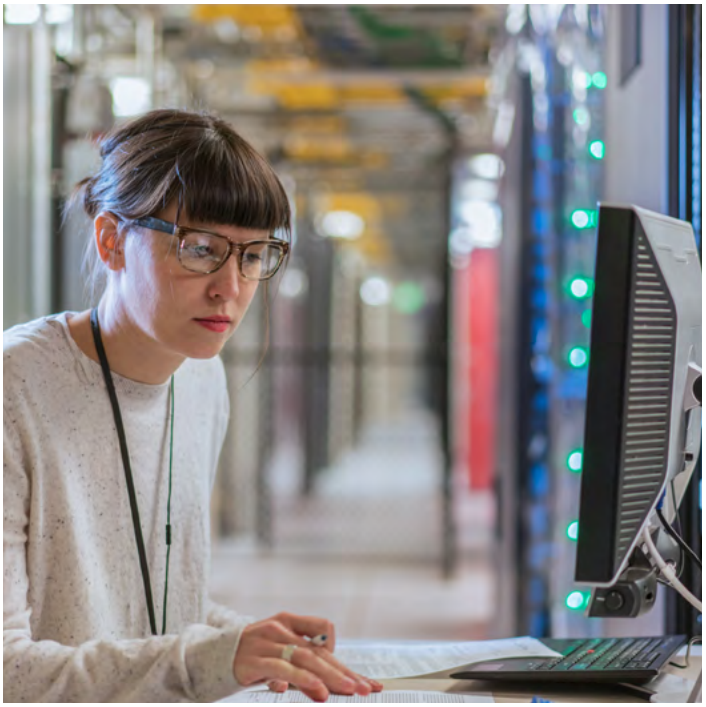
IBM **Security**

6 quick wins for ransomware preparedness in AWS

aws PARTNER Premier Tier Services

- L1 MSSP Services Competency
- Security Services Competency
- Security Software Competency



For over three years, ransomware has been the most prevalent cybersecurity attack type, as the IBM Security® X-Force® Threat Intelligence Index 2022 shows. Organizations must consider how to prepare their cloud infrastructure to detect, respond to and recover from ransomware attacks.

IBM Security X-Force experts recommend these six quick ways to improve your ransomware preparedness using solutions from Amazon Web Services (AWS).

01

Build and test a recovery strategy

Businesses that rely on data to function need to have a reliable backup solution in place. According to Andrew Gorecki, Global Remediation Lead, X-Force, traditional disaster recovery (DR) strategies are ineffective in ransomware attacks. In this context, organizations need to seriously rethink how they approach cyber recovery.

While snapshot creation using AWS Elastic Compute Cloud (EC2) can help customers recover their instances or virtual machines in the cloud, there are more aspects to disaster recovery that need to be considered. X-Force experts recommend that organizations address aspects such as file systems and object storage by creating logically air-gapped snapshots of primary storage, providing immutable, incorruptible data copies.

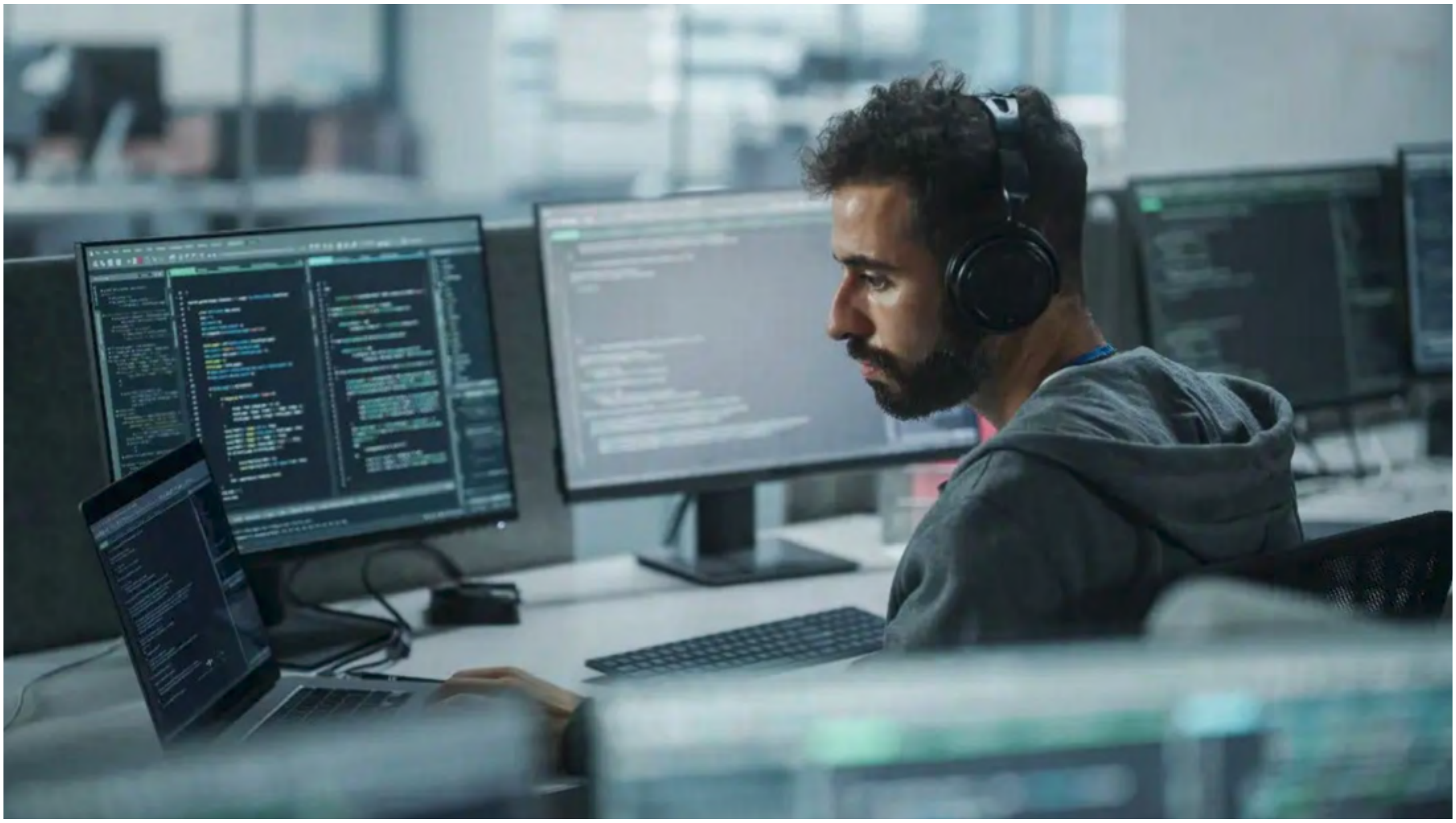
The following native AWS solutions can be used for backup and disaster recovery:

