AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

GPS212

Working with AWS Partners for anti-ransomware solutions

Dudi Matot
Principal Segment Lead, Security
AWS

Merritt Baer
Principal, Office of the CISO
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is ransomware?

Ransomware is a form of malware that threatens to publish victim's data or perpetually block access to business-critical information unless a ransom is paid off



Locker ransomware

Does not encrypt files; instead outside parties lock the victims out of their devices and prevent them from having access

Criminals then demand a ransom to unlock the device



Crypto ransomware

Prevents users from accessing important files by encrypting their data

Outside parties make money by demanding victims pay a ransom to get their files back, normally through cryptocurrency-based transactions

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ransomware is in the news . . . but it is not new



Panama 1989

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sutton’s Law:
“. . . because that’s where the money is.”

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How prepared are your customers for a ransomware attack?



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ransomware events are more likely when . . .



Technical maintenance is behind schedule

Patching not up to date

Irregular untested data backups

Manual time-consuming processes



Employee behavior creates security risks

Security awareness low

Vulnerable to social engineering



Security strategy doesn't prepare for events

Overly permissive credentials

Open trust model allows malware to spread

No clear governance model

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Let AWS do the heavy lifting

RELIEVE THE BURDEN OF OPERATING CONTROLS TO AWS AND FOCUS ON INNOVATION



Patching infrastructure



Configuration of infrastructure devices



Shifting management of IT controls



Automate manual tasks

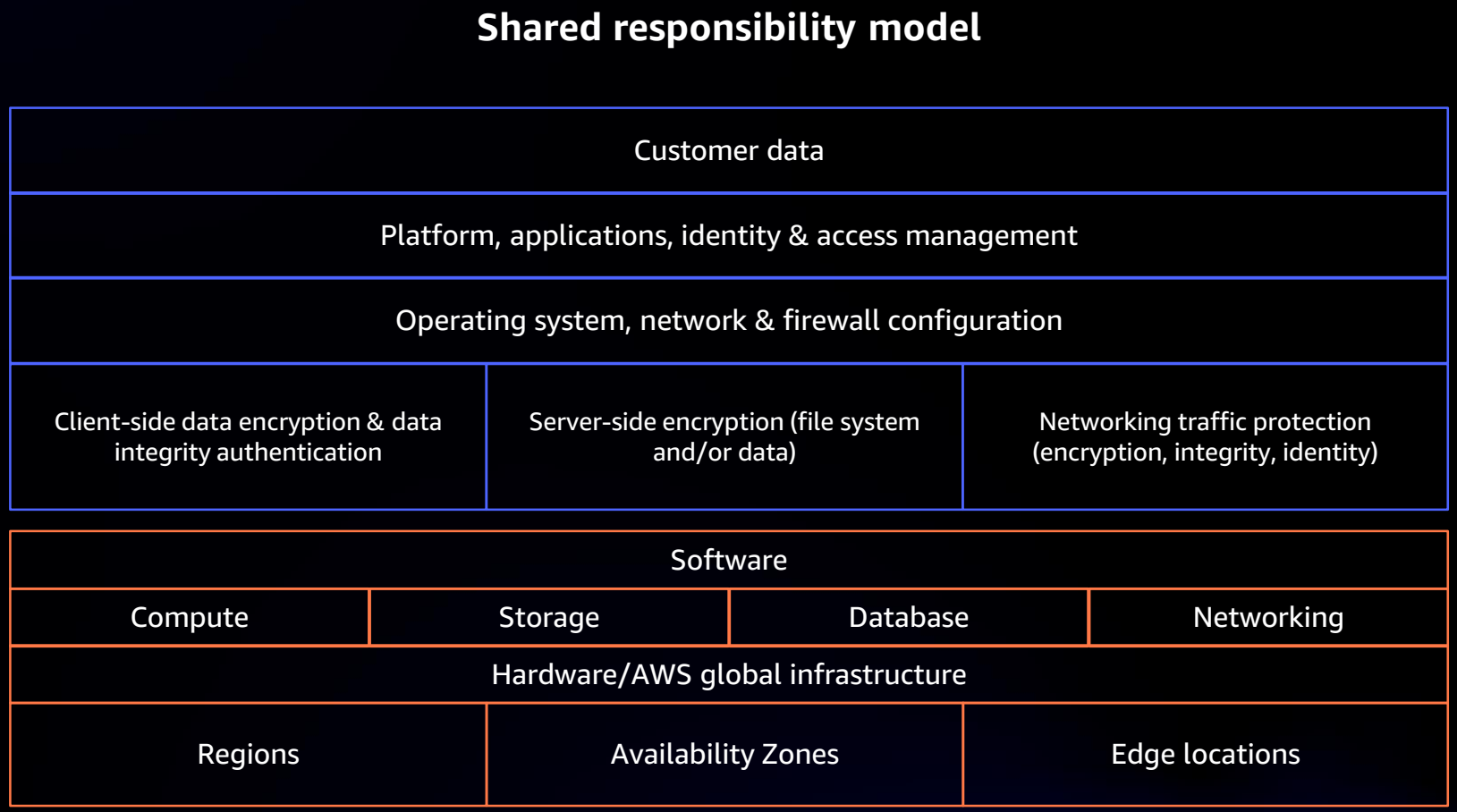
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared responsibility model

