Louisville AWS MeetUp

- Welcome
- Thank you Humana for hosting
- Our vision for this group
    - Monthly gatherings
    - Building community
    - Gain skills
    - Connecting talent to opportunity
    - Learn from each other
    - Member driven

After this: Troll Pub

Future Topics

- General AWS talks and demos
- Data analytics/Redshift
- Discussion on Training and Skill building (Free resources, how to leverage)
- Networking
- Resiliency
- Cost Optimization
- Serverless
- AWS Certs/training round table
- Security
- **Presentations from you - Your topics and Your work**

- **NOVEMBER – Kubernetes on AWS using EKS**

aws migrations

Ransomware Protection and Recovery

Brian Stucker
Sr. Security & Compliance SA

Agenda

- What is ransomware?
- Best practices for ransomware protection
- Best practices for ransomware related backup and recovery
- Where can I go for further learning?

What is ransomware?

aws migrations

What is ransomware?

Ransomware refers to a business model in which unauthorized users utilize a range of associated technologies to extort money from entities

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

The restriction is accomplished by the unauthorized user who

- **Encrypts** data using actor-controlled encryption keys
- Uses access controls to **lock out** the rightful owner from a system
- Threaten to **reveal the data or carry out acts of exfiltration**, which can result in large monetary fines from data privacy authorities, litigation from affected parties, among other potential consequences

Why is ransomware effective?

- Many organizations do not patch, or take too long to patch their systems
- 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
- Multiple attack vectors are being employed

NIST Cybersecurity Framework

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

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 threats and cyber risks promptly

RESPOND

Define the measures necessary to react to an identified threat

RECOVER

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

aws migrations

Why AWS?

AWS HAS MANY SECURITY SERVICES AND FEATURES TO HELP PROTECT AGAINST RANSOMWARE

- Use **partner security products** such as CrowdStrike Falcon and Trend Micro Deep Security to help protect you instances.
- Use Amazon GuardDuty for detecting **threats** or anomalous **activity**.
- Use AWS Security Hub to **automate security checks** and centralize findings
- Use Amazon Detective to **investigate** GuardDuty and Security Hub findings

Why AWS?

AWS MANAGED SERVICES AND OBJECT LOCKS

- Utilize **managed services** that don't require traditional patching such as Amazon API Gateway, AWS Lambda, Amazon DynamoDB, or Amazon Aurora
- Utilize services like DynamoDB and Aurora have **point in time recovery** features
- Utilize **Amazon S3 object lock** which offers Write Once Read Many (WORM) for objects stored in S3. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely
- Utilize **Glacier vault lock and vault access policies** that allow you to implement time-based data retention rules (deny deletes), and grant read access to designated parties (allow reads)

Why AWS?

IMMUTABLE AND EPHEMERAL INFRASTRUCTURE

Build for the cloud by embracing immutable and ephemeral architectures, some examples include:

- **Build security checks** into your deployment pipelines including AWS CloudFormation Guard to check for insecure configurations

- Utilize CloudFormation to define and build your **infrastructure as code** so you can efficiently 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, re-deploy if changes are needed

5 Best practices for ransomware protection

aws migrations

5 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

aws migrations

1. Patch and harden systems

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.

- Use Amazon Inspector to identity vulnerabilities and assess instances against security benchmarks
- Use Amazon ECR Image scanning to identity vulnerabilities and assess your container images.
- AWS Systems Manager Patch Manager to deploy OS and software patches automatically
- Use endpoint workload protection software on your instances in "Protect" mode

2. Continuously strive for least privilege

STATIC CREDENTIALS AND OVERLY PERMISSIVE POLICIES REMAIN ONE OF THE TOP SECURITY RISKS.

