AWS re:Invent

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

COP326

Data residency capabilities in AWS Control Tower

Kaushik Mohanty
Business Development and Specialist Sales Leader
AWS

Chuck Chemis
Principal Cloud Architect
Symetra

Jamie St. Onge
Senior Manager, AWS Control Tower
AWS

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

Agenda

- What is data residency, and why it matters
- Setting up a secure AWS environment with AWS Control Tower
- Applying data residency controls today in a regulated industry
- **NEW:** Data residency capabilities in AWS Control Tower
- How to enable data residency in AWS Control Tower
- Get started with AWS Control Tower

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

What is data residency and why it matters

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

Data residency

What?

Data residency is a requirement to store or process data in a particular geographic location

For whom?

Customers in highly regulated industries, public sector and multinational organizations

Part of a modern data strategy

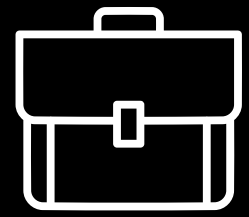


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The data compliance landscape







Regulatory requirements

Contractual requirements

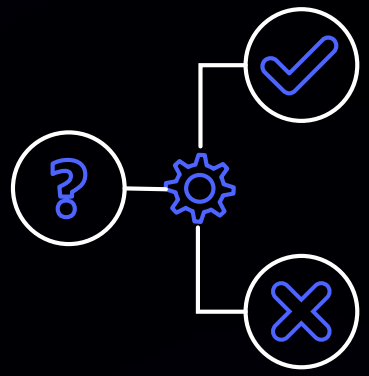
Corporate policies

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

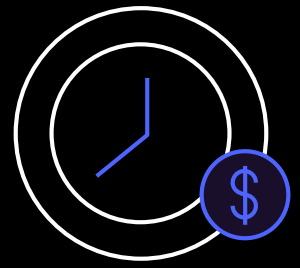
Challenges in implementing data residency