AWS Backup
This fully managed native Amazon backup service enables organizations to easily centralize and automate data protection across AWS services. The solution eliminates the need for AWS administrators to manage separate data protection strategies or solutions. AWS Backup centralizes a policy-based backup solution that extends across various AWS services.

Learn more →

AWS Elastic Disaster Recovery (DRS)
This solution continuously replicates block storage volumes from any supported source, be they physical, virtual or cloud-based servers. DRS orchestrates the recovery within AWS to dramatically reduce recovery time.

Learn more →



02

Address double extortion

Publications such as How Ransomware Attacks Happen and the IBM X-Force Threat Intelligence Index show that ransomware attackers frequently use a double extortion tactic. This tactic not only encrypts but also steals data and threatens to disclose it publicly if the ransom isn't met.

> "Ransomware attackers have found that this kind of 'double extortion' tactic is extraordinarily effective. Attackers know that if they steal data that belongs to a different organization than the one they're attacking, that gives them added leverage."

Camille Singleton
Manager
X-Force Cyber Range Tech Team

Organizations should implement protective measures such as creating an inventory of all sensitive data and using data encryption for all data at rest within storage systems.

Amazon Macie
This native Amazon data privacy service uses machine learning and pattern matching to discover and protect sensitive data within AWS. Amazon Macie builds an inventory of the data within the Amazon S3 buckets and creates a list of data that is unencrypted, publicly accessible and shareable with resources outside of your AWS organization. Additionally, the service actively collects an inventory of sensitive data like personally identifiable information (PII), credentials or financial information.

Learn more →

Data at rest encryption
AWS offers two options for protecting data at rest within Amazon S3: client-side encryption and server-side encryption. Client-side encryption requires the user to manage and maintain the data encryption process through an external mechanism. Server-side encryption allows users to encrypt data at rest using native AWS Key Management Service (AWS KMS) or Amazon S3 encryption, which automatically encrypts data before it's saved to disk in the AWS data centers.

03

Manage privileged access and network segmentation

Security in the cloud is an inherently shared responsibility between AWS and the users. A 2021 assessment of cloud deployments revealed that 70% of customer environments had internet-facing AWS instances and identities whose permissions could be used in a ransomware attack.[1] Additionally, the study showed that almost 80% of the environments contained identity and access management (IAM) users with enabled access keys that had not been used for 180 days or more.[2]

A balanced strategy includes tools for securing the underlying infrastructure, while still leaving room for customer-specific security measures. These measures can include determining internet access requirements or auditing user privileges.

Organizations that implement least privilege, protect privileged accounts and network segmentation are far more prepared to pre-empt the threat from the threat of ransomware. AWS provides the following native features to add layers of protection to accounts:

Multifactor authentication (MFA)
Through AWS, IAM accounts can be configured to require MFA to access the AWS console or API resources. It's recommended that organizations enable MFA for the root account as well as all user accounts.

Learn more →

IAM roles
AWS provides users with the ability to create roles, which are identities tied to specific permissions. A role can be configured with a permission policy that determines what can and can't be accessed within AWS and can be assumed by any user account that requires the defined permissions. As opposed to individual IAM user accounts, roles use a temporary security credential that is only good for one session, reducing the risk of credential compromise.