Customers have their choice of security configurations **IN** the cloud

Partners support customers throughout

AWS is responsible for the security **OF** the cloud



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use SI partners to forge the trail



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

North stars

WHAT ARE MY MAIN AREAS OF FOCUS TO PROTECT AGAINST RANSOMWARE?

Identity and access management

Including multi-account strategy and use of ephemeral, short-term credentials (no hard-coded, persistent credentials)

Storage, backup, and recovery

Including point-in-time recovery capabilities, ability to “lock” immutable backups, and architecting for high availability

Embrace immutability and ephemerality in your work

Including being able to get back to a known good state, but also being able to recreate known good states, to produce at scale

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Best practices for ransomware-related backup and recovery

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ransomware recovery strategy

IDENTIFY DATA, PRIORITIZE AND ASSIGN TRADE-OFF WITH SIZE, TIME TO RECOVER, AND COST



Selecting the AWS services and/or AWS Partners with the capability for vaulted data artifacts to be immutably stored

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identity and credential protection

CONTINUOUSLY STRIVE FOR LEAST PRIVILEGE AND PRUNING OF PERMISSIONS

Take advantage of cloud-scale capabilities, including:

- Visibility (e.g., tagging assets)
- Enforcement (e.g., AWS IAM Access Analyzer)
- Policy enforcement (e.g., service control policies in AWS Organizations)



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Stop breaches with smarter identity and access controls

CONTINUOUSLY STRIVE FOR LEAST PERMISSIONS

Take advantage of cloud-scale capabilities including

- Visibility
- Enforcement
- Policy enforcement



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Establish robust 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

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enable a backup and recovery solution

- AWS Backup for the cloud
- AWS Storage Gateway for on premises
- CloudEndure for both cloud and on premises
- Partner backup solutions (next slide!)

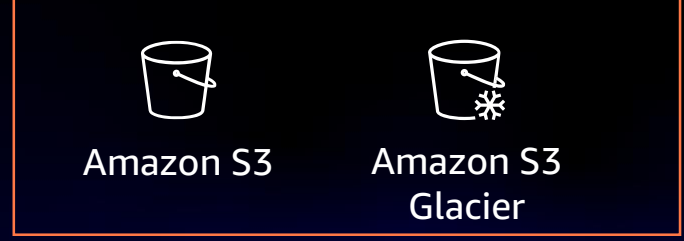
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup and partner backup solutions

Backup vendors | Backup on premises and in the cloud, advanced backup functionality, ability to use AWS Backup APIs to integrate with AWS services

