AWS re:Invent

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

GPS308

Protect yourself and your customers from ransomware

Henry Axelrod
Principal Partner Solutions Architect
AWS

Girish Chanchlani
Senior Partner Solutions Architect
AWS

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

Agenda

Importance of ransomware protection

What needs to be protected

Important services and features for ransomware

Solutions for protection

Call to action

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

Cybersecurity is increasingly important

75% of IT organizations will face one or more ransomware events **by 2025**

Source: Gartner 2021 study, gtnr.it/3vR5oKh

Analysts are estimating that ransomware events could occur every **11 seconds** in 2021 and result in financial loss of up to **$20B**

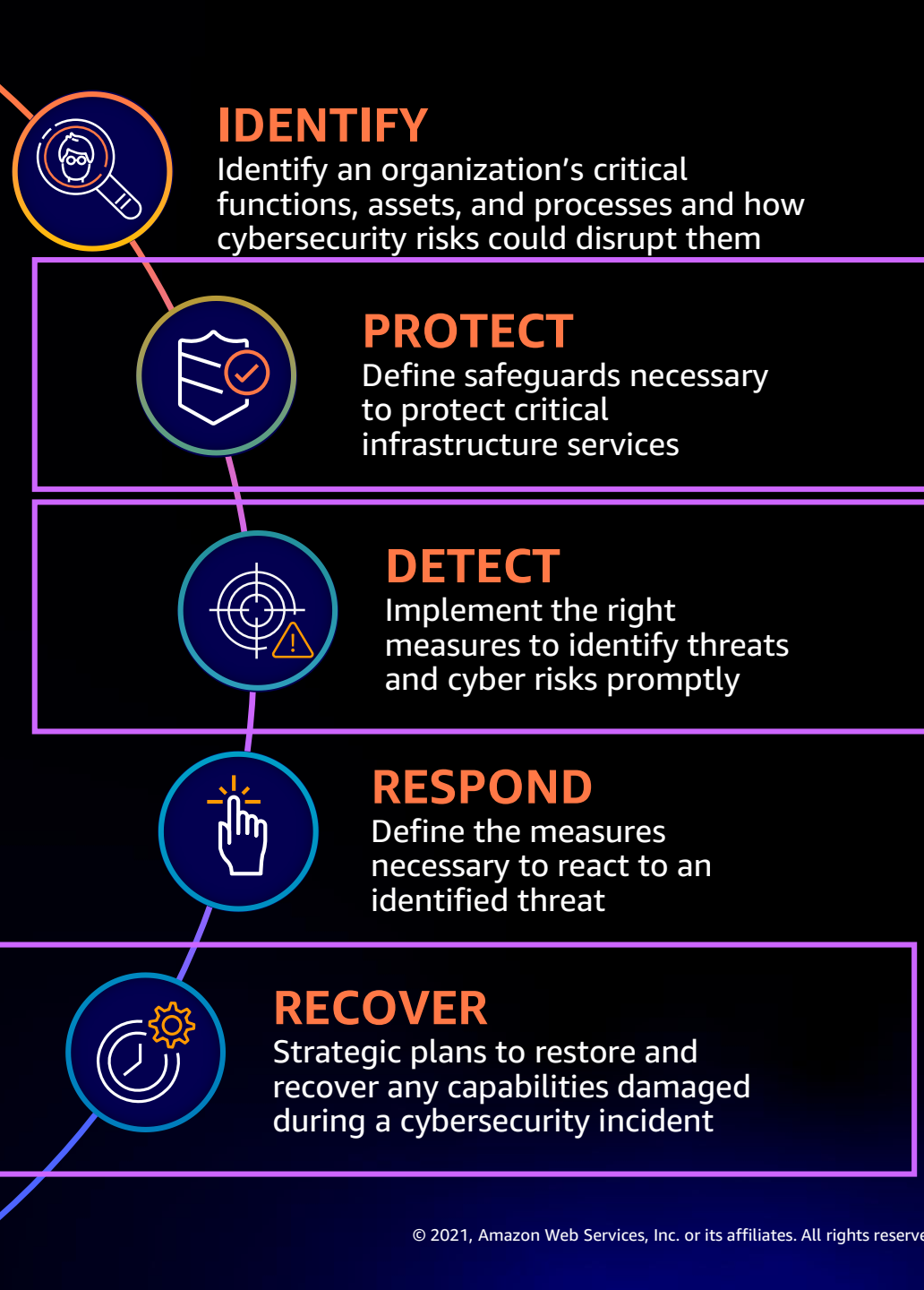
Source: Cybercrime Magazine, cybersecurityventures.com/cybersecurity-market-report/

aws

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

NIST Cybersecurity Framework

- is the industry standard,
- . . . but most companies lack a recovery strategy



aws

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

Ransomware recovery strategy formation

Identifying select data to be prioritized and associated trade-off with size, time to recover, and cost