Learn more →

IAM least privilege
This process limits access to IAM roles and users to only what is required to reduce the risk of privilege escalation in the event of a role or account compromise.

Learn more →

IAM Access Analyzer
This native AWS tool is designed to easily generate least privilege policies and permissions within IAM.

For more information on AWS IAM security best practices, see the AWS IAM security guide.

Highly segmented AWS deployments reduce the ability for ransomware attackers to propagate through various AWS subnets, networks and accounts. Organizations should audit and implement segmentation policies to ensure that only the required ports and protocols are available to traverse AWS subnets and virtual private clouds (VPCs).

Learn more →

04

Build and test detection and response strategies

Protective measures to prevent and recover from a ransomware attack are important. However, organizations should also look into developing and testing a detection and response strategy based on the telemetry within AWS.

> "While it's critical to focus on prevention, companies also need to strategize in advance for a possible attack. A lot of organizations have response plans, but there's great variance in the quality of these plans and whether they've been properly tested."

Charles DeBeck
Senior Strategic Analyst
IBM Security X-Force

AWS provides several native services that increase an organization's ability to detect and respond to a compromise before it becomes a crisis. Organizations should continually work with experts to test the effectiveness and identify gaps through technical and strategic exercises. The following data sources can be used to build detection capabilities:

Amazon CloudWatch
This native AWS service monitors resources and applications within your AWS account. The service collects metrics such as latency and utilization from various AWS services, enabling real-time monitoring of AWS resources such as Amazon EC2 instances, Amazon Elastic Block Store (EBS) volumes, Elastic Load Balancing and Amazon Relational Database Service (RDS).

Learn more →

AWS CloudTrail
This native AWS service collects data regarding activity within AWS by tracking application programming interface (API) calls, including when resources are accessed, when an account or role runs an AWS command, or when an AWS API is accessed. CloudTrail enables visibility into AWS activities that can be crucial for incident response investigations and detection of malicious activities.

Learn more →

VPC Flow Logs
This native AWS network monitoring solution enables organizations to track and analyze network traffic coming in and out of resources within a VPC. VPC Flow Logs enable organizations to detect unsanctioned access by identifying unauthorized IP addresses, ports and protocols being used to interact with AWS instances.

Learn more →

Amazon GuardDuty
This AWS threat detection service uses machine learning and integrated threat intelligence to identify malicious activity related to AWS accounts and users. GuardDuty is designed to detect malicious activity associated with compromised IAM roles and users, reconnaissance activity and compromised EC2 instances.

Learn more →

Amazon Detective
This AWS investigation service uses log sources from AWS CloudTrail, VPC Flow Logs and Amazon GuardDuty to identify associated and underlying activities that resulted in an incident or alert.

Learn more →

05

Address patch management

Exploitation of software vulnerabilities remains one of the most popular initial access vectors for ransomware attacks. Organizations must implement solutions and policies to ensure that security patches are being applied to all Amazon EC2 instances in a timely manner. Additionally, AWS offers solutions to enable organizations to run popular services outside of Amazon EC2 instances.

AWS Systems Manager
Patch Manager within AWS Systems Manager enables organizations to automate patching of Amazon EC2 instances for security patches for operating systems and applications. AWS Systems Manager can create custom patch baselines that can be used to automatically scan Amazon EC2 instances on a regular interval and apply patches continuously.

Learn more →

AWS Serverless Computing
AWS provides technologies that enable users to run code, manage data and integrate applications without managing servers. Using serverless computing reduces that attack surface of vulnerabilities on Amazon EC2 instances. It eliminates the instance altogether and uses the built-in functions as a service to run custom code or functions without the need of an underlying server.

Learn more →

06

Start your security journey with a trusted partner

It’s good practice for organizations to engage an AWS level 1 managed security services provider (MSSP) partner. Such a partner can provide guidance on ransomware preparedness and broader elements of the security shared responsibility model.

IBM Security is a leader in comprehensive AWS level 1 MSSP services, including digital forensics incident response specialization. Additional AWS level 1 capabilities include the following:

- AWS resource inventory visibility
- AWS best practices monitoring
- Compliance posture management
- Vulnerability management
- Threat detection
- Triage and respond
- Managed network intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- Managed host and endpoint security
- Distributed denial-of-service (DDoS) defense
- Web application firewall (WAF) and application security
- Modern computer security
- Managed application security testing
- Data privacy event monitoring
- Identity behavior monitoring

There’s no single solution to protecting yourself from ransomware. Staying protected requires a long-term strategy that involves constant vigilance to both your infrastructure and the latest industry trends. Cybercriminals are always finding new ways to exploit vulnerabilities. By staying vigilant and keeping up with the latest developments, you can help ensure that your company is prepared for whatever the next ransomware attack may bring.

If you want to have a deeper conversation around ransomware prevention, detection and response strategies, contact us to schedule a meeting.

Or call:
US hotline 1-888-241-9812
Global hotline (+001) 312-212-8034

Notes

[1,2] AWS ransomware attacks: Not a question of if, but when, Help Net Security, 12 October 2021.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States
of America October 2022

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.