

AWS SECURITY

Protecting your AWS environment from ransomware

Table of contents

What is ransomware	3
Protecting your AWS environment from ransomware	3
Cloud security in AWS	4
Top 10 best practices for ransomware protection	4
Use a security framework	5
Patch and harden systems	5
Eliminate long-lived credentials	7
Implement a standard AWS VPC design pattern and a multi-account topology	9
Use immutable infrastructure with no human access	10
Implement centralized logging and monitoring	11
Implement and test backup and restore processes	12
Prepare and exercise your incident response plan	13
Perform self-assessments	13
Automate security guardrails and response actions	14
Additional resources	14
AWS Resources	14
Global Resources	14
Get started with AWS	14

Notices

This document is provided for informational purposes only. It represents the current product offerings and practices from Amazon Web Services (AWS) as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and use of AWS products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create warranties, representations, contractual commitments, conditions, or assurances from AWS, its affiliates, suppliers, or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, agreements between AWS and its customers.



What is ransomware?

Ransomware refers to a business model and a wide range of associated technologies that bad actors use to extort money from entities. The actors use a range of tactics to gain unauthorized access to their victims' data and systems, including exploiting unpatched vulnerabilities, taking advantage of weak or stolen credentials, and using social engineering. They then restrict access to the data and systems, and make a ransom demand for the "safe return" of these digital assets. There are several methods such actors use to restrict or eliminate legitimate access to resources including encryption and deletion, modified access controls, and network-based denial of service attacks. In some cases, even after data access is restored, bad actors have demanded a "second ransom." They promise that this second payment guarantees they will return victims' sensitive data, instead of selling it or publicly releasing it.

Protecting your AWS environment from ransomware

Globally, multiple organizations have issued guidance calling for stronger information security measures against ransomware. For example, the U.S. Department of Homeland Security recently launched a new website to combat the threat of ransomware, saying "As ransomware attacks continue to rise around the world, businesses and other organizations must prioritize their cybersecurity."1 Additionally, Europol published its "Tips and advice to prevent ransomware," and Japan's National center of Incident readiness and Strategy for Cybersecurity (NISC) has published a "call for added attention in strengthening cyber security measures at this time." 3





https://www.europol.europa.eu/cms/sites/default/files/documents/new_infographic - police_ransomware_final.pdf

³ https://www.meti.go.ip/english/press/2022/0301 003.html



Cloud security in AWS

At AWS, security is our top priority. AWS is architected to be one of the most flexible and secure cloud computing environment available today, giving you the ability to control your environment so that it works to meet or exceed the control capabilities of legacy infrastructure options. AWS offers tools and support for compliance, assurance, and monitoring of infrastructure and application changes. It also saves you time by helping you create guardrails to allow innovation and to verify a security baseline without requiring manual security reviews. These measures help your security and IT teams focus more on your core business and less on security by automating incident response for anomalies or deviations from your security baseline. Millions of customers—including the some of the fastest-growing startups, large enterprises, and government agencies—are securely using AWS to lower costs, become more agile, and innovate faster.

Top 10 best practices for ransomware protection

We know that customers are concerned about ransomware. In particular, security teams for critical infrastructure, healthcare organizations, manufacturing, educational institutions, as well as state and local governments are ramping up measures to prevent and mitigate the effects of a ransom event. We want to empower our customers to protect themselves against ransomware by using a range of security capabilities. These include unparalleled visibility into your AWS environment, as well as the ability to update and patch efficiently, to seamlessly and cost-effectively backup your data, and to templatize your environment, enabling a rapid return to a known good state. Please keep in mind that there is no single solution or quick fix to mitigate ransomware. In fact, the mitigations and controls outlined in this document are general security best practices. We hope you find this information helpful and take action.





Use a security framework

While aligning your security program to a security framework may sound rudimentary, it is often overlooked when customers move into the cloud. Large gaps could exist in either the people, process or technology aspect of your cloud security program. Therefore, it is absolutely critical to verify that all areas of your security program have defined controls, responsibilities and mechanisms. We recommend using a security framework like the National Institute of Standards and Technology (NIST) Ransomware Risk Management: A Cybersecurity Framework Profile, which maps security objectives from the NIST Cyber Security Framework (CSF) to help manage and reduce cybersecurity risks. NIST CSF is a voluntary, risk-based, and outcome-focused framework designed to help you establish a foundational set of security activities organized around five functions—identify, protect, detect, respond, and recover—to improve the security, risk management, and resilience of your organization. The CSF has seen endorsements by governments and industries worldwide as a recommended baseline for organizations of all types and sizes. Sectors including healthcare, financial services, and manufacturing use the NIST CSF, and the program encourages international participation at all stages in the framework's development and evolution.⁴

Ransomware Risk Management on AWS Using the NIST Cyber Security
Framework (CSF), is a guide designed to help commercial and public sector
entities of various sizes throughout the world align with the CSF by using
AWS services and resources.