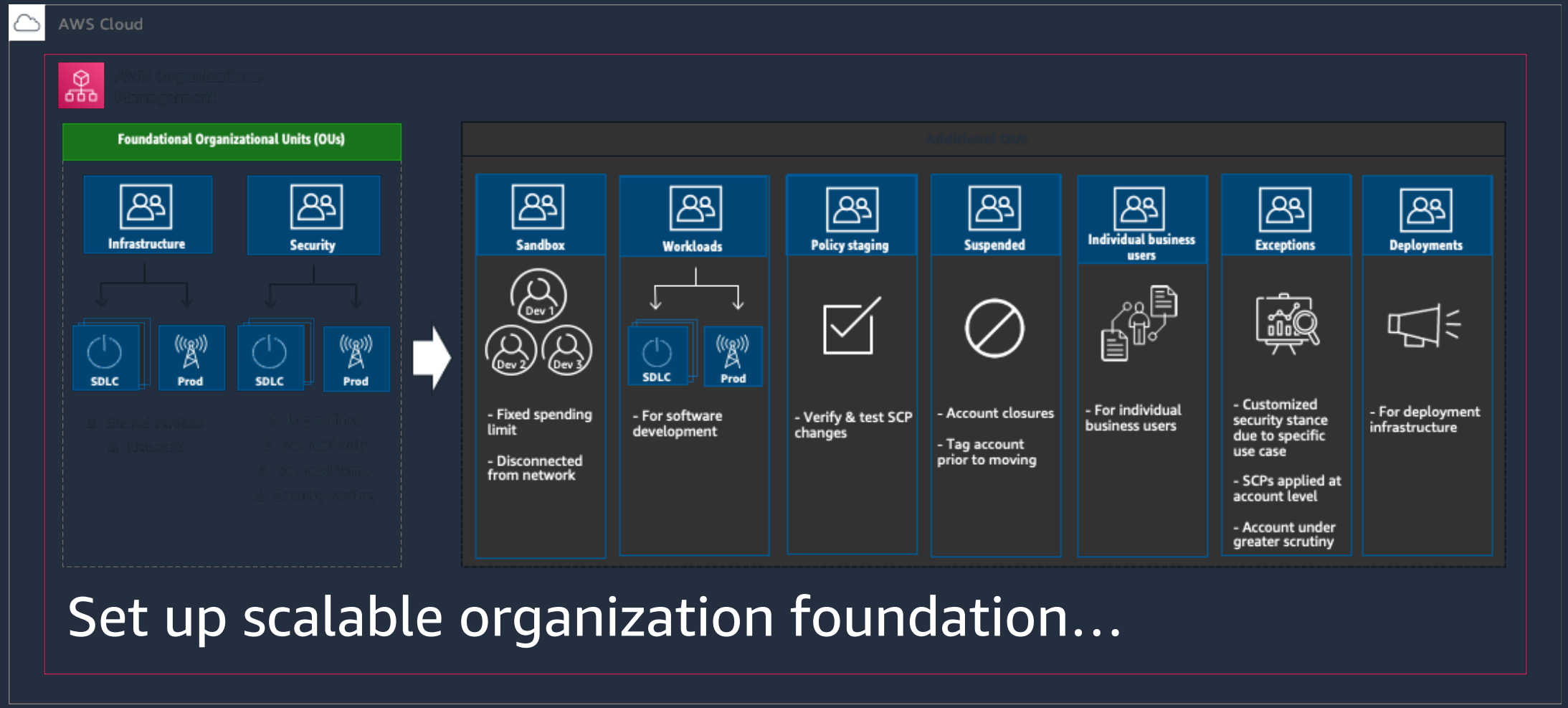
There are several services and features that can be used to mitigate these risks.

- **Eliminate** or minimize static IAM credentials
- **Federate** access using AWS SSO or existing federation provider
- Move to **least privilege** IAM roles and policies using **IAM Access Analyzer** to scope down permissions
- Utilize service control policies (SCPs) to **reduce access**

3. Use a multi-account strategy and network segmentation

» https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/

AWS Security Reference Architecture



Set up scalable organization foundation…

4. Develop and exercise your incident response plan

People

- ✓ Train security operations staff on AWS

Process

- ✓ Develop an incident response plan and strategy
- ✓ Run drills and automate simulations where possible