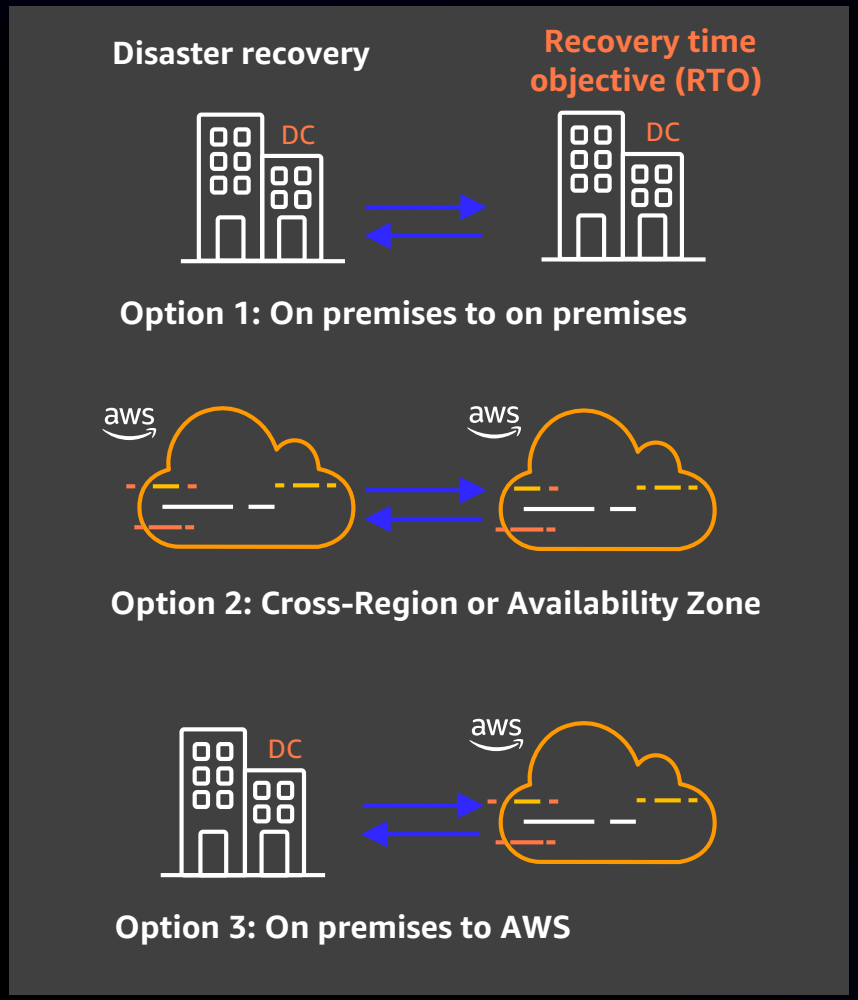


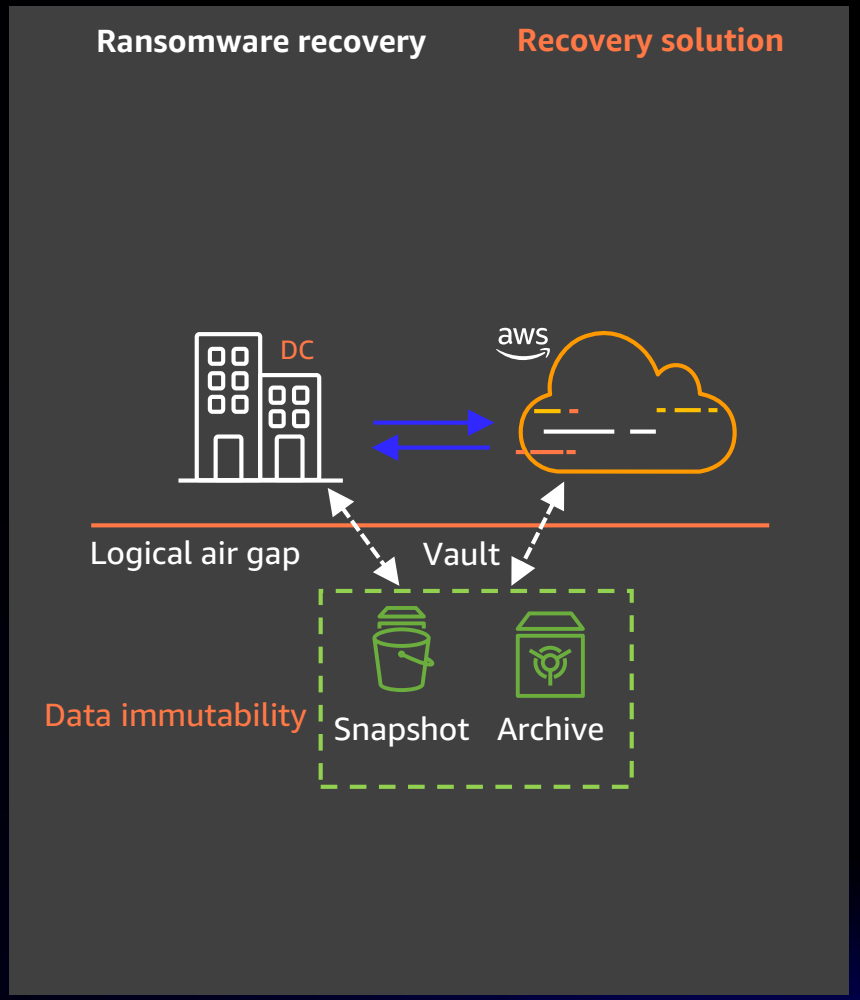
Selecting the AWS services and/or AWS Partners with the capability for vaulted data artifacts to be immutably stored

