Say yes to being prepared for ransomware

Protecting your cloud environment from threats with services from AWS and AWS Partners

Table of contents

Introduction

Are you confident in your organization's ability to prevent ransomware? Smart preparation and ongoing vigilance are effective counters against ransomware. And you have allies in ransomware defense. Amazon Web Services (AWS) Cloud and AWS Partners have a host of services and solutions that help prevent, protect against, mitigate, and recover from ransomware attacks.

Ransomware
malicious software designed to block access to a computer system and/or data until a sum of money is paid.

According to Gartner, by 2025, ransomware attacks are expected to increase by 700% and at least 75% of IT organizations will face one or more attacks.

Gartner, "Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware", January 2021.

How prepared are you for ransomware?

So, how prepared are you for a ransomware attack? To find out, ask yourself these questions:

When it comes to responding to a ransomware attack, do you have:

- An incident response plan?
- Data backup and restoration strategy?
- List of key contacts?

As you protect your company from attacks, do you:

- Use antivirus software at all times?
- Keep computers fully patched?
- Block access to ransomware sites?
- Allow only authorized apps?
- Restrict personally owned devices on work networks?
- Use standard user accounts versus accounts with administrative privileges?
- Avoid using personal apps like email, chat, and social media from work computers?
- Run an antivirus scan before opening external files?

If you answered no to even one of these questions, you could be at risk for a ransomware attack. That might come as a shock to you, because you might have thought that you are protected. Most likely, the fact that you probably answered yes to at least a few means you have a good base from which to start.

The good news is that AWS and AWS Partners offer services that can help you say no to ransomware instead of no to these questions. From aligning with the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) to following the recommendations in the White House Executive Order, these solutions help you be prepared for ransomware.

On May 12, 2021, U.S. President Joe Biden issued an executive order on improving the nation's cybersecurity, asking the private sector to partner with the federal government to foster a more secure cyberspace. Less than a month later, on June 3, Anne Neuberger, cybersecurity adviser at the National Security Council, wrote an open letter urging organizations to take the crucial steps needed to protect their organizations against ransomware.

AWS provides a foundation for ransomware protection

AWS helps protect millions of active customers across the globe from threats like ransomware. These customers represent diverse industries with a range of use cases, including large enterprises, startups, educational institutions, and government organizations. Because of the scale and reach of these customers, AWS has broad visibility and a deep perspective on cloud security, which it rapidly reinvests back into its infrastructure and services.

Follow expert guidance as part of mitigating risk

Best practices, recommendations, and AWS services can help you lower the risk of a ransomware attack and recover quickly if your organization is affected.

Migration

AWS offers migration recommendations in the Cloud Adoption Framework Security Perspective. This perspective provides guidance and best practices to help you build a comprehensive approach to cloud computing across your organization and throughout your IT lifecycle.

Workloads

The workload best practices in the Well Architected Security Pillar describe how to take advantage of cloud technologies to protect data, systems, and assets. You can improve your security posture and then check workloads against these recommendations. The Well Architected Tool in the AWS Management Console helps you review the state of your workloads and compares them to the latest AWS architectural best practices.

Infrastructure

Trusted Advisor uses checks to evaluate your AWS environments. These checks include recommendations for optimizing your infrastructure, improving security and performance, reducing costs, and monitoring service quotas.

Security posture

The AWS Security Hub Foundational Security Best Practices is a standard set of controls that detect when deployed accounts and resources deviate from security best practices. It monitors your AWS accounts continuously and provides actionable and prescriptive guidance on how to improve and maintain your organization's security posture.

Inherit security controls that relieve your operational burden

You can inherit controls from AWS compliance programs. These allow you to focus on securing workloads and the data you put in the cloud. AWS helps relieve your operational burden because it runs, 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.