Patch and harden systems

Unpatched vulnerabilities are among the most common ways that traditional ransomware enters an organization's environment. By rapidly identifying and patching vulnerabilities, organizations can reduce their exposure to ransomware events and limit the ways malware can get in.





Using Amazon Inspector, you can automate vulnerability management with continual scans of AWS resources, including Amazon Elastic Compute Cloud (EC2) and container workloads, for software vulnerabilities and unintended network exposure. Inspector calculates a highly contextualized risk score for each finding by correlating common vulnerabilities and exposures (CVE) information with factors such as network access and exploitability. Once the vulnerabilities have been identified, patching tools such as AWS Systems Manager Patch Manager can help you deploy operating system and software patches automatically across large groups of instances to close exposures. You can use endpoint detection and response software on your EC2 instances for further protection. The AWS Marketplace has several third-party endpoint security software solutions available. These solutions combine several capabilities that can help prevent and/or detect security events at the operating system layer.

You can apply hardening measures to your systems including applying <u>CIS Benchmarks</u> to the operating systems and software you're running. CIS Benchmarks are a set of hardening guidelines curated by a global community of cybersecurity experts that help you safeguard systems, software, and networks against security issues and events. In addition, there are <u>CIS Hardened Images</u> available for you to run, at a cost, directly from the AWS Marketplace.

Customers can avoid traditional ransomware events by utilizing managed services, where AWS handles the patching on the customer's behalf. AWS-managed services include Amazon API Gateway, Amazon RDS, Amazon DynamoDB, and AWS Lambda. AWS manages the underlying security of the hosts running these services, including patching. The operating systems of these managed services are not accessible through standard means, but rather interfaces such as public APIs or SQL connections. In addition, many of the AWS data store and storage services have advanced capabilities that can help prevent accidental or malicious data deletion. This includes AWS Backup Vault Lock, which provides write-once-read-many (WORM) on your AWS Backup Vault. Amazon S3 Object Lock and S3 Glacier Vault Lock provide WORM capabilities for data and archive objects in S3.5 DynamoDB has point-in-time-recovery (PITR) which enables you to back up your table data automatically with per-second granularity, so that you can restore to a given second in the preceding 35 days. Many AWS services provide advanced capabilities that can be used for further protection.



⁵ Please note, you should verify your data privacy and compliance policies before utilizing features like Object Lock and Vault Lock to verify that you are able to maintain compliance with applicable data privacy and compliance regulations

Eliminate long-lived credentials

One of the most common initial issues for ransomware events experienced by customers is related to unintended disclosure of static IAM access keys. Access keys can be inadvertently uploaded to code repositories or publicly disclosed through other means.

Given that many of these specific security events arise from disclosed long-lived credentials, particularly IAM access keys, we recommend eliminating static credentials as much as possible. Instead, you can use federation for human access into AWS, IAM roles for workload access, and IAM Roles Anywhere for hybrid machine access. Consider taking the following steps as you work toward eliminating long-lived credentials in your environment:

- 1. Create an inventory across all of your AWS accounts. Track IAM users with static access keys. This should include the following details:
- a. Use the <u>credential report</u> to determine when the credentials were last rotated and used.
- Review attached policies to verify least privilege access, including removing wild cards from all policies and specifying actions and resources instead.
- c. Remove unused users, roles, and credentials. IAM provides <u>last accessed</u> <u>information</u> to help you identify the users, roles, permissions, and policies that you no longer need so that you can remove them.
- 2. Re-architect the access that currently requires long-lived credentials to take advantage of temporary role-based access, such as the IAM role. Some examples and best practices for using IAM roles include the following:
- a. Require human users to use federation with an identity provider to access AWS using temporary credentials. You can use an identity provider for your human users to provide federated access to AWS accounts by assuming roles, which provide temporary credentials. For centralized

