Securing your AWS Cloud environment from ransomware

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 any 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 any 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, any agreement between AWS and its customers.

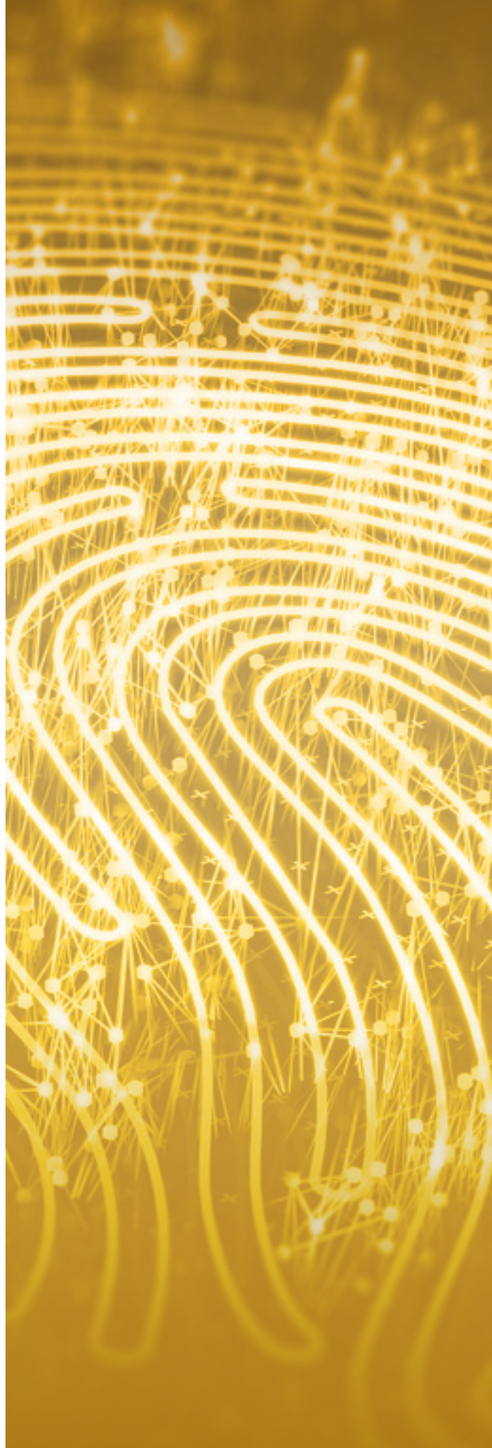
Table of contents

Ransomware:
A formidable threat

Since the first recorded ransomware attack in 1989 called PC Cyborg, ransomware has become a prominent cyber threat featuring dangers that sound more like the stuff of comic books continuing to attract worldwide attention (CryptoLocker [2014], Petya [2016], WannaCry [2017], NotPetya [2017], and Ryuk [2019]).

Ransomware attacks are costing governments, nonprofits, and businesses billions of dollars, and interrupting operations. Attacks like NotPetya forced shipping giant Maersk to reinstall 4,000 servers and 45,000 PCs for $300M due to "serious business interruption." The ransomware attack on the City of Baltimore cost over $18M, and local governments from Riviera Beach and Lake City, Florida will pay hackers $1M combined to hopefully get its systems and data back.

Even though it is difficult to estimate the frequency of ransomware attacks due to an unknown number of unreported incidents and thwarted attacks, the U.S. Federal Bureau of Investigation (FBI) anticipates the threat to become "more targeted, sophisticated, and costly" in the foreseeable future. These warnings reach beyond U.S. borders, with Europol also calling ransomware the "most widespread and financially damaging form of cyberattack."



What is ransomware?

Ransomware is malicious code designed by cyber criminals to gain unauthorized access to systems and data and encrypt that data to block access by legitimate users. Once ransomware has locked users out of their systems and encrypted their sensitive data, cyber criminals demand a ransom before providing a decryption key to unlock the blocked systems and decrypt data. In theory, if the ransom is paid within the allotted time, systems and data are decrypted and made available once again and normal operations continue. However, if the ransom is not satisfied, organizations risk permanent destruction or public-facing data leaks controlled by the attacker.

Bitcoin, a popular cryptocurrency, has been an ideal method of making ransom payments because it lacks oversight by any governing body and transactions are kept anonymous.