Technology

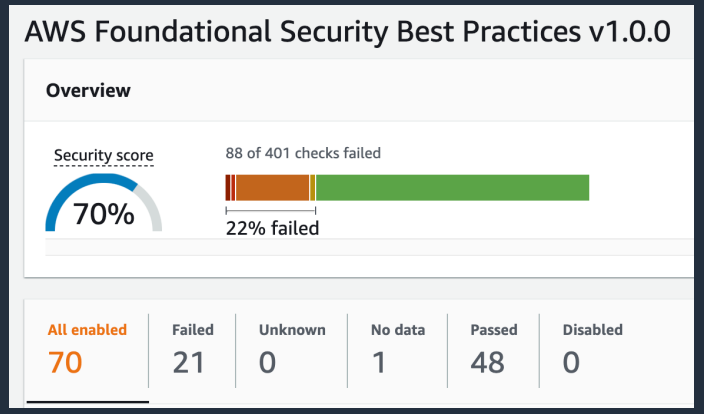
- ✓ Build AWS Accounts for: Security Operations & Log Archival
- ✓ Create read only and break glass roles for access to AWS accounts
- ✓ Setup security services like Amazon GuardDuty, AWS Security Hub to detect threats
- ✓ Use security services like Amazon Detective to help you investigate security findings.

5. Perform self assessments

AWS Well-Architected

Learn, measure, and build using architectural best practices

AWS Security Hub



awslabs / aws-security-assessment-solution

These security assessments are from the open source projects "Prowler" and "ScoutSuite," which include custom modules that **check for ransomware specific findings**.

aws migrations

Best practices for ransomware related backup and recovery

aws migrations

Industries are now prioritizing recovery.

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 threats and cyber risks promptly

RESPOND

Define the measures necessary to react to an identified threat

RECOVER

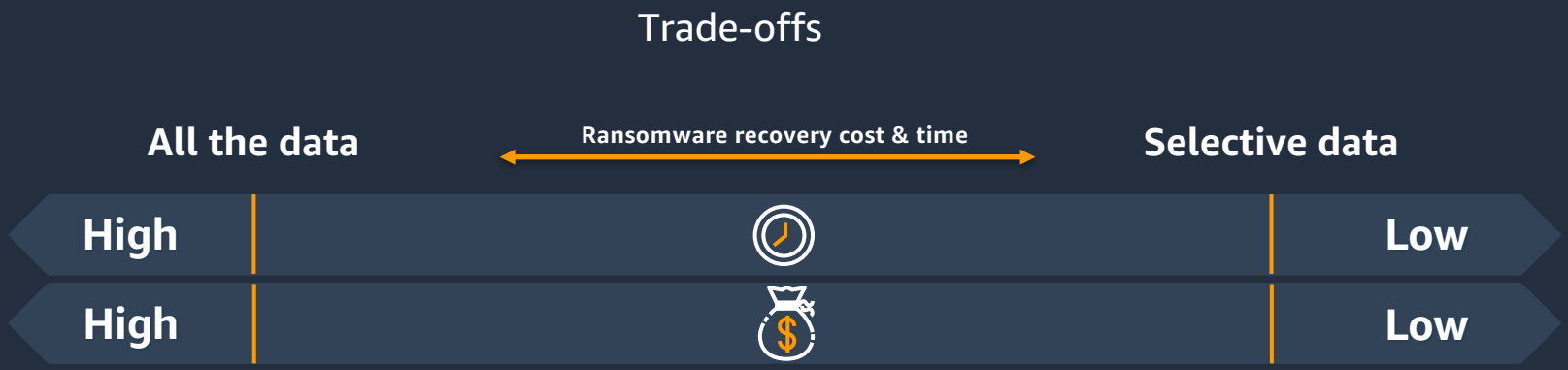
Strategic plans to restore and recover any capabilities damaged during a cybersecurity incident

Strategy formation

- What is the most important data that we want to protect?
- Should the recovery of some data be prioritized over others?
- What is an acceptable recovery time?
- What tradeoffs should be made among budget, time, and data completeness?

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 Amazon Partners with the capability for vaulted data artifacts to be immutably stored

Best practices for ransomware related backup and recovery

- Enable a backup & recover solution
  - AWS Backup
  - AWS Storage Gateway
  - CloudEndure
  - Partner Backup Solutions
- Establish robust backup and restore processes
- Utilize Air-gap “like” secure backup account structure
- Use data storage features to **minimal** downtime