Project delays due to security and compliance concerns



Complexity in interpreting regulations and defining controls



Time and effort to implement and monitor

aws

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

Setting up a secure AWS environment with AWS Control Tower

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

AWS Control Tower

EASIEST SELF-SERVICE SOLUTION TO AUTOMATE THE SETUP OF NEW AWS MULTI-ACCOUNT ENVIRONMENTS



AWS managed service version of multi-account environments



Deployment of AWS best practice blueprints and guardrails



Automated account creation based on AWS best practices

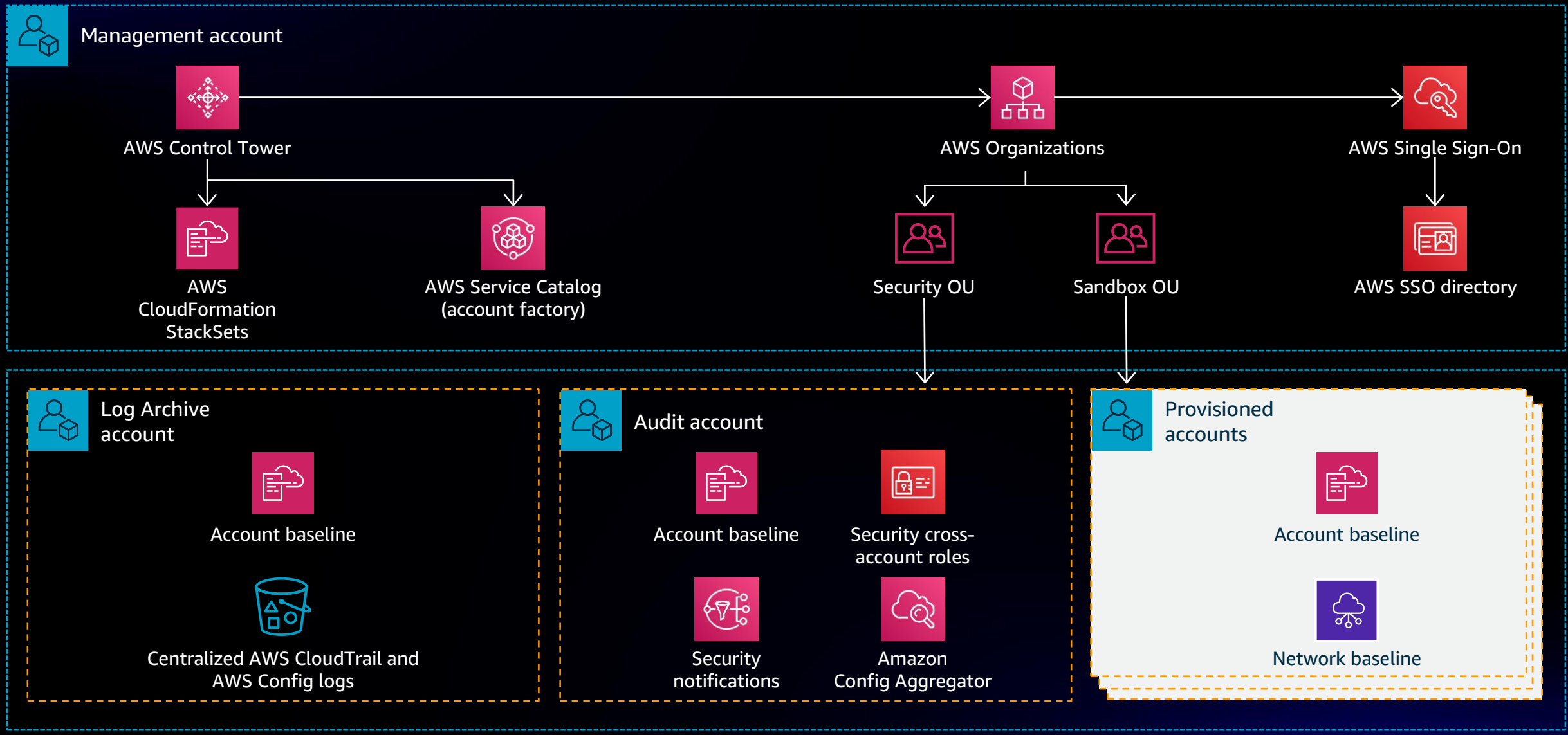


Dashboard for monitoring compliance status

aws

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

Landing zone provisioned by AWS Control Tower



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

How we apply data residency controls today in our regulated industry

Chuck Chemis, Principal Cloud Architect, Symetra

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

About Symetra

SYMETRA®
RETIREMENT | BENEFITS | LIFE

60 years in the business

Symetra has been going strong for more than 60 years. Offering annuities, life insurance, and benefits products to help provide security and confidence to people and businesses nationwide.



Financial Strength

Promises are backed by **$55.5B in assets,** getting “A’s” from rating agencies for Symetra’s ability to meet financial obligations—like paying claims.



Guiding Principles

Value, Transparency, Sustainability—the three principles that define how Symetra does business inside and out.



Commitment to Community

With a focus on women, at-risk youth, and housing and homelessness, Symetra is dedicated to serving the communities where employees live and work.