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

Disaster recovery – Ransomware recovery

EXPANDING ON DISASTER RECOVERY





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

AWS services

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

Amazon S3 storage classes



S3 Standard

Active, frequently accessed data

Milliseconds access

≥ 3 AZ

$0.0210/GB



S3 Intelligent-Tiering

Data with changing access patterns

Milliseconds access

≥ 3 AZ

$0.0210 to $0.00099/GB

Storage up to 95% less than S3 Standard*



S3 Standard-IA

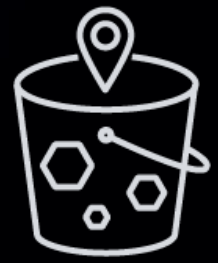
Infrequently accessed data

Milliseconds access

≥ 3 AZ

$0.0125/GB

Storage ~40% less than S3 Standard*



S3 One Zone-IA

Re-creatable, less accessed data

Milliseconds access

1 AZ

$0.0100/GB

Storage ~20% less than S3 Standard-IA*



S3 Glacier

Archive data

Minutes or hours access

≥ 3 AZ

$0.0040/GB

Storage ~78% less than S3 Standard-IA*



S3 Glacier Deep Archive

Archive data

Hours to access

≥ 3 AZ

$0.00099/GB

Storage ~75% less than S3 Glacier*

Frequent — **Access frequency** — **Infrequent**

aws

*Storage cost only; does not include access, retrieval, or other fees and minimums.

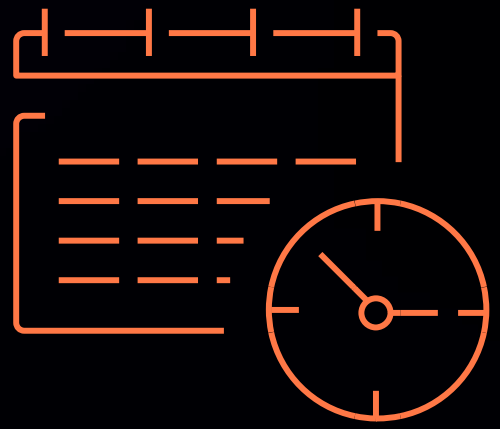
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 Object Lock