Ransomware does not care

Most ransomware attacks are opportunistic in nature, meaning that ransomware indiscriminately infects any accessible networks through human and/or machine vectors. It does not matter what industry or geography you are in, as virtually every industry globally has an example of a ransomware incident. However, there is a growing trend amongst bad actors to target certain industries where the probability of successful entry and payout is high. Security teams for education institutions, state and local governments, and healthcare organizations are ramping up measures to keep their data safe from an increase in ransomware attacks.

Bad actors understand how to identify weak spots in industry verticals. For example, many education and government organizations are vulnerable due to a combination of shrinking budgets, perceived gaps in security resources, and legacy IT systems with unpatched vulnerabilities. Similarly, ransomware may target industries with intolerance for downtime, like hospitals, in hopes of increasing the probability of payout.

RANSOMWARE: A FORMIDABLE THREAT

As long as cyber criminals continue to find ways to profit from ransomware, many organizational leaders say, “it’s not a matter of if but when an attack will occur.”

Why is ransomware effective?

- Security awareness amongst employees is low
- Organizations are not backing up data
- Attacks require little skill and result in significant payouts
- Organizations take weeks to patch critical common vulnerabilities and exposures (CVE)
- Overburdened technical staff cannot address or anticipate all security gaps
- Multiple vectors or channels are being used in a single attack

To pay or not pay?

Active debates exist among cyber security professionals regarding the decision to pay or deny ransom payments. Many experts, including the FBI, advise organizations not to pay the ransom, arguing that paying doesn’t guarantee that locked systems and data will be made available again and any payments to cyber criminals will only continue to motivate nefarious behaviors.

Even though system and data access is not guaranteed after paying the ransom, some organizations take a calculated risk to pay in hopes of quickly resuming normal operations. By doing so, they hope to reduce potential ancillary costs of attacks, including lost productivity, decreased revenue over time, exposure of sensitive data[1], and reputational damage.

The ransomware threat is serious but smart preparation and ongoing vigilance are effective counters against ransomware. The full armor of data security includes both human and technical factors but there are features of the AWS Cloud that helps to mitigate against ransomware attacks.

AWS is committed to providing you with tools, best practices, and services to help with high availability, security, and resiliency to address bad actors on the internet.

[1] Including Personally Identifiable Information (PII) and Protected Health Information (PHI).

AWS is purpose-built for security

AWS protects millions of active customers around the world who represent diverse industries with a range of use cases including large enterprises, startups, educational institutions, and government organizations.
The scale and global reach of these customers gives us broad visibility and deep perspective on cloud security, which we rapidly reinvest back into our infrastructure and services. Security at AWS starts with our core infrastructure, which is custom-built for the cloud and designed to meet the most stringent security and regulatory requirements in the world.

Inherit physical, environmental, and security controls for IT infrastructure

Before migrating to the AWS Cloud, customers may have been responsible for the entire control set in their security compliance and auditing program. With AWS, you can inherit controls from AWS compliance programs, allowing you to focus on securing workloads and the data you put in the cloud. AWS helps relieve your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

AWS IS PURPOSE-BUILT FOR SECURITY

Securing systems and data on AWS is a shared responsibility

When you deploy systems in the AWS Cloud, AWS helps by sharing the security responsibilities with you. AWS engineers the underlying cloud infrastructure using secure design principles and customers can implement their own security architecture for workloads deployed on AWS.

AWS is responsible for protecting the infrastructure that runs all of the services offered on the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

The AWS Cloud services that a customer selects determine the customer's responsibilities. This determines the amount of configuration work the customer must perform as part of their security responsibilities. Customers are responsible for managing their data (including encryption options), classifying their assets, and using AWS Identity Access Management (IAM) to apply the appropriate permissions.

Customer

Responsibility for security 'in' the cloud

- Customer Data
- Platform, Applications, Identity & Access Management
- Operating System, Network & Firewall Configuration
- Client-side Data Encryption & Data Integrity Authentication
- Server-side Encryption (File System and/or Data)
- Networking Traffic Protection (Encryption, Integrity, Identity)

aws

Responsibility for security 'of' the cloud

- Software
- Compute | Storage | Database | Networking
- Hardware / AWS Global Infrastructure
- Regions | Availability Zones | Edge Locations

Before ransomware strikes:
Network hardening and prevention

Adopt a security framework

Implementing a security framework like the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) will help to set standards for managing and reducing cybersecurity risks for your organization. It's a voluntary, risk-based, outcome-focused framework designed to help you establish a foundational set of security activities organized around five functions—identify, protect, detect, respond, recover—to improve the security, risk management, and resilience of your organization.