Sharing security responsibilities reduces risks

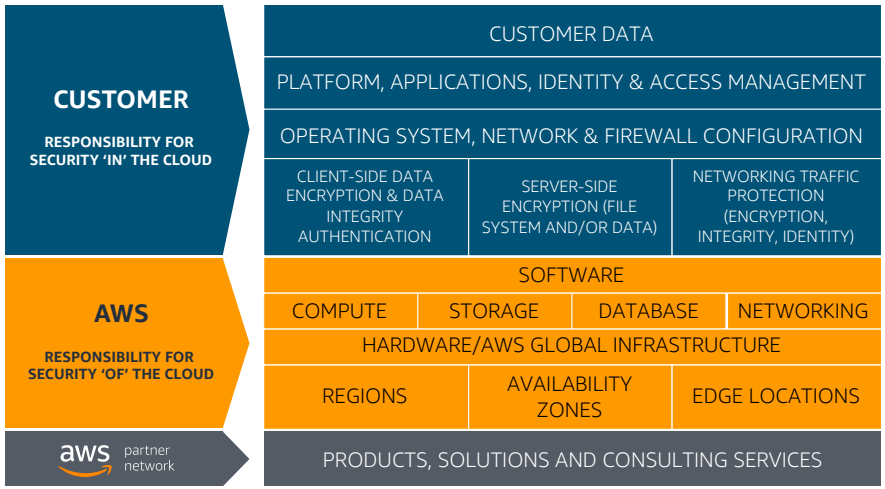
When you deploy systems in the AWS Cloud, AWS helps by sharing the security responsibilities with you. AWS engineers its underlying cloud infrastructure using secure design principles. You are responsible for your own security architecture for workloads deployed on AWS. This is called the AWS Shared Responsibility Model.

AWS is responsible for the security of the cloud

AWS is responsible for protecting the infrastructure that runs all the services offered on the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Other responsibilities depend on the AWS solutions you are using. For example, if you are running Amazon Elastic Compute Cloud (Amazon EC2), AWS is also responsible for its global infrastructure, including regions, availability zones, and edge locations. If you are using AWS container services, the responsibility expands to platform and applications management, operating system, and network configuration. Since the nature of some container technology introduces vulnerabilities that attackers can easily exploit, this responsibility information is important.

You are responsible for security in the cloud

The AWS Cloud services you select determine your responsibilities, such as the amount of configuration work you must do as part of your security responsibilities. In general, you are responsible for managing the security of your data and its encryption, classifying your assets, and using AWS Identity Access Management (IAM) to apply the appropriate permissions. For example, your additional Amazon EC2 responsibilities are operating system, network, and firewall configuration (security groups), client and server-side encryption, and network traffic protection. For AWS container services, your responsibility is similar, removing only operating systems from the mix.



If your company isn't teeming with security experts, AWS Partners have services and solutions that can help. Together with AWS, they can help you harden your AWS infrastructure against ransomware attacks by following five steps that are based on the core functions in the NIST Cyber Security Framework.

Improve your ransomware security in 5 steps

To just say no to ransomware, you start by identifying everything in the cloud you need to be kept safe from harm and end with a plan for recovering from the attack. Here are five steps, which are the same as the five core functions in the NIST Cyber Security Framework, along with the AWS services and solutions that can help.

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, Mainenance, Protective Technology

Detect

Anomalies and Events, Security Continuous Monitoring, Detection Processes

Respond

Response Planning, Communications, Analysis, Mitigation, Improvements

Recover

Recovery Planning, Improvements, Communications

Step 1: Identify

Before you can take steps to prevent and protect against ransomware, you need a comprehensive understanding of everything that could be at risk or that you must safeguard. To do this requires identifying your assets, risks, environments, and supply chain entry points. AWS and AWS Partners can help. You can use the AWS Management Console as a visual point-and-click interface, the command line interface (CLI), or application programmable interface (API) to query and obtain visibility of AWS service assets.

