Protecting your AWS environment from ransomware

Top 10 Best Practices for Ransomware Protection

Megan O’Neil
Principal Security Specialist SA
2023
What is ransomware?
What is ransomware?

Ransomware refers to a business model and a wide range of associated technologies that unauthorized users use to extort money from entities.

Unauthorized users use system vulnerabilities to access data and then restrict the rightful owner from accessing it.
What is ransomware?

Accomplished by unauthorized user who encrypts data using actor-controlled encryption keys, using access controls to lock out the rightful owner from a system.

Or, unauthorized users may threaten to reveal data or acts of exfiltration, which can result in large monetary fines from data privacy authorities and/or litigation from affected parties.
Why is ransomware effective?

- Many organizations struggle with privileged access management, resulting in overly permissive credentials and compromised credentials.
- Many organizations have an open trust model, which allows malware to spread.
- Security awareness amongst employees is low.
- Some organizations are not backing up data or not testing their backup and restore processes.
- Ransomware and attack services have been commoditized.
- Overburdened technical staff relying on time-consuming manual processes.
Top 10 best practices for ransomware protection

1. Leverage a security framework
2. Patch and harden systems
3. Eliminate long-lived credentials
4. Implement a standard AWS VPC design pattern and multi-account topology
5. Use immutable infrastructure with no human access
6. Implement centralized logging and monitoring
7. Implement and test backup and restore processes
8. Prepare and exercise an incident response plan
9. Perform self assessments
10. Automate security guardrails and response actions
2.0 Patch and harden systems

2.1 Utilize Amazon Inspector to perform vulnerability management

2.2 Utilize AWS Systems Manager Patch Manager

2.3 Apply OS and application hardening configuration
2.1 Utilize Amazon Inspector to perform vulnerability management

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.

- **Scale** with simplified management
- **Gain centralized visibility**
- **Automated discovery and continual scanning**
- **Prioritize with contextualized scoring**
- **Automate workflows and take actions**
2.2 Utilize AWS Systems Manager Patch Manager

PATCH MANAGER
AUTOMATE THE PATCHING PROCESS

- Automate patching by defining rules for auto approval
- Scan and install patches on a regular basis by scheduling maintenance windows
- View aggregate patch compliance using Explorer
- Supported OS include Windows Server, Amazon Linux/2, CentOS, Debian, Oracle Linux, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Ubuntu Server
2.3 Apply OS and application hardening configuration

Benchmarks available for various versions of:

- Ubuntu Linux
- Microsoft Windows
- Amazon Linux
- Red Hat Enterprise Linux
- Debian Linux
- CentOS Linux
3.0 Eliminate long-lived credentials

3.1 Use federation for Developer Access and eliminate long-live credentials

3.2 Re-Architect to utilize IAM Roles Anywhere
3.2 Use federation for Developer Access and eliminate long-live credentials

- **Federate** all user access and use AWS Identity and Access Management (IAM) roles for system to system access

- **Restrict** creation of static IAM users and keys

- **Audit and track**
  - **Inventory** static users and keys do exist across all accounts?
  - **Rotate** keys
  - Limit the IAM policy/no **wildcards** as actions or resources
  - **Re-architect** to eliminate use?
3.2 Re-architect to utilize IAM Roles Anywhere

**Step 1: Establish trust**
Create trust anchor
Establish trust between AWS and your CA

**Step 2: Configure roles**
Configure your existing role trust policies for IAM Roles Anywhere
Create a profile to apply to your roles using a role session policy

**Step 3: Use IAM Roles Anywhere**
Request temporary credentials
Audit the activities of your certificates
6.0 Implement centralized logging and monitoring

- 6.1 Logging and monitoring security considerations
- 6.2 Utilize AWS Security Services for monitoring
6.1 Logging and monitoring considerations

- Enable log read and write management events in CloudTrail
- Log file validation and log file encryption in CloudTrail
- Enable AWS Security Services as a function of AWS Organizations including CloudTrail and GuardDuty
- Centralize CloudTrail into a Log archive account
- Log data events for Lambda and S3 buckets
- Host based logs
- ELB access logs
6.2 Utilize AWS Security Services for monitoring

And more to come…

Plus dozens of others…

AWS Security Hub

Remediation Actions

Taking Action Partners

AWS CloudWatch Events

Investigations

Amazon Detective

© 2023, Amazon Web Services, Inc. or its affiliates.
7.0 Implement and test backup and restore processes

7.1 Best Practices for Backup and Restore

7.2 Secure Backup Strategy

7.3 Use Managed data/database services and Lock features
7.1 Best practices for backup and restore processes

- Categorize applications based on criticality
- Evaluate data protection, backup, and recovery processes against the criticality of your applications
- Identify tooling to bring up virtual machines and rehydrate data
- Build detailed playbooks and test them periodically
- Store backups and images in an isolated account with minimal access
- Use different encryption keys for different sets of data
- Have backup servers in the cloud
7.2 Air gap-like secure backup account architecture

Data center A

Third-party cloud providers

AWS production accounts

Production accounts

Staging account

Vault account

Recovery account

Vault forensics account

(Pulled when required)

(Created when required)
7.3 Use data/databases services and “lock” features

WHY MANAGE YOUR OWN BACKUP AND RESTORE PROCEDURES?

- AWS Backup Vault Lock
- Amazon S3 Object Lock and Glacier Vault Lock
- Point-in-time recovery (PITR) for Amazon DynamoDB
9.0 Perform self-assessments

These security assessments are from the open source projects “Prowler” and “ScoutSuite.” This includes custom modules that check for ransomware specific findings.
Resources

Protecting your AWS environment from ransomware (ebook)

AWS Ransomware Resources
https://aws.amazon.com/security/protecting-against-ransomware

AWS Security Resources Hub
https://aws.amazon.com/security/security-learning

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

AWS Well-Architected Framework – Security Pillar
https://docs.aws.amazon.com/wellarchitected/latest/security-pillar
Thank you!