The CSF was originally intended for the critical infrastructure sector but has seen endorsements by governments and industries worldwide as a recommended baseline for organizations of all types and sizes. Sectors as diverse as healthcare, financial services, and manufacturing use the NIST CSF, and the list of early global adopters includes Japan, Israel, the UK, and Uruguay.

NIST Cybersecurity Framework

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Assessment Strategy
- Supply Chain Risk Management

Protect

- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

- Recovery Planning
- Improvements
- Communications

Align to the framework

The guide, NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud, is designed to help commercial and public sector entities of any size and in any part of the world align with the CSF by using AWS services and resources.

Deploy secure and compliant AWS infrastructure

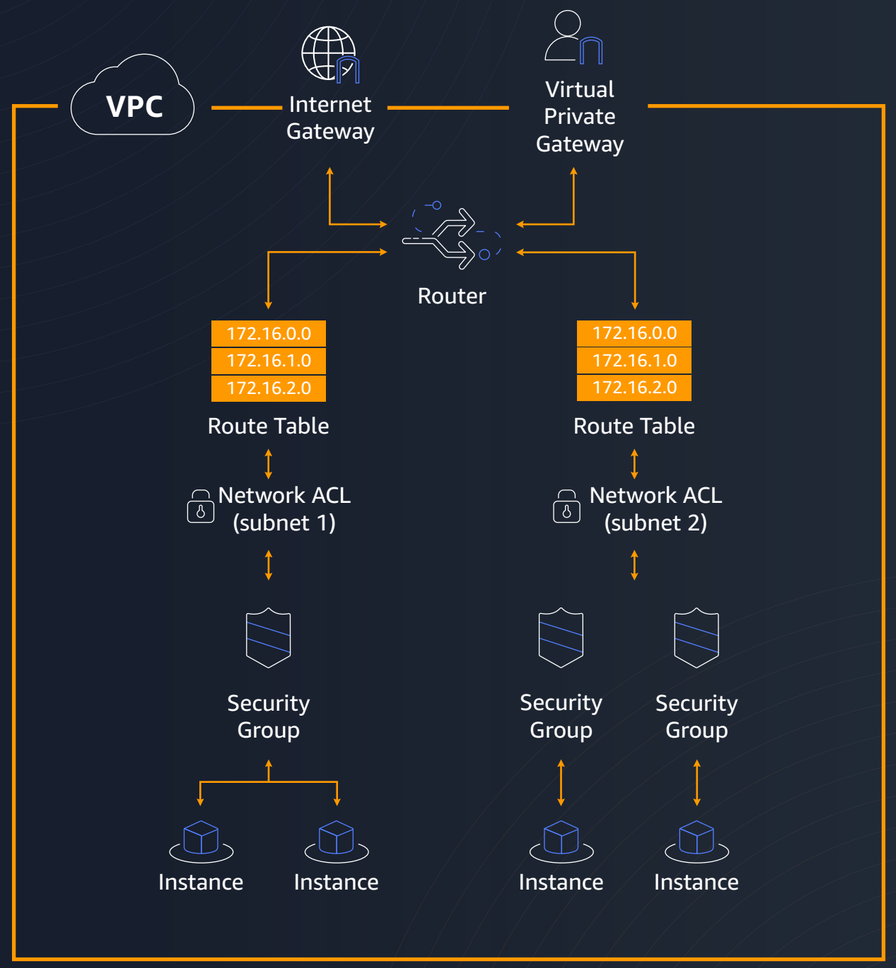
Customers can automatically deploy and configure secure and compliant AWS Cloud architectures using the National Institute of Standards and Technology (NIST) Quick Start template to reduce hundreds of manual procedures to just a few steps, so you can build your production environment quickly and start using it immediately.

BEFORE RANSOMWARE STRIKES

Segment Amazon Virtual Private Clouds (Amazon VPCs)

Network segmentation mitigates local traffic congestion and also improves security by allocating only the resources specific to the user, which significantly diminishes ways for attackers to move laterally within the network.

You can provision logically isolated sections of the AWS Cloud where you can launch AWS resources in virtual networks that you define. Segmenting Amazon VPCs into isolated components, either by security groups and network access control lists (ACL) so that only necessary traffic is available can reduce ransomware's ability to spread indiscriminately across AWS environments.