Immutable objects in S3

Assessed for SEC compliance by Cohasset Associates



Retention controls

Down to the object and object version levels



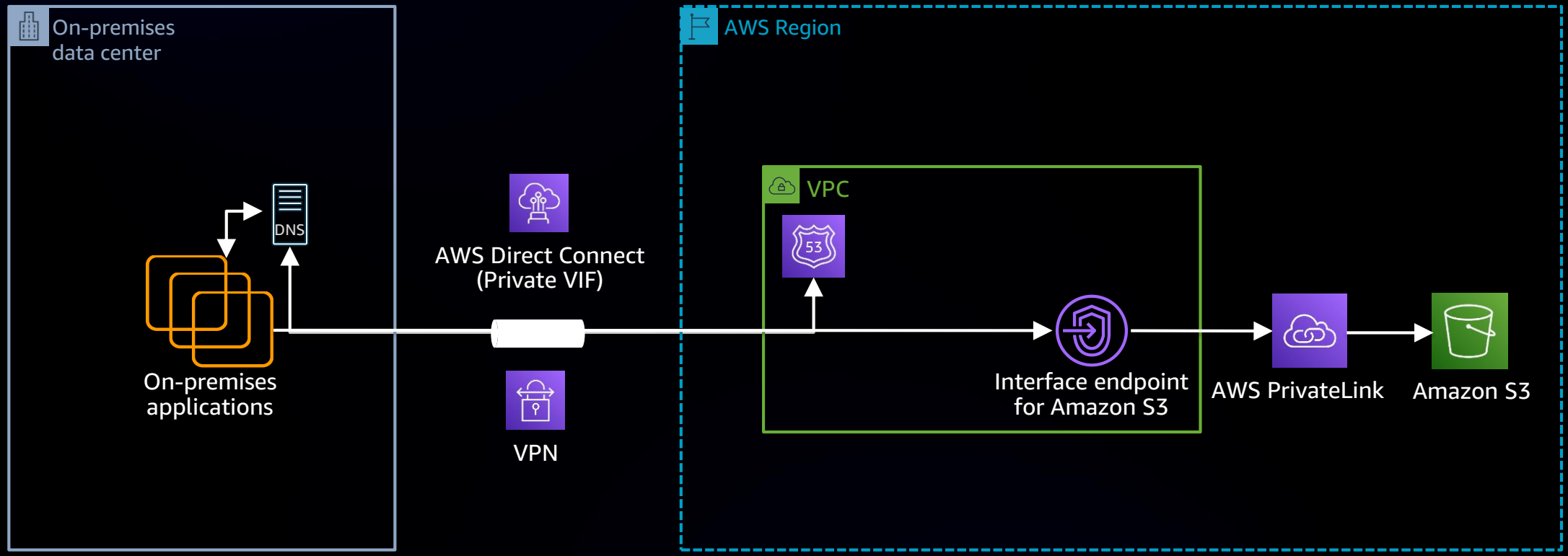
Auditing and visibility

Track, report, and alert on access and retention changes

aws

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

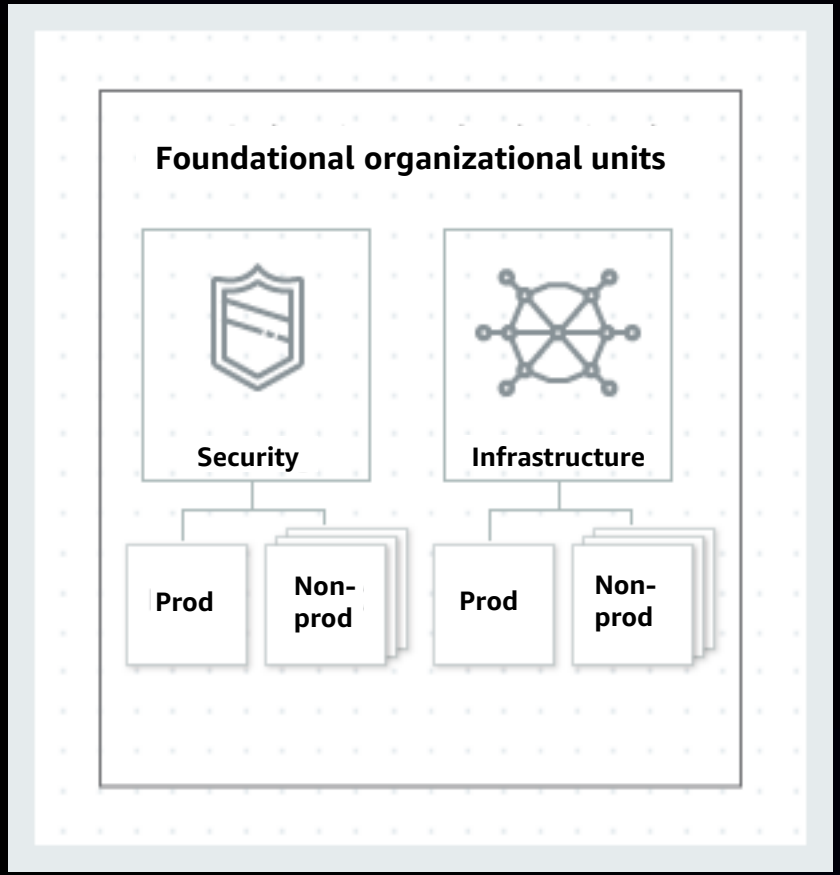
AWS PrivateLink for Amazon S3

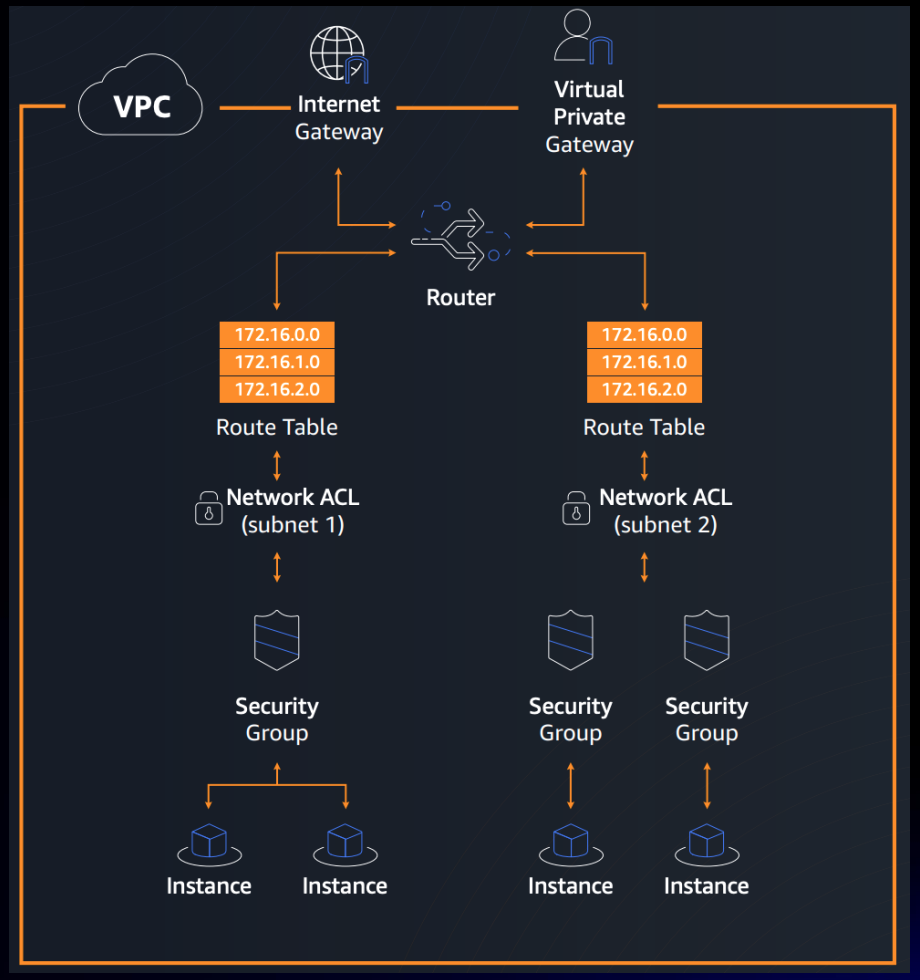


Private connectivity to Amazon S3

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

Multi-account strategy and network segmentation





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