- access management, we recommend that you use <u>AWS IAM Identity Center</u> (successor to AWS Single Sign-On) to manage access to your accounts and permissions within those accounts. You can manage your user identities with IAM Identity Center, or manage access permissions for user identities in IAM Identity Center from an external identity provider.
- b. Require AWS workloads to use temporary credentials with IAM roles for access within AWS. A workload is a collection of resources and code that delivers business value, such as an application or backend process. Your workload can have applications, operational tools, and components that require an identity to make requests to AWS services, such as requests to read data. These identities include machines running in your AWS environments, such as Amazon EC2 instances or AWS Lambda functions. You can also manage machine identities for external parties who need access. To give access to machine identities, you can use IAM roles. IAM roles have specific permissions and provide a way to access AWS by relying on temporary security credentials with a role session.
- c. You can use <u>AWS Identity and Access Management Roles Anywhere</u> to obtain <u>temporary security credentials in IAM</u> for workloads such as servers, containers, and applications that run outside of AWS. Your workloads can use the same <u>IAM policies</u> and <u>IAM roles</u> that you use with AWS applications to access AWS resources. To use IAM Roles Anywhere, your workloads must use X.509 certificates issued by your <u>certificate authority (CA)</u>. You can register the CA with IAM Roles Anywhere as a trust anchor to establish trust between your public-key infrastructure (PKI) and IAM Roles Anywhere. You can also use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a CA and then use that to establish trust with IAM Roles Anywhere. ACM PCA is a managed private CA service for managing your CA infrastructure and your private certificates. For more information, see <u>What is AWS Certificate Manager</u>.



3. Rotate the credentials and apply multi-factor authentication (MFA) to the user until you are able to re-architect, per item 2 above.

For scenarios where you need IAM users with interactive access and static access keys, we recommend that you rotate access keys on a regular, frequent cadence. Regularly rotating long-term credentials helps you familiarize yourself with the process, which is useful in case you are ever in a situation where you must rotate credentials, such as when an employee leaves your company. For scenarios in which re-architecting is not feasible in a short time frame, we recommend that you require MFA for additional security. With MFA, users have a device that generates a response to an authentication challenge. Consider that you may want to require MFA-protected API access for sensitive actions.

Achieving <u>least privilege</u> is a continuous cycle to grant the right fine-grained permissions as your requirements evolve. The <u>AWS IAM Access Analyzer</u> analyzes the services and actions that your IAM roles use, and then generates a fine-grained policy that you can use. After you test each generated policy, you can deploy the policy to your production environment. This verifies that you grant only the required permissions to your workloads. Authoring IAM policies in the AWS console provides policy validation to help you author and validate secure and functional policies with more than 100 policy checks. For more information and to help secure your AWS resources, follow these <u>best practices for AWS Identity and Access Management (IAM)</u>.



Implement a standard AWS VPC design pattern and a multi-account topology

The careful planning and management of your network and multi-account design forms the foundation of how you provide isolation and boundaries for resources within your workload. AWS recommends building a standard VPC design that will meet the networking requirements for around 80% of your applications and use cases, minimizing "snowflake" VPC structures across your AWS accounts. For example, use the same number of Availability Zones (AZs) and public and private subnets in each AZ with common NACLs, ingress/egress routing, and additional security controls, as needed. When you use a standard VPC design, you will be able to reason about VPC security controls, which can provide strong segmentation and isolation to limit and control traffic, reducing ransomware's ability to spread across an environment. In addition, AWS offers accounts, which provide security, access, and billing boundaries for your AWS resources. AWS accounts enable you to achieve resource independence and isolation. The use of multiple AWS accounts plays an important role in how you meet your security requirements, as discussed in the **Benefits of using multiple** AWS accounts section of the Organizing Your AWS Environment Using Multiple Accounts whitepaper.

You can use Route 53 Resolver DNS Firewall to filter and regulate your VPC outbound DNS traffic based on managed domain lists. These managed domain lists are updated automatically with new vulnerabilities and emerging threats. AWS Network Firewall also supports AWS managed threat signatures to detect threats and block attacks against known vulnerabilities so you can stay up to date on the latest security threats without writing and maintaining your own rules. You can enable stateful managed rules for intrusion detection and prevention signatures that help protect against threats such as malware, botnets, web attacks, and emerging events. You can select managed rule groups to add to your AWS Network Firewall policies, or you can copy and modify rule groups to meet your specific needs.

AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for a variety of protections, including AWS WAF, AWS Shield, Amazon VPC security groups, AWS Network Firewall, and Amazon Route 53 Resolver DNS firewall. With Firewall Manager, you set up your protections just once and the service automatically applies them across your accounts and resources, even as you add new accounts and resources.



