Ransomware-Proof Your AWS Cloud
with the Ultimate Disaster Recovery Strategy

Brought to you by:

SIIA
VeeAM
N2WS
Today’s expert presenters

Vitaly Lyaskovsky

- Director of Technical Support at N2WS
- Cloud & Disaster Recovery Expert
- 20+ years of experience specializing in Cloud/Enterprise Security solutions
- Previously at IBM, FilesX, Intel
Today’s expert presenters

Mike Somerville

- Chief Cloud Evangelist & IT Manager of Systems/Support University of San Diego
- 20+ years experience in leading the adoption of cloud services and providing innovative cloud solutions
- Founder and Chief Architect at several cloud computing consulting firms
Understanding the Risk of Ransomware
The costly growth of cyber-crime

Ransomware is the fastest growing type of cybercrime.

$20 billion in 2021. This is up from just $325 million in 2015.
The evolution of ransomware

- Ransomware = **malicious code** designed to gain unauthorized data access and **encrypt data** to block access by legitimate users.

- First instance of ransomware (1989) had simple encryption tools and user interaction was necessary. Now more complicated, using complex algorithms, no interaction necessary.


- Current trends include RaaS, cryptocurrency mining.
Concerning ransomware stats

- A company gets hit every **40 seconds**
- **50%** of organizations attacked by ransomware are hit **more than once**
- **$532,914** is the average ransomware recovery cost
- **23 days** is the average amount of time to recover data
The biggest cost isn’t the ransom

Downtime creates **loss of productivity of users and responders**, exposure of **sensitive data**, **loss of revenue** – current and future costs include:

- Data damage
- Restoration of host systems and data
- Downtime due to attacks (no productivity/revenue)
- Forensic investigation
- Damage to the reputations of victims

*Loss of productivity & non-availability is the primary business impact of ransomware*
The Code Spaces nightmare

Backups *were performed* BUT cross account backups were not created

Code Spaces went out of business **12 hours after the attack** took place
What about more recent attacks?

- NotPetya forced shipping giant Maersk to reinstall 4,000 servers and 45,000 PCs for $300 million due to "serious business interruption"

- Baltimore ransomware attack will cost the city over $18 million (and counting...)

- Riviera Beach and Lake City Florida will pay hackers $1M combined to (maybe?) get its computer systems back

*All attacks were due to lack of strong security/backup practices*
To pay or not to pay the ransom?

**MYTH:** Paying ransom guarantees your data back

- Only 42% of companies report being able to fully recover data after an attack.
- Many times bad guys will attack a 2nd time knowing they can *extort another payment*.

**TRUTH:** The *only* guarantee of returning your data is to have a reliable backup & recovery solution in place.
The Need for Backup and Restore on AWS
Do I really need to backup in AWS?

**MYTH:** I don’t need to backup Amazon EBS, because it’s so redundant I’ll never lose data

**TRUTH:** EBS is designed for an annual failure rate of about 1/1000. But more common than that are these risks...
AWS Shared Responsibility Model

AWS provides the virtual hardware and protects that infrastructure

But the data you store within it is YOUR responsibility –this often goes unrealized
How does data loss happen in the cloud?

- EBS Failure
- Ransomware
- Compliance + Data Security
- AZ Failure
- Human Error/Malicious intent
Reduce the Risk of a Ransomware Attack
### Internal Awareness

**Improve user awareness**

- Get training!
- Have a security awareness person/program to deploy regular phishing tests. (Phishing emails are becoming both more clever and pervasive).
- Implement anti-phishing software in your backend.
Prevention

- Install anti-malware software
- Engage email filtering, web blocking, etc.
- Keep your software and hardware up to date
“Ransomware-Proofing” your Cloud with AWS Backup & Recovery
**How to prevent a ransomware attack?**

1. **Back-up! Back-up! Back-up!** Have a recovery system in place so a ransomware infection can be corrected. Make copies of important files and store them in the cloud (remember to use a service that makes an automatic backup, e.g., thumb drive, extra laptop, etc.). Disconnect these from your computer when you are done. Don’t delete a critical file or experience a hard drive failure.

2. **Use robust antivirus software** to protect your system from ransomware. Do not switch off antivirus software that have not yet been formally detected.

3. **Keep all the software on your computer up to date.** When your operating system (OS) or application has an update, take it.