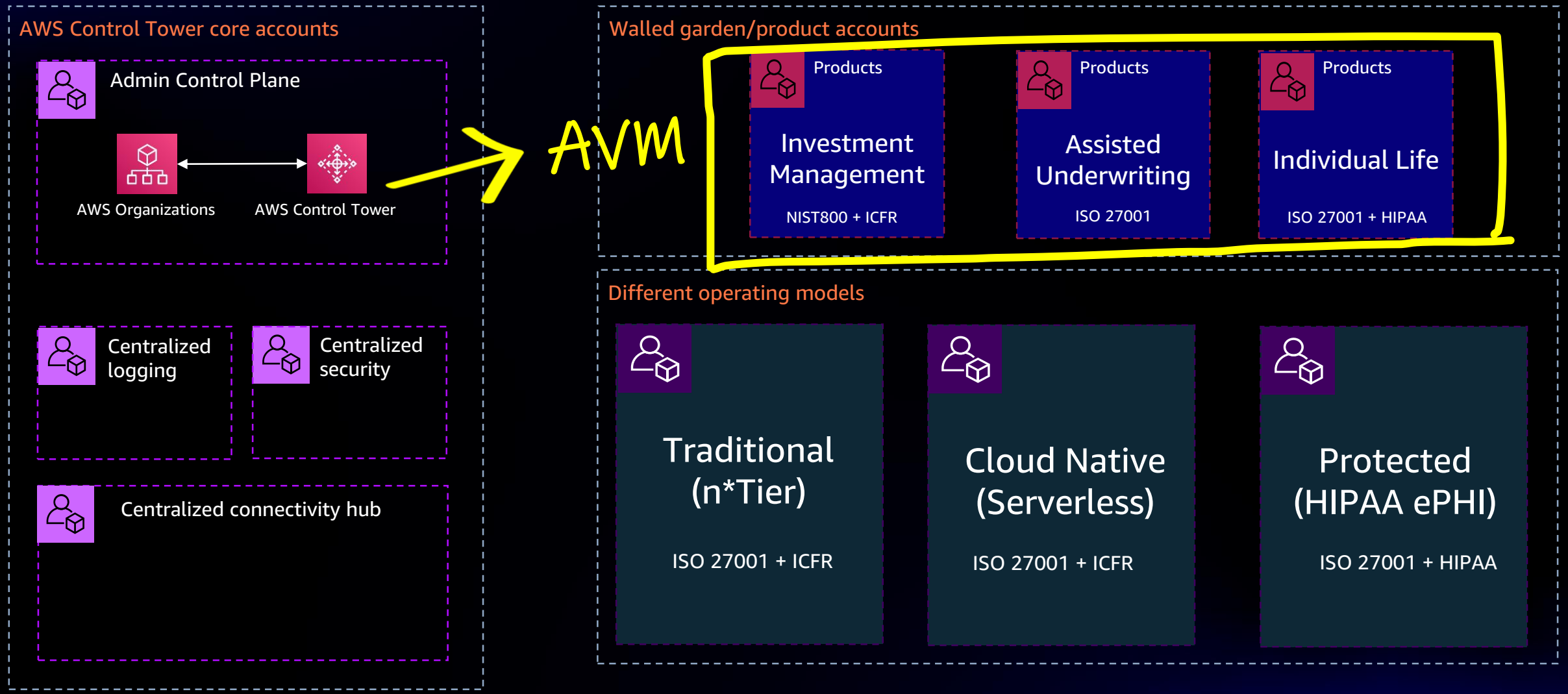
Annuities - Life Insurance

Stop Loss - Select Benefits - Group Life & Disability

aws

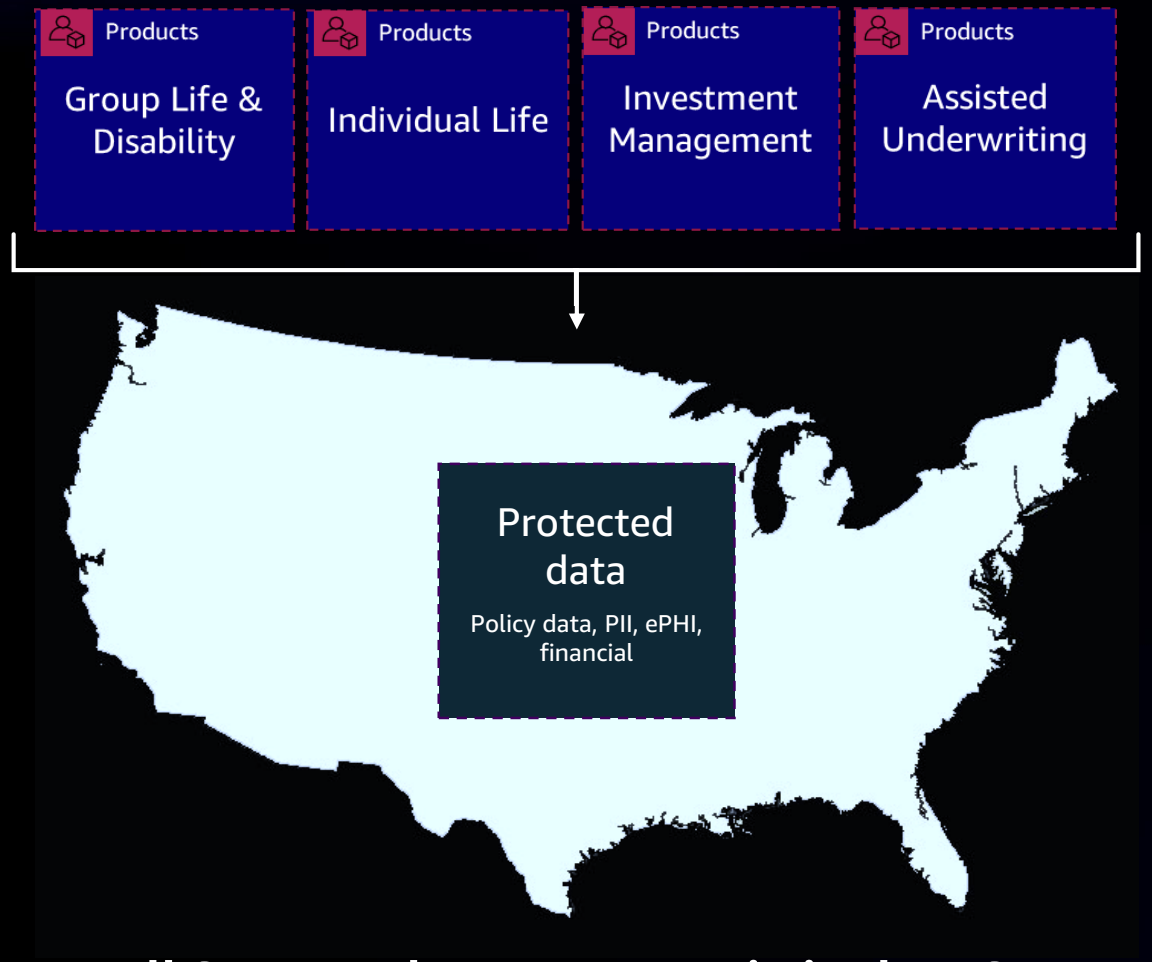
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Symetra cloud model