Enable a backup & recovery solution

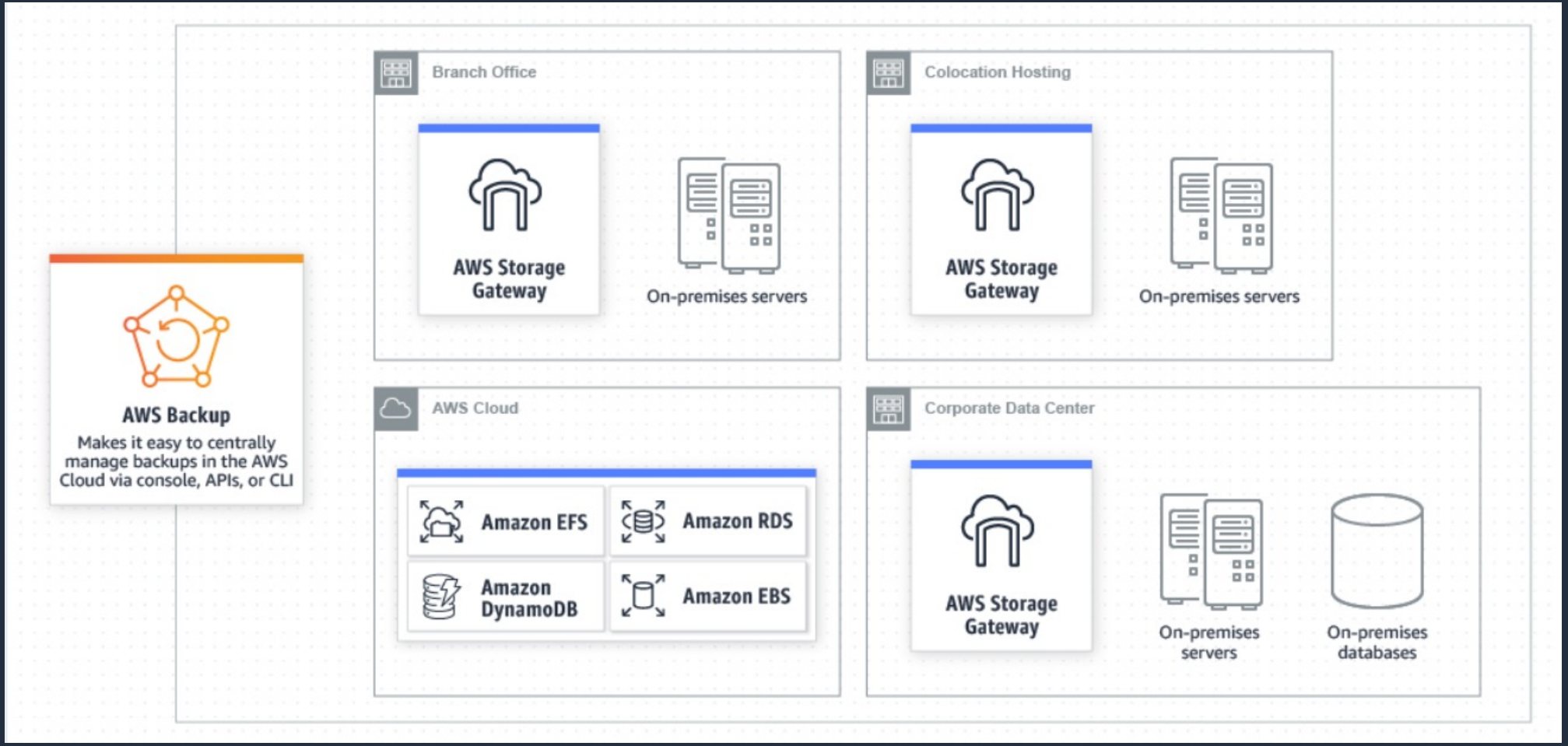
- AWS Backup for the cloud
- AWS Storage Gateway for on-premises
- CloudEndure for both cloud and on-premises
- Partner Backup Solutions