Use immutable infrastructure with no human access

You can adopt immutable infrastructure practices with no human access to reduce the risk of mishandling, modification, and human error when it comes to handling your critical systems and data. This approach includes replacing your infrastructure rather than patching in place. You should apply all configuration updates, including hardening and installing security software such as endpoint detection and protection software, before launching the system in production. You should also centralize logs and metrics, off the local system, for troubleshooting. This strategy verifies that no changes can reduce the effectiveness of the systems' hardening, including the disabling of security software or critical security configurations on the host. When patches are released, you can use services like EC2 Image Builder to create an AMI pipeline, which can be used to roll out patches with new versions of the AMI. This strategy aligns with infrastructure as code best practices and provides a secure, auditable trail for your compute resources. You will be able to version control your infrastructure, and handling failure will be a routine and continuous way of doing business.

Obtaining a fully immutable infrastructure can be challenging for some customers. Another strategy to secure infrastructure is to use tools to make changes to instances instead of allowing manual changes via direct access or a bastion host. This can be achieved using AWS Systems Manager Automation, which uses automation documents that contain steps you use to perform tasks. These documents can be stored in source control, be peerreviewed before running, and tested thoroughly to minimize risk compared to interactive access. This allows you to better protect your data and reduce the risk of unauthorized access by ransomware.





Implement centralized logging and monitoring

Security operations teams rely on the collection of logs and the use of search tools to discover potential events of interest, which might indicate unauthorized activity or unintentional change. A current recommendation for building a mature security operations team is to deeply integrate the flow of security events and findings into a notification and workflow system such as a ticketing system, a bug/issue system, or other security information and event management (SIEM) system. This recommendation applies not only to security events generated from log messages depicting user activity or network events, but also from changes detected in the infrastructure itself.

Responding to security events requires that you are able to detect the threat's existence in the first place. If ransomware is detected by a ransom demand popping up on the computer screen, it is usually too late. Early detection of anomalous user behavior or network activity is key to thwarting ransomware threats and initiating incident response processes. With an understanding of what "normal" looks like in your AWS environment, security alerts can be automatically configured to send notifications when malicious or unauthorized behaviors are identified.

In AWS, Amazon GuardDuty is a threat detection service that provides you with an accurate and simple way to continuously monitor and protect AWS accounts and workloads. AWS CloudTrail logs provide event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. VPC flow logs enable you to capture information about the IP traffic going to and from network interfaces in your VPC. AWS Security Hub can assess your high priority security alerts and security posture across your accounts and regions. This includes AWS security services such as AWS Services GuardDuty, AWS Config, Amazon Inspector, Amazon Macie, AWS Firewall Manager, and a significant number of third-party security products. Security Hub also generates its own findings by running automated and continuous checks against the rules in a set of supported security standards. We recommend enabling the AWS Foundational Security Best Practices checks in Security Hub, as a minimum. This standard allows you to continuously evaluate your AWS accounts and workloads to quickly identify areas of deviation from current security best practices across many AWS services. It provides actionable and prescriptive guidance on how to improve and maintain your organization's security posture.



Considerations for storing data backups

Organizations that can effectively back up data to a specific point in time and rapidly restore it to production environments significantly reduce the impact of ransomware. Some newer ransomware variants are designed to search for stored backups and encrypt or delete them to disrupt recovery efforts. Still other variants will remain dormant to not only become incorporated into backups, but also until prior clean backups are no longer available, thereby impacting the recovery attempt. Multiple copies of backups should exist and they should be stored in a logically isolated and immutable format to prevent tampering. Create a backup plan that includes considerations such as:

- Recovery point objectives (RPOs) These allow you to determine how
 frequently backups should be performed so the data is current enough
 to be useful if it's to be placed in an active production environment.
- Recovery time objectives (RTOs) Establish how quickly backed-up
 information can be retrieved and put into the production environment to
 resume normal operations. AWS environments, resources, databases, code,
 and other data sources will likely have different RPOs and RTOs based on
 their priority and criticality to the organization's operations.
- Backups To protect against a security event that impacts stored backups in the source account, AWS Backup supports cross-account backups and the ability to centrally define backup policies for Accounts in the Organization using the Backup Admin Account. Also, AWS Backup Vault Lock enforces a write-once, read-many (WORM) backup to help protect backups (recovery points) in your backup vaults from inadvertent or malicious actions. You can copy backups to a known logically isolated destination account in the organization, and you can restore from the destination account or, alternatively, to the third account. This gives you an additional layer of protection should the source account experience disruption from accidental or malicious deletion, disasters, or ransomware.



^{*}Please note, you should verify your data privacy and compliance policies before utilizing features like Object Lock and Vault Lock to verify that you are able to maintain compliance with applicable data privacy and compliance regulations.