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

Symetra operates in a highly regulated industry



All Symetra data must remain in the US

Symetra data must remain in the United States

Internal and external audit and compliance requirements:

- HIPAA
- ICFR
- ISO 27001

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

Data guardrails: Regionality

How we do it today…

- **Actively monitor news feeds for new Region announcements**
- **With a new Region — manually update ALL accounts with the following actions:**
  - **Disable AWS STS from issuing security tokens to endpoints**
  - **Remove default VPC in new Region**
  - **Enable managed services e.g., Amazon Macie, Amazon GuardDuty, AWS Config, AWS Security Hub, AWS CloudTrail, etc.**

Why…?

- We don’t have native cloud preventative controls
- Service-linked roles can work outside of the “Region Blocking” SCPs — the SCP doesn’t provide full coverage
- Prevent our applications builders from deploying workloads and data outside of the allowed Regions

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

"In collaboration with AWS, we asked for an 'Easy Button' to address our data residency requirements. AWS delivered by providing new capabilities in AWS Control Tower that will save us hours of work and automates security improvements."

Chuck Chemis

Principal Cloud Architect, Symetra

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

Data residency enabled by AWS Control Tower

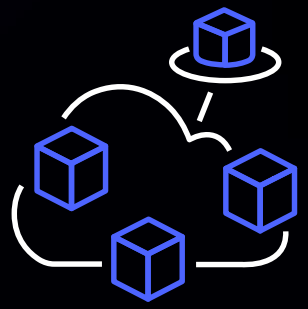
Jamie St. Onge, Senior Manager, AWS Control Tower

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

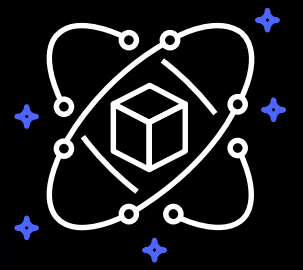
NEW: Data residency guardrails in AWS Control Tower