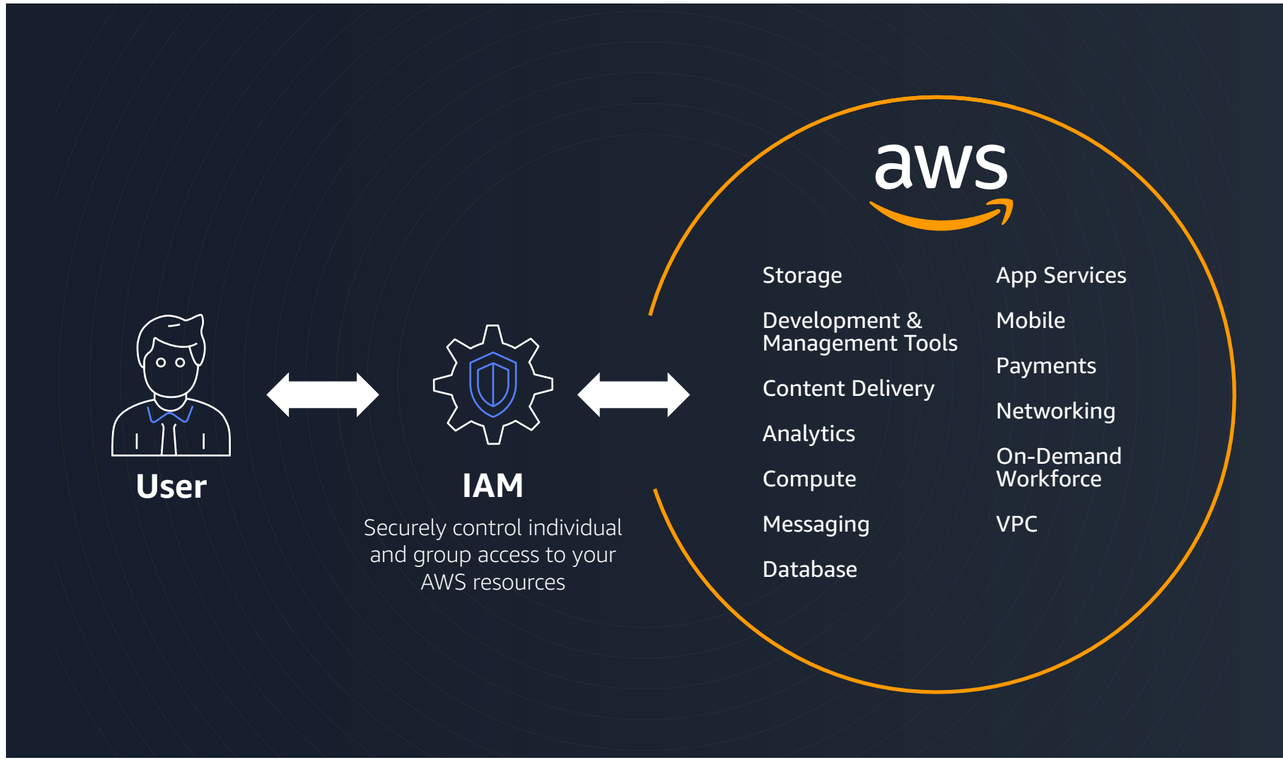
Manage users' access to critical systems and data

Setting strong IAM policies that determine what systems and data are available to individual users, or groups of users, and under which conditions that data is accessible, can limit how widely ransomware is able to access the environment.

At the user level, AWS allows you to define fine-grained access control provisions by defining which users or roles have access to certain systems and data. These controls determine which actions can be performed on a given resource in AWS, allowing users privileges on a "need-to-know" basis based on business needs and job responsibilities.

AWS IAM enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

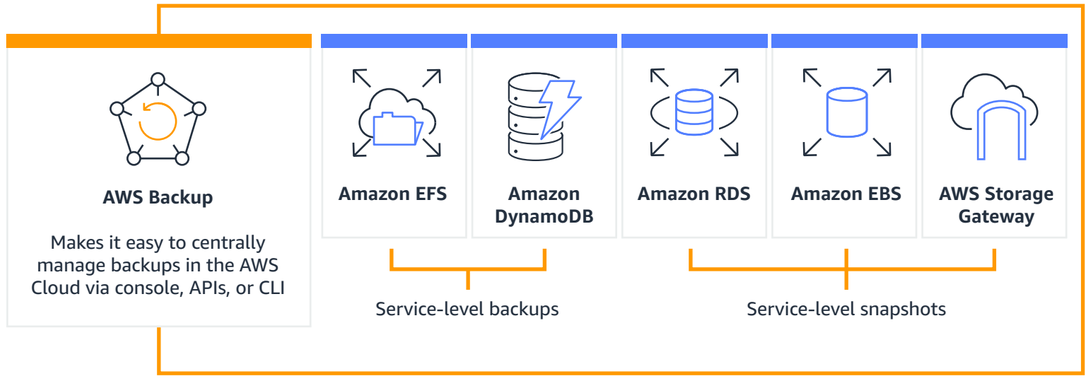
As a best practice, AWS recommends following the principle of least privilege for internal and external network users. For example, some strains of ransomware are designed to use a system administrator account to perform their operations. With this type of ransomware, decreasing user account privileges and terminating all default system administrator accounts can create an extra security roadblock.