Implement and test backup and restore processes

It is critical to create backups of enterprise data in advance of any disruptive-security or operations event. It is also critical to protect these backups and other potentially important data against alteration. So, it is key to identify your important and sensitive data upfront to be able to capture a known good backup. You should start by creating a data classification strategy and use AWS tags to identify and classify your data across AWS. As a next step, you should map your data classification to specific Disaster Recovery needs. You can then determine what must be recovered and how quickly (Recovery Time Objective - RTO), as well as how recent the recovered data must be (Recovery Point Objective - RPO).

You can use services such as AWS Backup and AWS Elastic Disaster Recovery to build and deploy highly available and resilient applications.

Using AWS Backup, you can centrally configure backup policies and monitor backup activity for AWS resources, such as Amazon Elastic Block Store (Amazon EBS) volumes, Amazon Relational Database Service (Amazon RDS) databases, Amazon DynamoDB tables, Amazon Elastic File System (Amazon EFS), and AWS Storage Gateway volumes. If a ransomware event occurs, you can use Elastic Disaster Recovery to restore your systems to the last known good backup.

Defining and exercising your recovery strategy will streamline a recovery process by being prepared to make data stored in a backup readily available in production environments. Regular testing of your restore processes will lead to improved response and assurances that the approach is effective.



Prepare and exercise your incident response plan

While AWS provides capabilities to automate policies and procedures in a policy-driven manner to improve detection times, shorten response times, and reduce attack surface, it is the customers' responsibility to develop policies and procedures to respond to security events.

We highly recommend simulating incident response scenarios before experiencing a potential security event, so that you can validate that your existing processes are effective and efficient when responding to an actual event. Using this approach, you can determine if you can effectively recover and respond to incidents when they occur. AWS Professional Services, for example, offers AWS Security Incident Response Simulations, which are a collaborative learning exercise that tests your team's incident response scenario in a gamified, risk-free environment.

For additional detailed guidance around building an incident response program in AWS please review the <u>AWS Incident Response whitepaper</u>. In addition, the <u>Customer Incident Response Team</u> (<u>CIRT</u>) has released a <u>customer playbook framework</u> that includes detailed guidance for handling specific security events in AWS.

Perform self-assessments

AWS has developed AWS Well-Architected to help architects build secure, high-performing, resilient, and efficient infrastructure in AWS for a variety of applications and workloads. The security pillar focuses on protecting information and systems. The <u>AWS Well-Architected Tool</u>, available at no additional cost in the <u>AWS Management Console</u>, provides a mechanism for regularly evaluating workloads, identifying high-risk issues, and recording improvements.

AWS Security Hub Foundation Security Best practices standard is a set of controls that detect when your deployed accounts and resources deviate from security best practices. This standard allows you to continuously evaluate your AWS accounts and workloads to quickly identify areas of deviation from best practices. It provides actionable and prescriptive guidance on how to improve and maintain your organization's security posture. The standard includes best practices across multiple AWS services and are managed by the internal AWS Security community. It is updated regularly with additional checks.





Automate security guardrails and response actions

One significant scaling mechanism for security teams includes the implementation of automated remediation for a subset of security findings. Automated remediation includes using tools such as Amazon EventBridge and AWS Lambda to script remediations, such as changing insecure configuration back to the secure standard you expect. This will significantly drive down the number of security findings in your environment, lower mean time to repair (MTTR), and allow your security practitioners to focus on high value work. We recommend automation to remediate as much as possible, then where you do not want to automate, you can gather as much info and correlate it for your IT team to make faster decisions. To learn more about automating security responses on AWS and download sample code, please visit AWS Solutions.

Visit Nomoreransom.org

Nomoreransom.org is a collaboration between law enforcement, IT security companies, and international governments with a goal of helping victims of ransomware retrieve their encrypted data without having to pay the ransom.

Since it is simpler to avoid the threat than to fight against it once the system is affected, the project aims to educate users about how ransomware works and what countermeasures can be taken to effectively prevent infection. This initiative is open to other public and private parties.



Additional Resources

AWS Resources

AWS Ransomware page

AWS Security Resources Hub

Aligning to the NIST CSF in the AWS

AWS Well-Architected Framework

- Security Pillar

Building a Threat Detection Strategy in AWS

AWS Security Incident Response Guide

AWS Compliance

Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF)

Zero Trust on AWS

FBI IC3 – File a complaint

U.S. Federal Government Resources

ENISA Threat Landscape 2021

US CISA / Multi-state ISAC Ransomware Guide

Global resources (from NIST CSF)

Get started on AWS

Learn AWS fundamentals, connect with the AWS community, and advance your knowledge with certifications. Register for your free account now.

Sign up >

Have questions or need help?

No matter where you are in your journey to AWS, we are here to help and answer any and all of your questions about AWS.

Contact us >

