistent security controls can lead to unmonitored and uncompliant resources, **dramatically increasing** security risk.

Instead of managing each account individually, AWS offers **a tool called Organizations** to unify several accounts under a single security and billing model. **Service Control Policies** allow you to **enforce** security controls across organizations, such as permission limits, globally enabling logging, restricting sensitive operations, and more.

All security controls discussed in this guide should be **propagated** to **every account** in your Organization using Service Control Policies. This will prevent insecure deployments, unmonitored accounts, and poor access control.

Conclusion



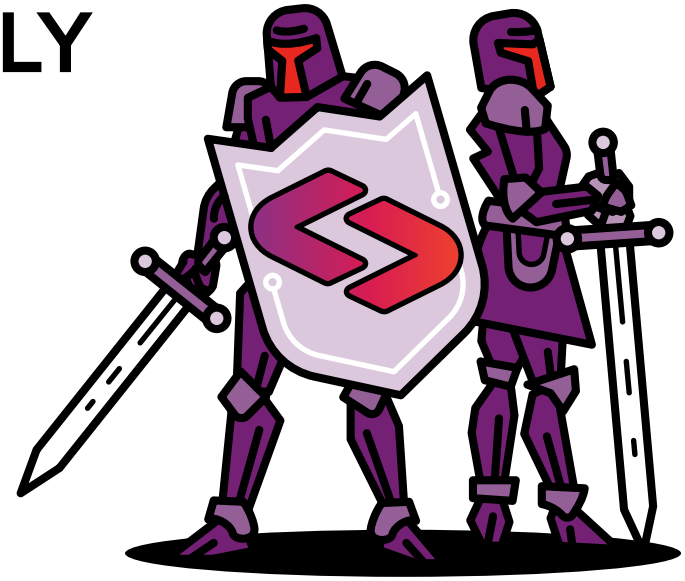
Check to make sure you've addressed the Top 10 AWS observed security issues with your own checklist on the next page...

These ten areas form the foundation of a secure AWS environment. While not exhaustive, they represent the **most frequent** and **high-impact security gaps** found in real-world environments. Prioritize them early in your cloud security roadmap to reduce risk, improve detection, and align with AWS best practices.

Your next step is execution. If your team needs experienced, peer-level help to architect or implement these fixes at scale, we specialize in making environments like yours resilient. Speak directly with one of our lead architects about your security roadmap for the next quarter.

Schedule Time with a Lead AWS Security Architect and...

THRIVE SECURELY



CLOUD SECURITY PARTNERS

contact@cloudsecuritypartners.com

cloud-security-partners

Top 10 AWS Security Issue Checklist

Enable Multi-Factor Authentication

- [ ] On the Root Account
- [ ] On all IAM Accounts
- [ ] Audit IAM Accounts to see if roles can be used instead

Use Federated Identity

- [ ] Migrate any existing IAM users to a federated identity provider

Enable Amazon GuardDuty

- [ ] Enable on all regions
- [ ] Forward alerts to an external S3 bucket
- [ ] Create response playbook

Enhance Logging and Monitoring

- [ ] Enable AWS CloudTrail
- [ ] Enable AWS CloudWatch
- [ ] Enable AWS Config
- [ ] Forward Logs to a central SIEM

Eliminate Overly Permissive IAM Policies

- [ ] Run IAM Access Analyzer
- [ ] Remove any * permissions
- [ ] Analyze cross-account roles

Audit for Public Data Exposure

- [ ] S3 Buckets
  - [ ] Enable S3 Block Public Access feature
- [ ] Databases
- [ ] SNS / SQS
- [ ] EKS

Enable Network Segmentation

- [ ] Verify that NACLs and private subnets are enabled wherever possible

Set up Appropriate Encryption

- [ ] Use CMKs wherever possible
- [ ] Regularly rotate CMKs

Enable Patch Management

- [ ] Publish golden images for all base operating systems and container images
- [ ] Adopt immutable infrastructure principles
- [ ] Tag and version images
- [ ] Integrate security scanning of source code and container images

Audit for Organizational Gaps

- [ ] Set up AWS Organizations to manage multiple accounts under a single security and billing model
- [ ] Apply Service Control Policies for all security controls

We Don't Just Leave You Hanging
After We Find Your Vulnerabilities

Unlike most pentesting companies, we combine experience in both security and engineering, enabling us to both find and remediate vulnerabilities, and prevent them in the future.

CLOUD SECURITY PARTNERS

Assessment Client Satisfaction:

100% vulnerabilities identified

99% client retention rate

50% faster project execution compared to competitors

30% more vulnerabilities identified compared to competitors

80% of vulnerabilities remediated within 30 days of assessment

Trusted By Industry Leaders:

Fannie Mae · RBC · CLOUDFLARE · Capital One · lumos · CURRI

Experience You Can Count On:

5000+ projects delivered

Security Certified and experienced engineers

Senior Engineers assigned to projects

100+ applications reviewed

10+ years of experience

Work with our experienced team of senior engineers to reduce your risk!

CLOUD SECURITY PARTNERS

cloudsecuritypartners.com

cloud-security-partners