AWS Backup

BACKUP YOUR AWS SYSTEMS AND RESOURCES

AWS Storage Gateway

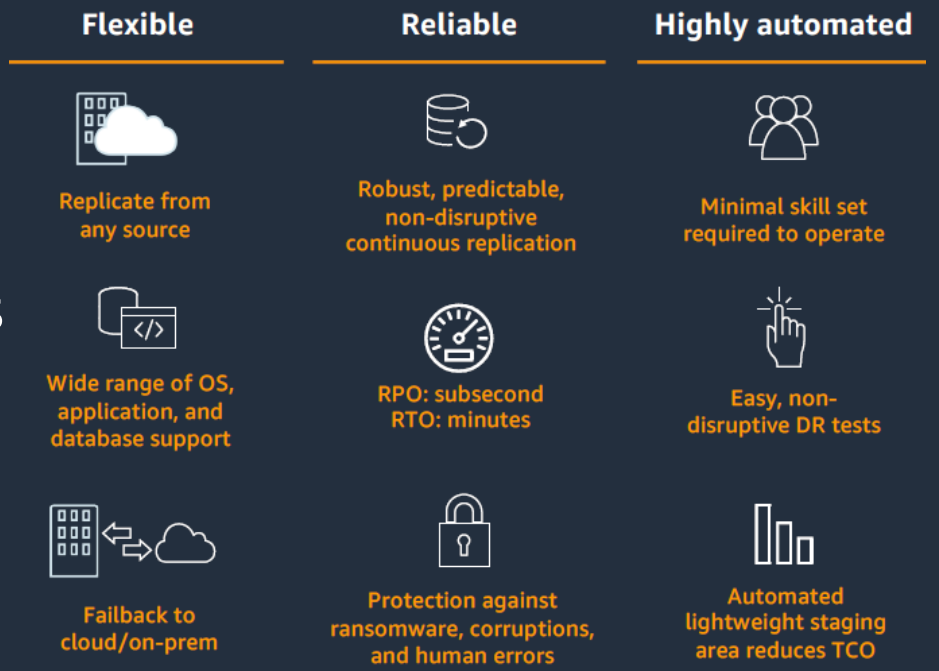
BACKUP YOUR ON-PREMISES SYSTEMS



CloudEndure Disaster Recovery

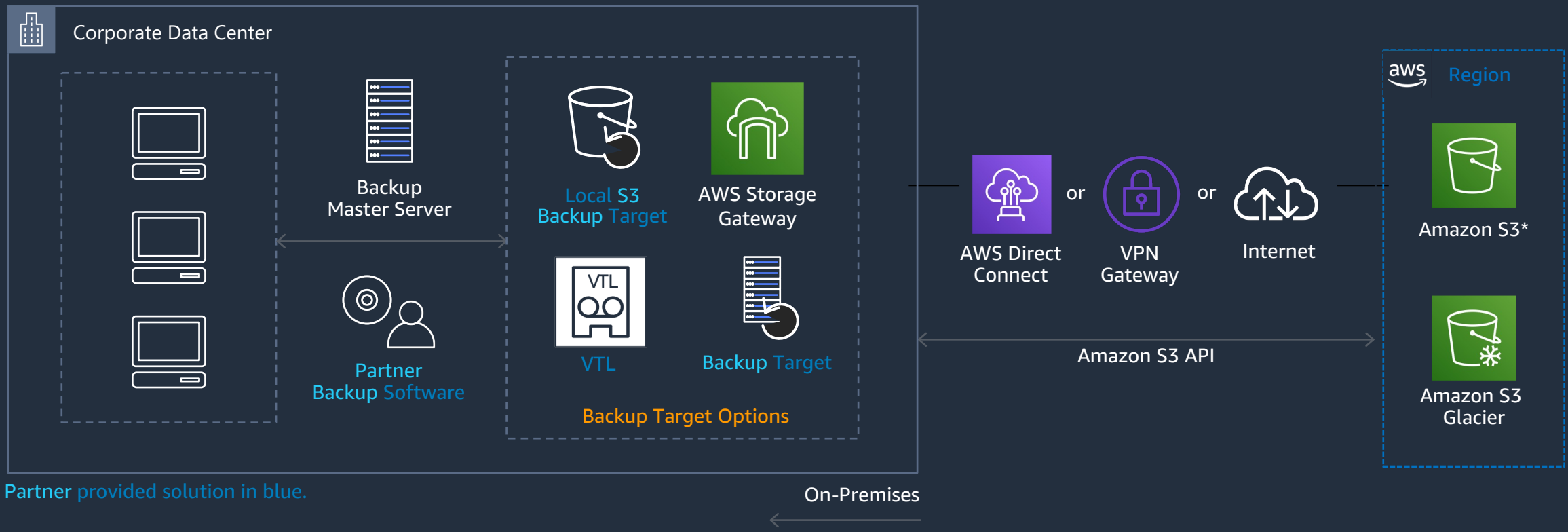
BACKUP AWS OR ON-PREMISES SYSTEMS

- Improve recovery objectives and reduce TCO
- Simple setup lets you start in minutes
- Same highly automated process for all workloads
- Minimizes complexity and reduces risk
- Easy failover and failback