- **In addition, there are AWS Partner solutions that can check the configurations of all components, aggregate network traffic entering and leaving the workload, audit API calls, and provide runtime visibility to make it easier to identify vulnerable spots.**

Step 2: Protect

Now that you know what needs safeguarding, you must take the steps to protect it. To address this step, AWS offers Access Control Identity Management, Authentication and Access Control (PR.AC). This offering can protect your AWS infrastructure, assets, and associated facilities by restricting access to physical assets, logical assets, and associated facilities. Only authorized users, processes, or devices with authorized activities and transactions can gain access, and this is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

- **And, AWS Partner solutions provide end point blocking and monitoring for additional protection.**

Step 3: Detect

Malicious actors are constantly coming up with new ways to attack your systems. Locking up your data, assets, intellectual property, and infrastructure is only part of defending against ransomware. You also need to detect attempts to get in at the network level. AWS has several services you can use as part of a comprehensive security operations strategy for continuous monitoring and threat detection:

- AWS CloudTrail logs all API calls. Amazon Server-Side Encryption with Amazon Simple Storage Service (Amazon S3) managed encryption keys (SSE-S3) can digitally sign and encrypt the logs and store them in a secure Amazon S3 bucket.
- Amazon Virtual Private Cloud (VPC) Flow Logs monitor all network activity going in and out of your VPC.
- Amazon CloudWatch monitors your AWS environment and generates alerts.
- Amazon GuardDuty correlates activity in your AWS environment with threat intelligence from multiple sources that provides additional risk context and anomaly detection.
- Amazon Macie can identify sensitive data, classify, and label it, and track its location and access.

› **AWS Partner solutions enable you to quickly access data from AWS services so you can understand and detect issues more quickly.**

CHECK POINT
splunk>
f5
Trellix

Step 4: Respond

You've detected an anomaly, outlier, or possible breach. How do you respond? If you used Incident Manager, a capability of AWS Systems Manager, to build an effective automated incident management and response solution to security events, then you're covered. Otherwise, start off by staying calm and taking the time to investigate the issue thoroughly. Follow your plan that outlines your procedures, steps, and responsibilities for your incident response program.

› **AWS Partners streamline incident response, allowing you to address issues quicker.**

zscaler
SentinelOne
CROWDSTRIKE
TREND MICRO

Step 5: Recover

Despite your preventative and incident response measures, the malicious actors got in. But you can get through this relatively unscathed because you had plans for this step. AWS has resilient infrastructure, reliable automation, and exceptional people that make it possible to recover from events very quickly and with minimal (if any) disruption. For example, if an attack takes down an Amazon EC2 image, it's possible to replace it rapidly with a new Amazon Machine Image (AMI). Amazon CloudWatch and AWS Lambda can also automate recovery actions like deploying an entire AWS environment and application, failing over to a different AWS region, restoring data from backups, and more.

By following these steps, you are well on the way to saying no to ransomware. For a more comprehensive guide, be sure to read the whitepaper, Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF). Now it's time to examine how AWS and AWS Partners can help ensure you meet the five executive order recommendations.

› **AWS Partners have recovery automation tools that make it faster to access immutable files from another AWS region and get up and running again.**

CLUMIO
COHESITY
COMMVAULT
druva
rubrik
VEEAM
VERITAS

Take all 5 steps with global security services

Deloitte global security services and AWS take a holistic approach to security, designing and orchestrating innovative solutions that enable companies to reduce cyber risk and avoid ransomware. With a global network, tools, and accelerators backed by years of security experience, Deloitte can help you take all five of the ransomware security steps together. Data-driven insights reinforce key security decisions and identify areas for improvement.

Deloitte.

Strengthen protection with these 5 recommendations

President Biden's executive order for strengthening cyber defenses against ransomware is a good rule of thumb for all organizations, no matter what part of the globe they occupy. Here are the five recommendations and the AWS services and solution to support them.