Keep your customer data compliant



Use purpose-built guardrails

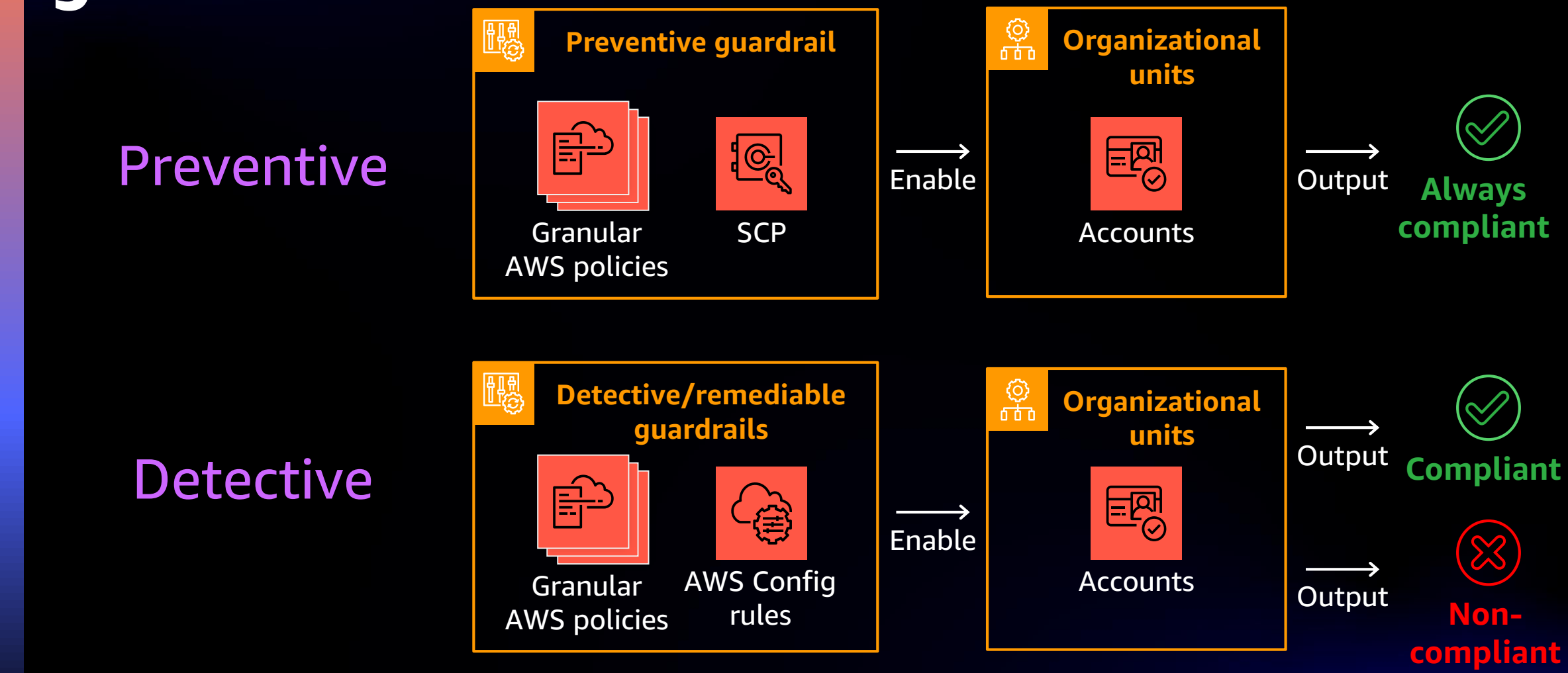


Set up in minutes

aws

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

Data residency enabling policy enforcement guardrails

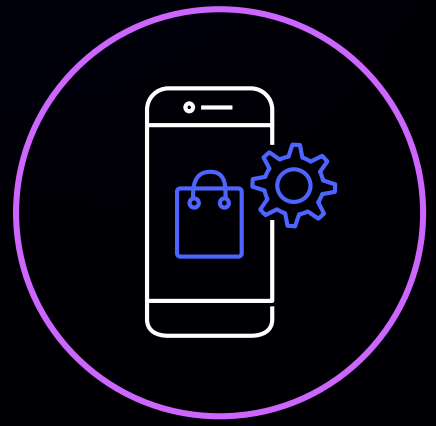


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use cases for data residency guardrails



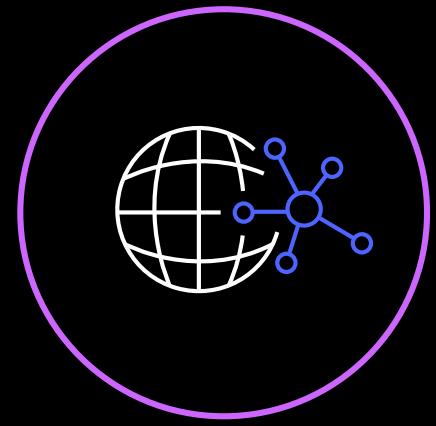
Prevent unwanted transfer of customer data