Backup from on-premises to AWS

BACKUP AWS OR ON-PREMISES SYSTEMS WITH PARTNER SOLUTIONS

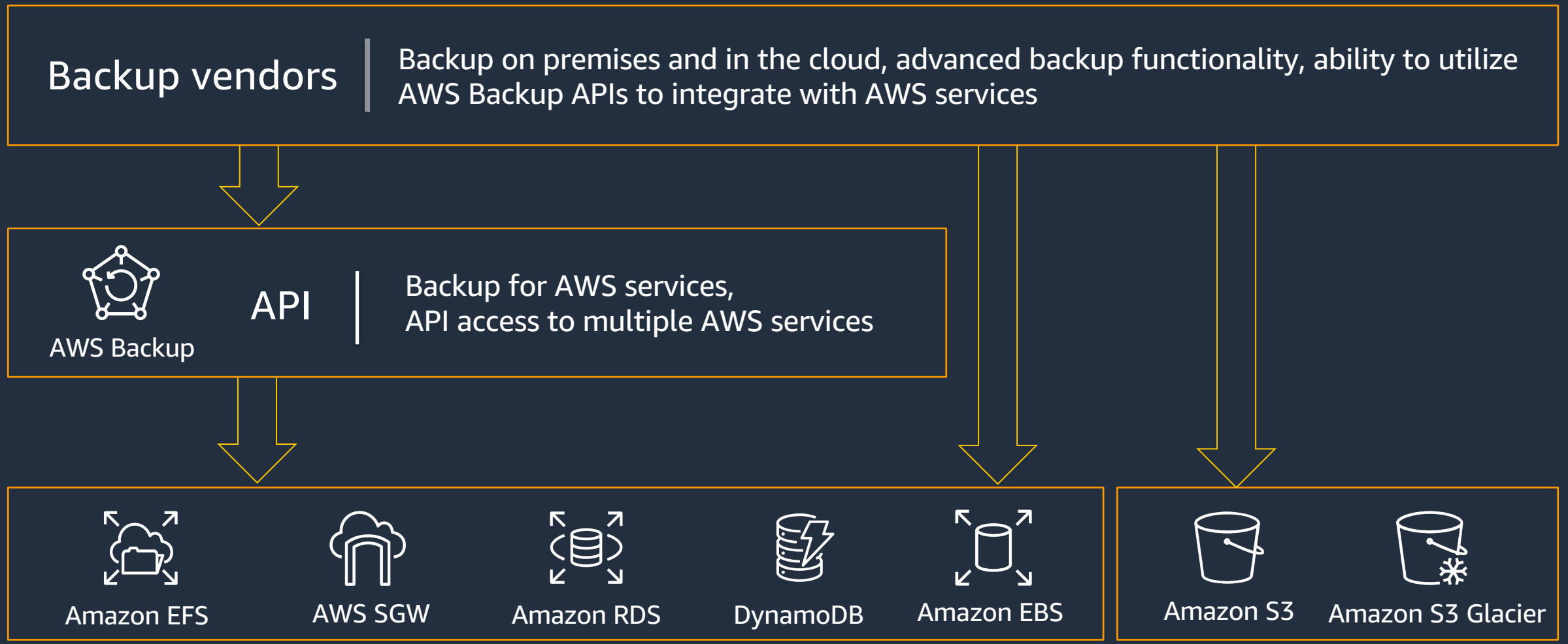


- Backup data flows from on-premises into AWS object storage services
- One of the most common use cases

Partners

CloudBerry Lab · ctera · IBM · CLUMIO · PURESTORAGE · COMMVAULT · DELL EMC · NetApp · VEEAM · COHESITY · druva · rubrik · VERITAS