Define, test, and perform data backup and recovery plans

Backups are critical in mitigating the impact ransomware can have on your organization. The most effective deterrent to ransomware is to regularly back up and then verify your systems. By defining your data backup and recovery strategy, you help protect against deletion or destruction of data during a ransomware attack by being prepared to make data stored in a backup readily available in production environments. Regular testing of defined backup and recovery plans in a game day scenario can lead to improved response and assurances that the approach is effective.

Customers can use services such as AWS Backup and CloudEndure 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 ransomware strikes, CloudEndure Disaster Recovery can spin up the most up-to-date version of your machines within a few clicks to restore system and data availability to users.



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 ransomware's impact.

Some newer, smarter ransomware variants are designed to search for stored backups and encrypt or delete them to disrupt recovery efforts. Multiple copies of backups should exist and they should be stored in isolated, offline locations.

- Including **recovery point objectives (RPOs)** 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.

- Similarly, the recovery plan should have **recovery time objectives (RTOs)** that 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 its priority and criticality to the organization's operations.

BEFORE RANSOMWARE STRIKES

Find and patch vulnerabilities within AWS workloads

Unpatched vulnerabilities are one of the most common ways ransomware infects an organization's environment. By rapidly identifying and patching vulnerabilities, organizations can reduce their exposure to ransomware threats by limiting the ways it can get in.

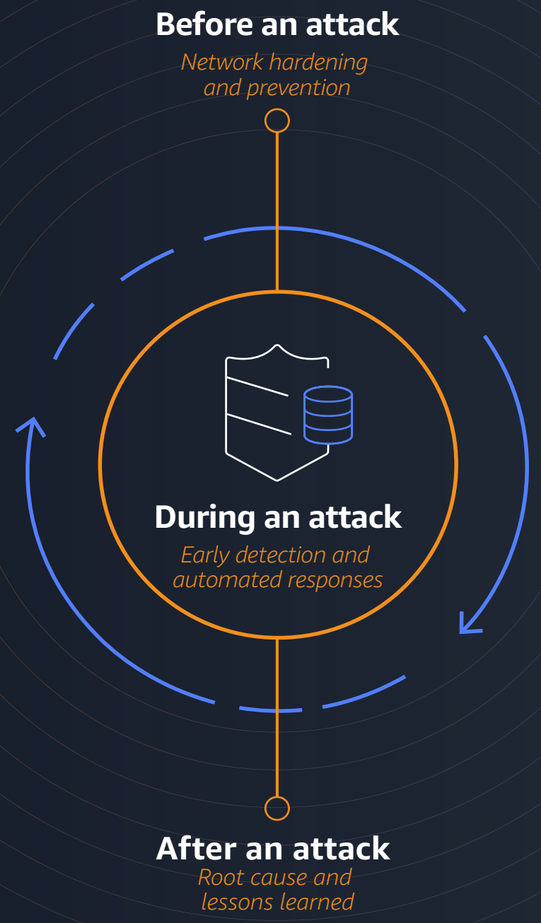
Using Amazon Inspector, you can search AWS environments for CVEs, assess your instances against security benchmarks, and fully automate notifying security and IT engineers when findings are present. Once the vulnerabilities have been identified, patching tools such as AWS Systems Manager Patch Manager can help you deploy operating system and software patches automatically across large groups of instances to close exposures.

During an incident:
Early detection and automated responses

Automate security incident detection and alerting

Responding to any cyber incident requires that you're 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 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 the AWS environment, security alerts can be automatically configured to send notifications when malicious or unauthorized behaviors are present.

To help identify such threats, Amazon GuardDuty, a threat detection service, continuously monitors and correlates activity within your AWS environment for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats.



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 cyber incidents.

During an incident, your incident response teams must have access to the environments and resources involved in the incident. Identify and discuss the AWS account strategy and cloud identity strategy with your organization's cloud architects to understand what authentication and authorization methods are configured.