Implement five best practices

AWS and the AWS Partner Network can provide the capabilities you need to implement the president's five best practices-- multifactor authentication, endpoint detection, response, encryption, and a skilled, empowered security team. AWS makes it easier for you to implement requirements for data protection, encryption, and multi-factor authentication. Using our AWS Professional Services and AWS Partner Network, and CloudEndure Disaster Recovery, you can accelerate your ability to follow these best practices.

1. Backup and restore

Build and deploy highly available and resilient applications that are easy to backup and restore using services such as AWS Backup and CloudEndure Disaster Recovery. With Amazon S3 Glacier Vault, you can create a policy that denies users permissions to delete an archive for a given time, test the policy, and then lock it so it becomes immutable.

Do you have an existing backup provider you prefer? In most cases, AWS Storage Partner backup and restore solutions offer significant coverage and capabilities for ransomware recovery to fit any business requirement.

2. Update and patch systems

How can you rapidly identify, protect, update and patch vulnerabilities so that you limit the number of entry points for ransomware? Here are some AWS services that can help:

- Amazon GuardDuty, a threat detection service that continuously monitors for malicious activity and unauthorized behavior, can analyze and process a variety of AWS data sources to identify potential security issues.
- AWS Security Hub can prioritize and manage security alerts and provide centralized views of findings, from multiple AWS services and AWS Partner Network Solutions.
- AWS Systems Patch Manager automates the process of patching managed instances with security and other types of updates.

3. Test your incident respons plan

Incident response plans are critical in this time when the ransomware threat level is high. What are your policies and procedures for responding to security events? For help in this area, there's the AWS Security Incident Response Guide, which includes a section on security incident response simulations. You can also use Incident Manager in AWS Systems Manager to automate your response.

4. Implement penetration testing

Using trained and certified professionals to try to hack into your environments, apps, and data sources can reveal your soft security spots—and you're in control. AWS Partners provide penetration testing to check your security team's work. Discover known vulnerabilities, which remain one of the most commonly used entry points for ransomware exploits. You can carry out security assessments or penetration tests against your AWS infrastructure without prior approval for a subset of permitted services, if these activities are aligned with the policy defined on the AWS Penetration Testing webpage.

5. Implement penetration testing

Dividing a network into smaller sub-networks with limited inter-connectivity between them enables you to control traffic flows and by restricting attacker lateral movement. As a result, it prevents unauthorized users from accessing your intellectual property and data.

In the cloud, you can provision logically isolated sections and launch resources from them in virtual networks that you define. For example, segmenting Amazon Virtual Private Clouds (VPCs) into isolated components, either by security groups or network access control lists (ACL), helps ensure that only necessary traffic is available while reducing ransomware's ability to move laterally in the network or impact other AWS environments. AWS Network Firewall is a managed service that makes it easy to deploy essential network protections for all your Amazon VPCs.

Network segmentation should include Zero Trust because it sets up secure perimeters around your internal systems. AWS identity and networking services provide core Zero Trust building blocks that can be applied to both new and existing workloads. In addition, you can work with AWS Network and Infrastructure Security Partners to detect and protect your workloads.

AWS Security Competency Partners provide solutions that help prevent, detect, respond, and hunt for ransomware across all enterprise assets. For example, you can harden your operating systems using CIS hardening benchmarks or run CIS hardened images, which are available in AWS Marketplace. For full-time support, AWS Managed Security Service (MSSP) Partners provide 24/7 security protection and monitoring of essential AWS resources.

Summary

Ransomware can hobble your systems, steal your data, and put a dent in your company's bank account. But with smart preparation, ongoing vigilance, and the right technology, you can just say no to ransomware.

AWS and AWS Partners offer services and solutions that can keep your data, workloads, applications, and environments secure and safe from ransomware. With these offerings, you can take proactive measures to reduce the likelihood and impact of ransomware in your AWS environments.

Find an AWS Security Competency Partner and protect your system from ransomware.

Find an AWS Security Competency Partner ›