Technology partner solutions

© 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
- Have backup servers in the **cloud**

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

Customer-deployed solutions

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

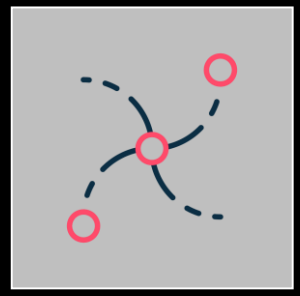
Commvault ransomware protection



Intelligent adaptive
anomaly detection



Immutable data via
S3 Object Lock

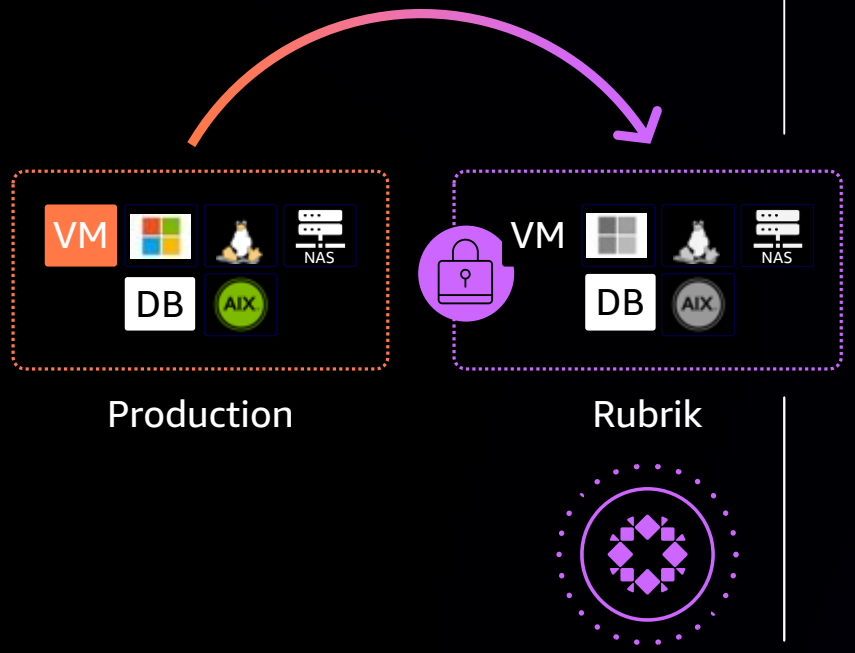


Automated action
for rapid response

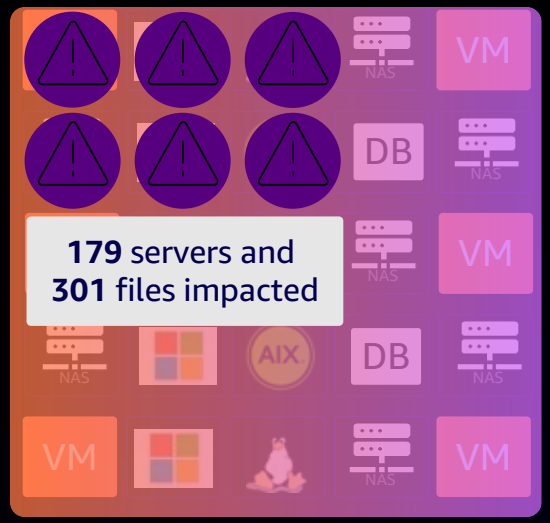
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Rubrik ransomware protection