By simulating incident response scenarios before a real attack, you can validate that the controls and processes you have put in place will react as expected. Using this approach, you can determine if you can effectively recover and respond to incidents when they occur.

DURING AN INCIDENT

Report ransomware to authorities

The FBI encourages organizations to report ransomware incidents to law enforcement. The Internet Crime Complaint Center (IC3) accepts online internet crime complaints from either the actual victim or from a third party to the complainant and will work with them to determine the best course of action going forward.

Be prepared to share:

- Victim's name, address, telephone, and email
- Financial transaction information (account information, transaction date and amount, recipient details)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- Email header(s)
- Any other relevant information you believe is necessary to support your complaint

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 much easier 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.

Recovering from ransomware:
Root cause and lessons learned

Perform root cause analysis

In most cases, your existing forensics tools will work in the AWS environment. Forensic teams will benefit from the automated deployment of tools across AWS Regions and the ability to collect large volumes of data quickly with low friction using the same robust, scalable services their business-critical applications are built on.

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to conduct faster and more efficient security investigations.

Update security program with lessons learned

Documenting and cycling lessons learned during simulations and live incidents back into “new normal” processes and procedures allows organizations to better understand how they were breached – such as where they were vulnerable, where automation may have failed, or where visibility was lacking – and the opportunity to strengthen their overall security posture.

Conclusion

Ransomware is evolving, but so can your security awareness and preparedness. Government agencies, nonprofits, and businesses around the world trust AWS to power their infrastructure and keep their systems and data secure. Using the AWS services and best practices shared in this guidebook, you can take proactive measures to reduce the likelihood and impact of ransomware in your AWS environments.

Resources

AWS Resources

AWS Cloud Security Resources Hub

Aligning to the NIST CSF in the AWS Cloud

AWS Well-Architected Framework – Security Pillar

Building a Threat Detection Strategy in AWS

AWS Security Incident Response Guide

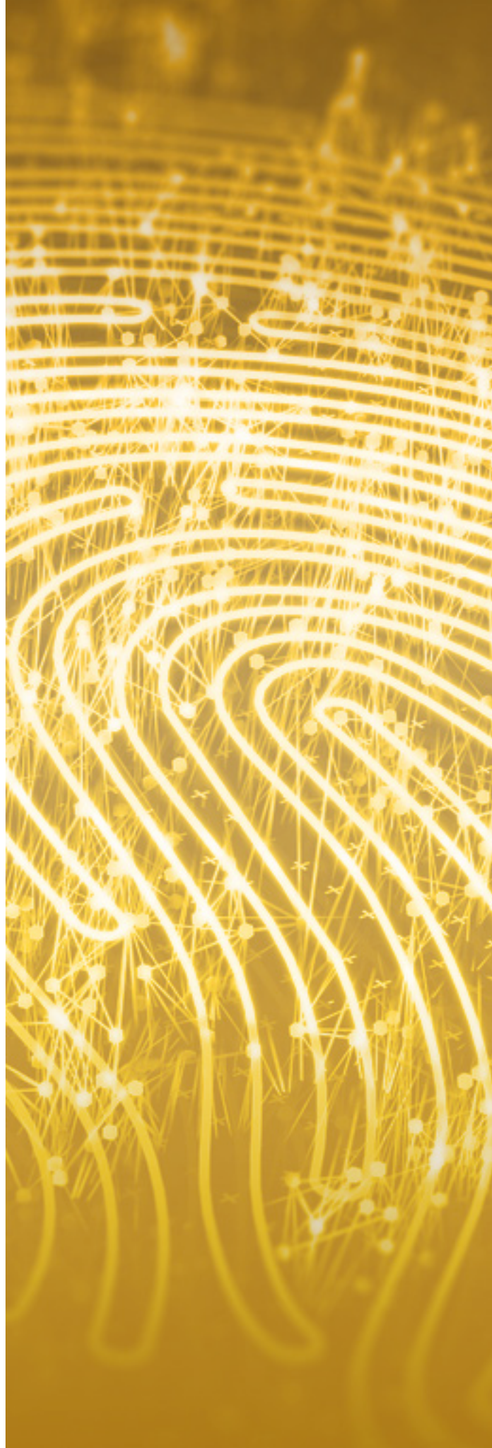
AWS GovCloud (US) Regions

AWS Compliance

U.S. Federal Government Resources

FBI IC3 – File a complaint

The Cybersecurity and Infrastructure Security Agency (CISA) publications



Get started with 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 the cloud, we are here to help
and answer any and all of your questions about AWS.

CONTACT US


aws