4. **Trust no one. Literally.** Any account can be compromised and malicious links can be sent from a trusted or gaming partner. Never open attachments in emails from someone you don’t know. Cybercriminals email notifications from an online store, a bank, the police, a court or a tax collection agency to malware into your system.
Backup Terms

- **RTO** – Recovery Time Objective
- **RPO** – Recovery Point Objective
- **Crash Consistent Backup** – General backup of instances, to restore as if the power cord had been pulled
- **Application Consistent Backup** – Quickly “quiesce” the applications to allow complete backups that capture all transactions in process
- **Offsite Backup** – Backups that are stored in a physically distinct location to the production environment
AWS global infrastructure

21 regions worldwide, 66 availability zones, 180 POPs

Select your region based on:

- Latency
- Compliance
- Cost
Some benefits of backup and restore on AWS:

- **Secure**
  - Encrypt data to tightly control access and increase security

- **Scalable**
  - Scale automatically no need to manually scale up or scale down

- **Easy**
  - Hardware-free no need to buy/maintain on-premises hardware

- **Low cost**
  - Usage-based fees pay ONLY for what you’re using each month
About N2WS

• Founded in 2012

• #1 Backup & Recovery Solution on the AWS Marketplace

• Purpose-built for AWS

• Distributed via AWS Marketplace
The “promise of the cloud”, delivered

Disaster Recovery

- Amazon EBS Snapshots
- APIs + CLI
- Durable Storage
- AWS Lambda Scripting
- Regions and Availability Zones

- VPC Backup
- Archive to S3
- File-Level Recovery
- Auditing, Reports + Alerts
- Application-Consistent + Application-Aware
- Simple UI

#1 AWS Backup

Veeam N2WS
Used by AWS builders, worldwide

5K+ AWS Accounts
HUNDREDS of THOUSANDS of Protected Instances
13+ Petabytes of Backup

#1 AWS Backup
Your giant recovery button

**Automated policies and schedules**
Configure what to back up and when - define backup targets, set backup frequency and retention periods

**Cross-region & cross-account DR**
Replicate snapshots to one more regions and recover quickly in the event of an issue

**VPC Capture and clone**
Configure regular backups of VPC settings and recover to any region

#1 AWS Backup
Protect against regional outages

Use **cross-region** DR

- Protect against **region failure**
Protect against account compromises

Use cross-account DR

- Protect against account compromise
Protect against ANY type of data loss

Use BOTH cross-region and cross-account DR to create a highly secure “Snapshot Vault”

• Protect against BOTH region failure and account compromise
Top cost saving features

Archive snapshots to S3 buckets
Save big on your AWS storage bill by copying EBS snapshots to a low-cost S3 repository

Stay compliant for less
Store data for as long as you need while paying a third of the standard cost

Start/stop instances on demand
Reduce your AWS bill by turning off non-critical EC2/RDS instances automatically or on-demand
How University of San Diego Ransomware-Proofed Using AWS & N2WS
Journey to the Cloud

- 8900 Students
- 500 Servers (Linux & Windows)
- 4 Onsite data centers
- 1 Offsite data center
- 2 Main ERM Systems
- ellucian®
- ORACLE E-BUSINESS SUITE

#1 AWS Backup
Recoverability

Ransomware attacks will continue to adapt and evolve. *All enterprise data should be backed up, available and recoverable.*

Have a recovery scenario in place with **frequent backups**, minimal manual interference, minimal RTO, and minimal downtime.
Basic DR Strategy using N2WS

Using AWS Snapshots to backup EC2 and RDS

Backup volume snapshot scheduled 2x/day

Crash-consistent + application-consistent on backup volume
Main advantages of N2WS

- **Disaster Recovery**
  - *Near-instant* recovery of entire volumes or single files in 1 click

- **Customer focused**
  - Responsive support and customer-focused product roadmap

- **Deployment Ease**
  - *Easy install from AWS Marketplace* takes less than 30 minutes to deploy

- **Cost Savings**
  - *With archive-to-S3 & Resource Control* you can save up to 60% on costs
The N2WS Advantage and an End to Downtime
The Problem

Modern ransomware attacks disable known backup products before encrypting data.
Even if your N2WS Server is somehow compromised - a new N2WS server can restore from snapshots that were created by an old N2WS Server, using metadata that is automatically backed up already.

And N2WS backups can be restored even without N2WS - using EC2 console (for native snapshots) or Veeam B&R (for S3).
N2WS Advantages Against Ransomware

- Backups aren't kept on any Windows/Linux machine, or network share – so an attacker can't destroy them!
- Backups can continue to run **even if** N2WS Agent is disabled
- Even without an active Agent, **backups are fully restorable**
Key Takeaways

Cloud environments need a reliable, flexible and automated solution to manage backups.

N2WS Backup & Recovery provides an easy, scalable and efficient way to manage snapshot-based backup in AWS.

The best ammo to disrupt Ransomware is to take regular backups and have a rapid DR plan in place.
Talk to us!

Sign up for our **fully-featured v2.6 solution** by spinning up a 30-day FREE TRIAL → n2ws.com/trial

Email us with any questions: info@n2ws.com

Please take 1 minute to **fill out our survey!**

Stay tuned for our **upcoming Ransomware webinar Part 2!**