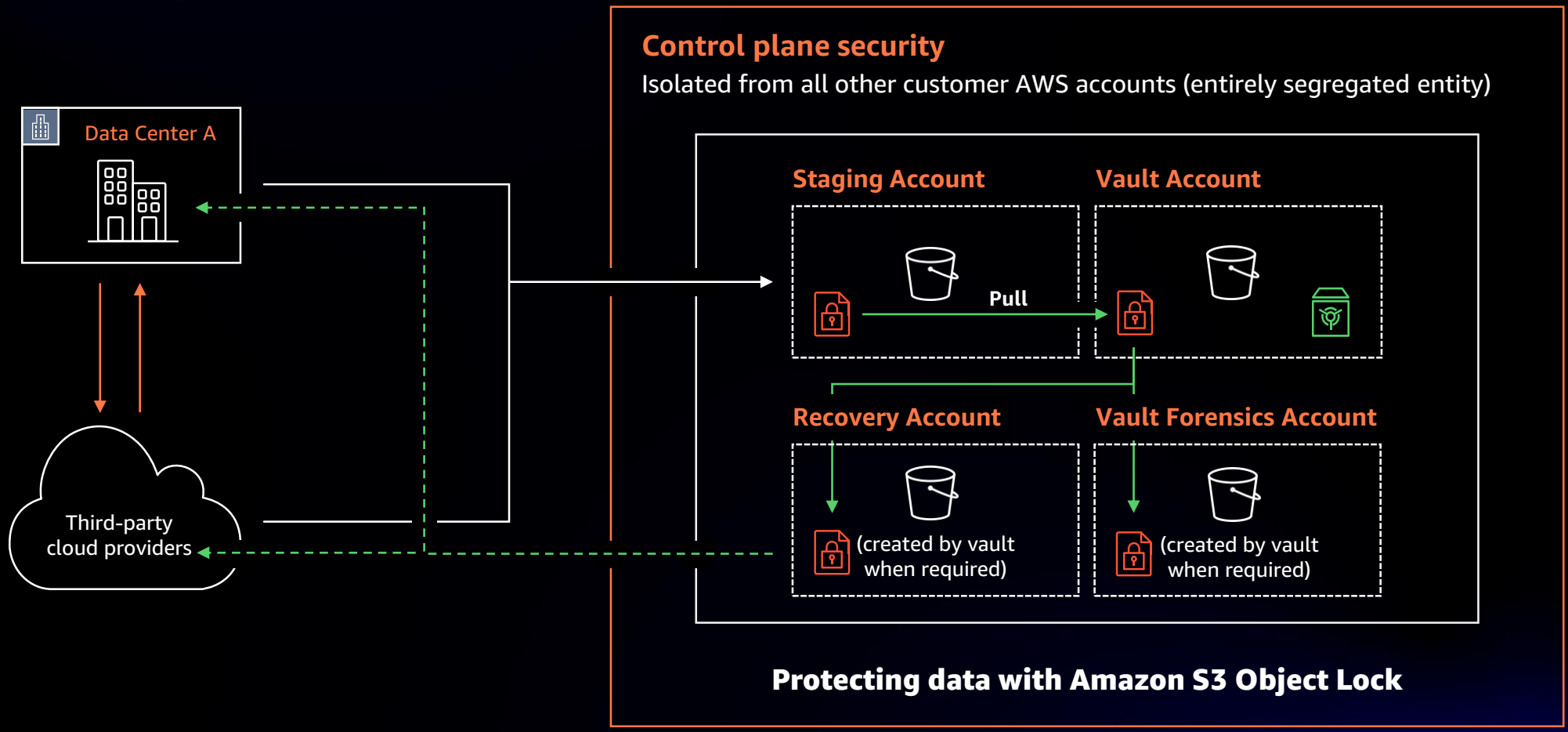






© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use air-gap-like secure backup account architecture



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Immutability and ephemerality

- **Build security checks** into your deployment pipelines including AWS CloudFormation Guard to check for insecure configurations
- Utilize AWS CloudFormation to define and build your **infrastructure as code** so you can easily audit and redeploy if needed
- Build **immutable** infrastructure with no human access using tools like AMI Builder, AWS Auto Scaling groups, and Amazon CloudWatch Logs to help ensure configuration doesn't change after deployment, redeploy if changes are needed

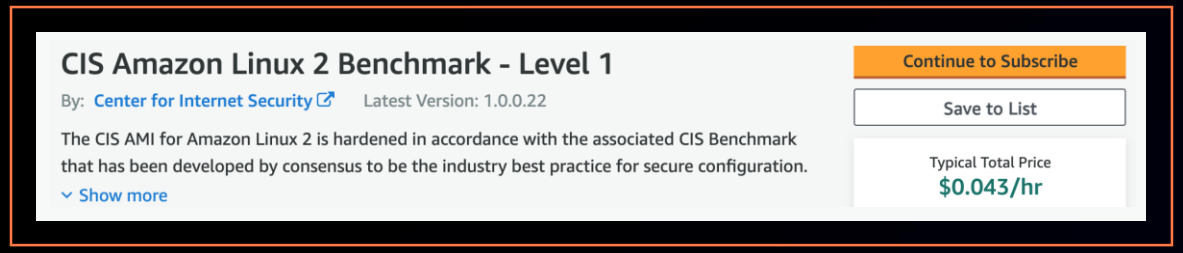
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Harden OS and application configuration

aws marketplace



CIS Center for Internet Security®



Benchmarks available for: Linux

ubuntu

Red Hat Enterprise Linux

Windows

debian

amazon

CentOS

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NIST Cybersecurity Framework

Consists of standards, guidelines, and best practices to manage cybersecurity risk.