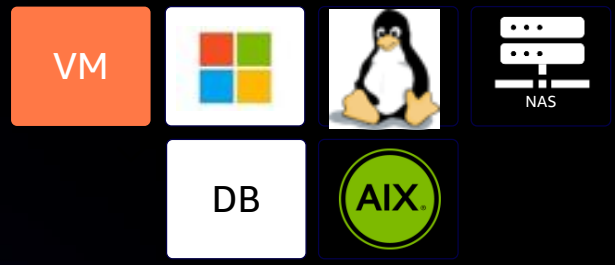
Immutability
Safeguard backups



Impact visibility
Reduce data loss



Instant recovery
Lower RTOs



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

Veeam ransomware protection

SureBackup



Check for malware during
backup verification

S3 Object Lock



Veeam leverages this in
Capacity Tier and Archive Tier

Secure Restore



Scan system before
restoring to production

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

Veritas ransomware protection

Protect

Safeguarding data and integrity with system hardening and immutability

- Management data encryption
- Encrypted backups (AES 256-bit, FIPS 140-2)
- Immutable storage with S3 Object Lock
- Encrypted backup
- RBAC

Detect

Monitoring and reporting on system activity to mitigate threats and vulnerabilities

- Backup monitoring and recovery readiness
- Discovery of new VMs so they can be protected
- Mapping of critical systems to applications
- Anomalous app/compromised account detection

Recover

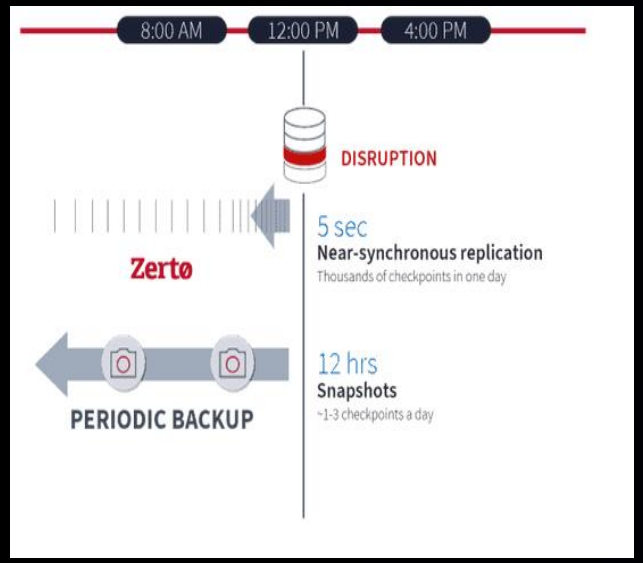
Automating and orchestrating complete cross-system restoration

- Full, instant, granular, and self-service
- Automated recovery at scale
- NetBackup orchestration
- Non-disruptive recovery rehearsals
- Continuous data protection
- Replication

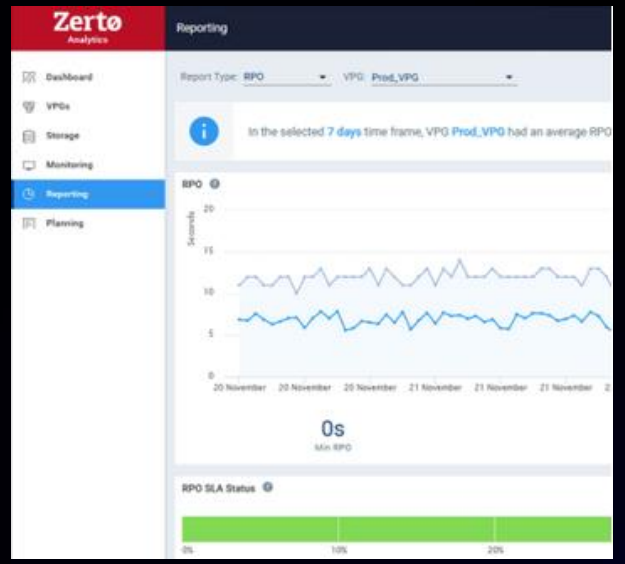
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Zerto ransomware protection