Restrict application teams from violating data residency requirements



Prevent sandbox content from reaching public internet



Prevent unwanted cross-Region networking

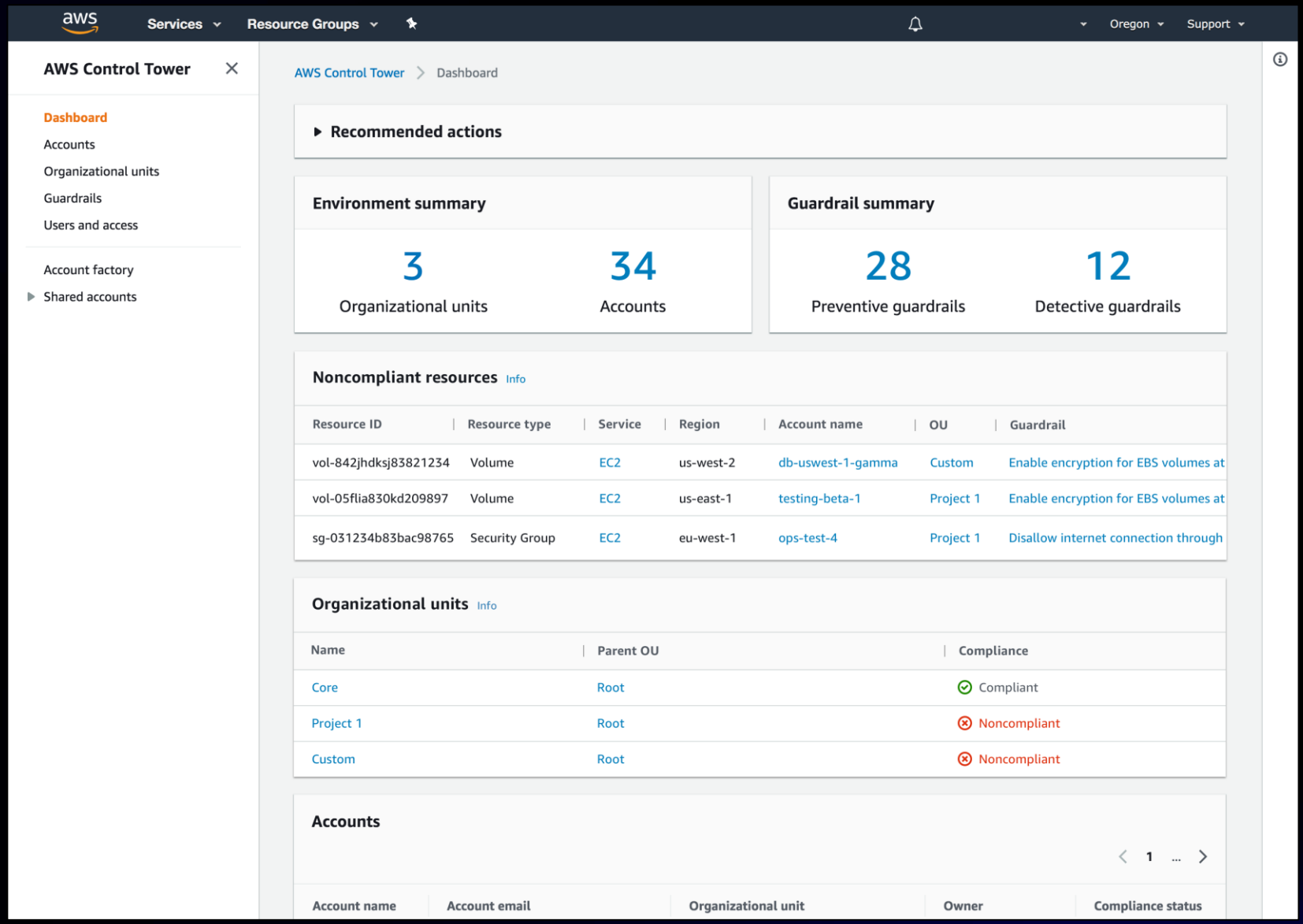
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data residency preventive and detective guardrails

Preventive	Detective
• 4 new preventive guardrails • Deny access to services and operations in selected AWS Regions • Disallow internet access for an Amazon VPC instance • Disallow Amazon Virtual Private Network (VPN) connections • Disallow cross-Region networking for Amazon EC2, Amazon CloudFront, and AWS Global Accelerator	• 13 new detective guardrails • Range from detecting whether replication instances for AWS Database Migration Service (AWS DMS) are public to whether any Amazon VPC subnets are assigned a public IP address

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

Dashboard for oversight



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

Launch customers and partners











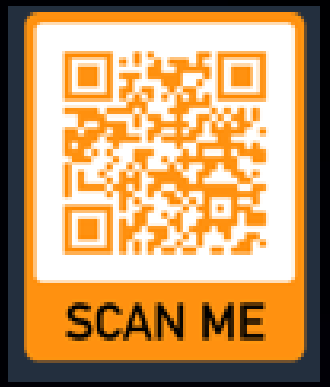




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Get started with AWS Control Tower today

AWS Control Tower



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

Thank you!

Kaushik Mohanty
kmohanty@amazon.com

Chuck Chemis
Chuck.Chemis@symetra.com

Jamie St. Onge
grecjami@amazon.com

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