Partners strengthen each function of the framework



Identify

Identify an organization's critical functions, assets, and processes and how cybersecurity risks could disrupt them



Protect

Define safeguards necessary to protect critical infrastructure services



Detect

Implement the right measures to identify issues and cyber risks promptly



Respond

Define the measures necessary to react to an identified issue



Recover

Strategic plans to restore and recover any capabilities damaged during a cybersecurity incident

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Leverage partners to work out your “muscle groups”



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identify



- Identify your assets, risks, environments, and supply chain entry points
- AWS manages the physical assets that comprise the AWS Cloud infrastructure
- Achieve deep visibility and asset inventory
- Query and obtain visibility of AWS service assets

AWS Services



AWS Console

AWS Partners

orca security

paloalto NETWORKS

RAPID7

RSA Archer

tenable

Lacework

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Protect

- Take the steps to protect assets you've identified
- Limit access to authorized users, processes, or devices, and to authorized activities and transactions

AWS services

AWS Identity and Access Management (IAM)

AWS Partners

Barracuda Your journey, secured.

CLOUD STORAGE SECURITY

Forcepoint

proofpoint.

Identity Partners

CYBERARK

SailPoint

PingIdentity

okta

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detect



- You need to be able to detect attempts to get into your assets
- AWS can help with a security operations strategy

AWS Services


Amazon VPC


AWS CloudTrail


Amazon Macie


Amazon CloudWatch


Amazon GuardDuty


Amazon Inspector

AWS Partners

Check Point SOFTWARE TECHNOLOGIES LTD

FIREEYE

IBM

paloalto NETWORKS

RAPID7

radware

splunk>

sumo logic

tenable

Qualys.

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Respond

- Respond to anomalies, outliers, or possible breaches
- AWS policies to address purpose, scope, roles, responsibilities, and management commitment

AWS services

- AWS Config
- AWS Step Functions
- AWS Security Hub
- AWS Systems Manager
- AWS Lambda

AWS Partners

Check Point SOFTWARE TECHNOLOGIES LTD
CROWDSTRIKE
SentinelOne
SOPHOS
paloalto NETWORKS
zscaler

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recover



- Have a plan in place to recover if impacted
- Recover from events quickly and with minimal (if any) disruption
- Auto Scaling groups across multiple Availability Zones

AWS services


AWS Backup


Amazon CloudWatch


AWS CloudEndure


AWS Lambda

AWS Partners

Barracuda
Your journey, secured.

COHESITY

DELL

NetApp®

rubrik

VERITAS

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How AWS Partners help ransomware defense



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Partner ransomware categories

- DDoS detection and mitigation
- Centralized event management
- Monitoring and reporting
- Emergency response to issues
- Email security
- Endpoint agent
- Identity
- Incident response
- Multi-layer security
- Data backup
- Zero day
- Network protection
- Multi-vector events
- Next-gen network security
- OWASP top 10

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Wide selection of security partners



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Level 1 MSSP Competency overview

- Launch new competency in Fall 2021
- For both technology and consulting partners
  - ISVs with 24/7 managed service
  - SIs



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Managed Security Service (MSSP) Competency Partners

PROVIDE 24/7 SECURITY PROTECTION AND MONITORING OF ESSENTIAL AWS RESOURCES

PROFICIO

REDBEAR

Capgemini

pwc

CloudHesive

claranet

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security best practices for ransomware protection

1. Patch and harden systems
2. Continuously strive for least-privilege access
3. Use a multi-account strategy and network segmentation to limit scope of impact
4. Develop and exercise an incident response plan
5. Perform self-assessments



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“Business leaders have a responsibility to strengthen their cyber defenses to protect the American public and our economy.”

Anne Neuberger

Cybersecurity Adviser, National Security Council

June 2021

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“There are two ways to learn incident response. One will be chosen for you.”

Beetle@amazon.com
AWS Security

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudEndure ransomware success story

- Unauthorized user gained access via Windows Server 2008
- Once compromised, ransomware moved laterally and spread to additional servers
- CloudEndure was not fully set up
- The customer was able to recover the application data

OUTCOME: Despite not being fully set up, the customer with the help of Cloud303 was able to recover their servers and data leveraging CloudEndure and avoid paying a ransom

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Let’s beat ransomware as a team

- **Join our ransomware marketing campaign**
- **Join the AWS Security Competency**
  https://aws.amazon.com/security/partner-solutions



Create joint offerings

Talk to us!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Dudi Matot

dmatot@amazon.com

Merritt Baer

merrbaer@amazon.com
@merrittbaer (Twitter)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.