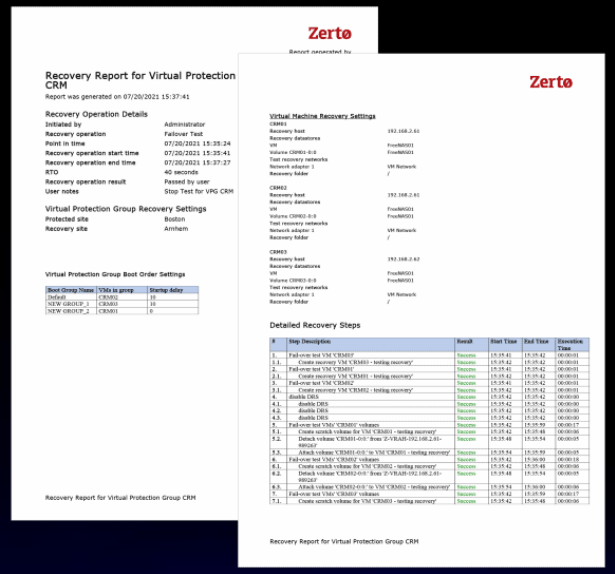
Continuous protection and periodic backups to S3 with S3 Object Lock for immutability



Analyze malicious activities via Zerto Analytics

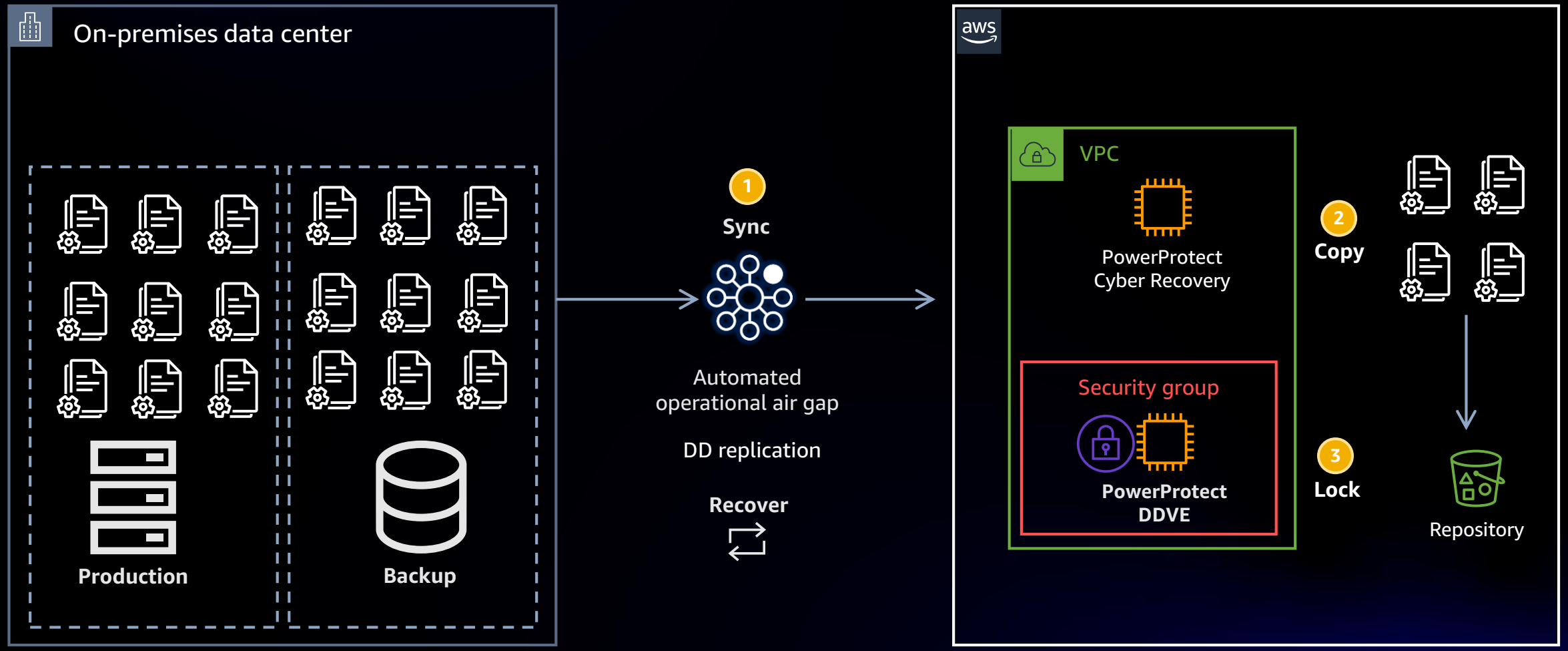


Recover at scale with compliance reporting



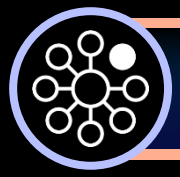
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing Dell EMC PowerProtect Cyber Recovery



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

Dell EMC ransomware protection



Operational air gap for off-site data isolation



Flexible deployment and recovery options



Multi-layered enhanced cloud security with AWS



Automated, orchestrated operation with a modern UI



Reliable, proven protection with PowerProtect DD Virtual Edition



Software-based immutability protects data from corruption, deletion, or destruction

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

SaaS solutions

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

Cohesity ransomware protection



User

Production apps servers

Immutable file system

Protect

- Backup immutability via DataLock
- Role-based access control/MFA
- Encryption framework
- Reduce attack surface
- AD protection