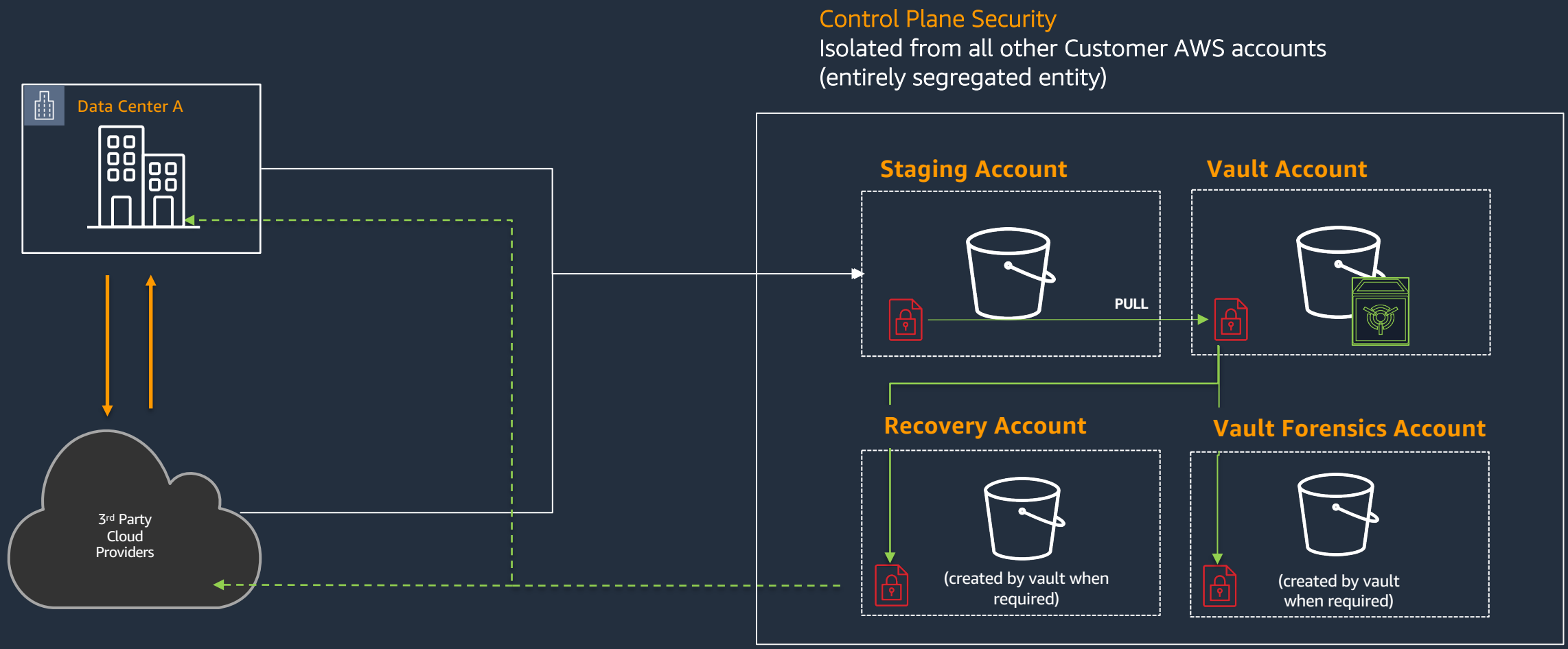
AWS Backup and APN backup partners



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**

Utilize Air-gap “like” secure backup account architecture



Protecting data with Amazon S3 Object Lock

aws migrations

Use managed data/databases services for minimal downtime

WHY MANAGE YOUR OWN BACKUP AND RESTORE PROCEDURES?

- Point-in-time recovery (PITR) for Amazon RDS and DynamoDB
- Amazon Aurora database cloning
- Amazon S3 Object Lock and Glacier Vault Lock

Resources

Community

nomoreransom.org/en/index.html

US federal government

FBI IC3 – File a complaint
www.ic3.gov

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

AWS

AWS Cloud Security Resources Hub
amzn.to/3gcnv6W

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

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

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

AWS Security Incident Response Guide
bit.ly/3sq7mj6

Securing your AWS Cloud environment from ransomware eBook
bit.ly/3zgaSz9

Classic Intrusion Analysis Frameworks for AWS Environments: Application and Enhancement
https://amzn.to/2WqkTeP

aws migrations

AWS offerings and professional services

- AWS Security Assessment
- Security Incident Response Simulations
- Security and Resiliency Table Top Exercise
- AWS Executive Security Simulation
- AWS Professional Services Security Epics
- AWS Security Jam
- Security Specialist Deep-Dive sessions
- Simulated Conditions Response and Management
-

Questions?