Detect

- Machine-driven anomaly detection
  - Backup data
  - Unstructured data
- Automated alerts
- Vulnerability scanning

Respond

- Scalable file system to store years' worth of backup copies
- Global actionable search
- Instant mass restore

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

Cohesity ransomware recovery as a service



Air-gapped vault

Immutable snapshots
Copy data of Cohesity vault
Isolated environment
Data lock



Ransomware detection

Detect ransomware anomalies
Restore from clean PIT
Auto-block malicious users, content and sources



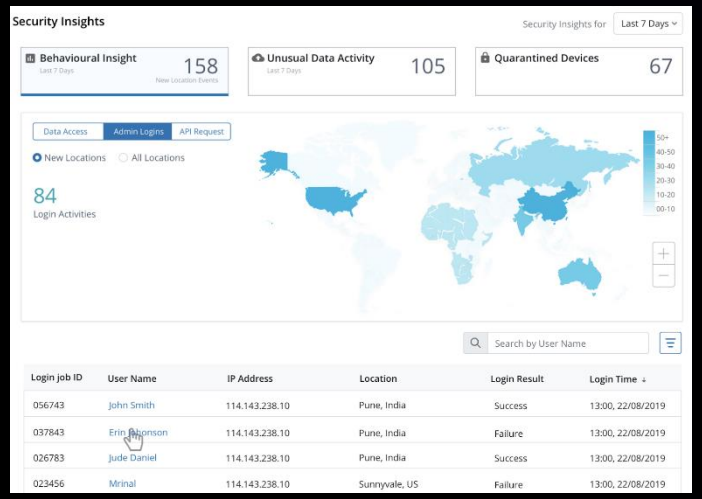
Sandbox

Environment to simulate event
Scan and test for known vulnerabilities

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

Druva ransomware protection

Detect
Access insights and anomaly detection





Respond
Orchestrate and automate quarantine

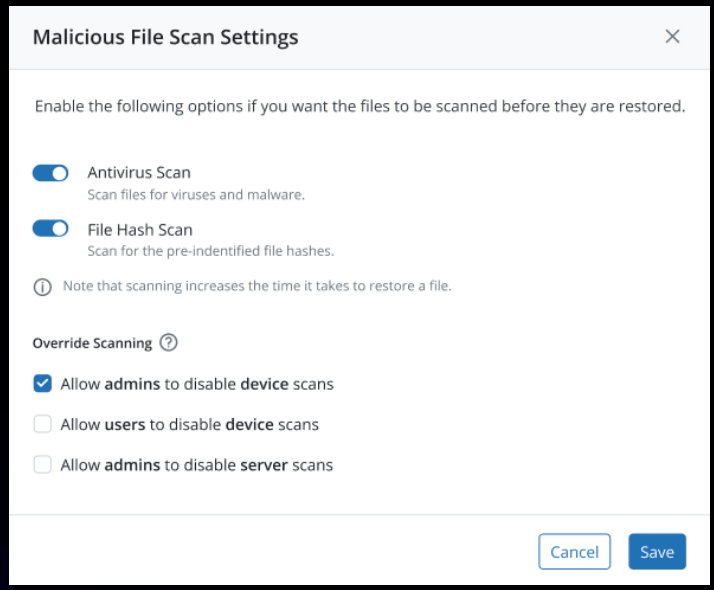


Built-in integrations with:

paloalto NETWORKS

FIREEYE

Recover
Recovery scans and curated snapshots for clean, uninfected data



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

Many more storage solutions provide ransomware recovery

Primary storage partners

ctera

NASUNI

panzura

Backup and recovery partners

CLUMIO

MSP360
#1 MSP BACKUP

N2WS

AWS services



AWS Backup



CloudEndure
Disaster Recovery

aws

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

Call to action

Create a plan for ransomware

Consider ransomware with your backup and DR strategy

Review AWS services and features that can help

Follow security best practices

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

Additional resources

AWS Cloud Security Resources Hub
amzn.to/3gcnv6W

Building a Threat Detection Strategy in AWS
bit.ly/3k1GNNl

Aligning to the NIST CSF in the AWS Cloud
bit.ly/3AQc3WC

AWS Security Incident Response Guide
bit.ly/3sq7mj6

AWS Well-Architected Framework – Security Pillar
amzn.to/3m9bfI3

Securing Your AWS Cloud Environment from Ransomware ebook
bit.ly/3zgaSz9

The Cybersecurity and Infrastructure Security Agency (CISA) publications
www.cisa.gov/stopransomware

Classic Intrusion Analysis Frameworks for AWS Environments: Application and Enhancement
go.aws/3EpBvEa

aws

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

Other related sessions

STG203 – Backup, disaster recovery, and ransomware protection with AWS

SEC308 – Use AWS to improve your security posture against ransomware

SEC320 – Detecting ransomware with AWS security services

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

Thank you!

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