



# Microsegmentation Powered By Zero Trust

**Peter Smith**

VP, Zscaler Workload Segmentation

# Agenda

Why microsegmentation?

Limitations of existing approaches

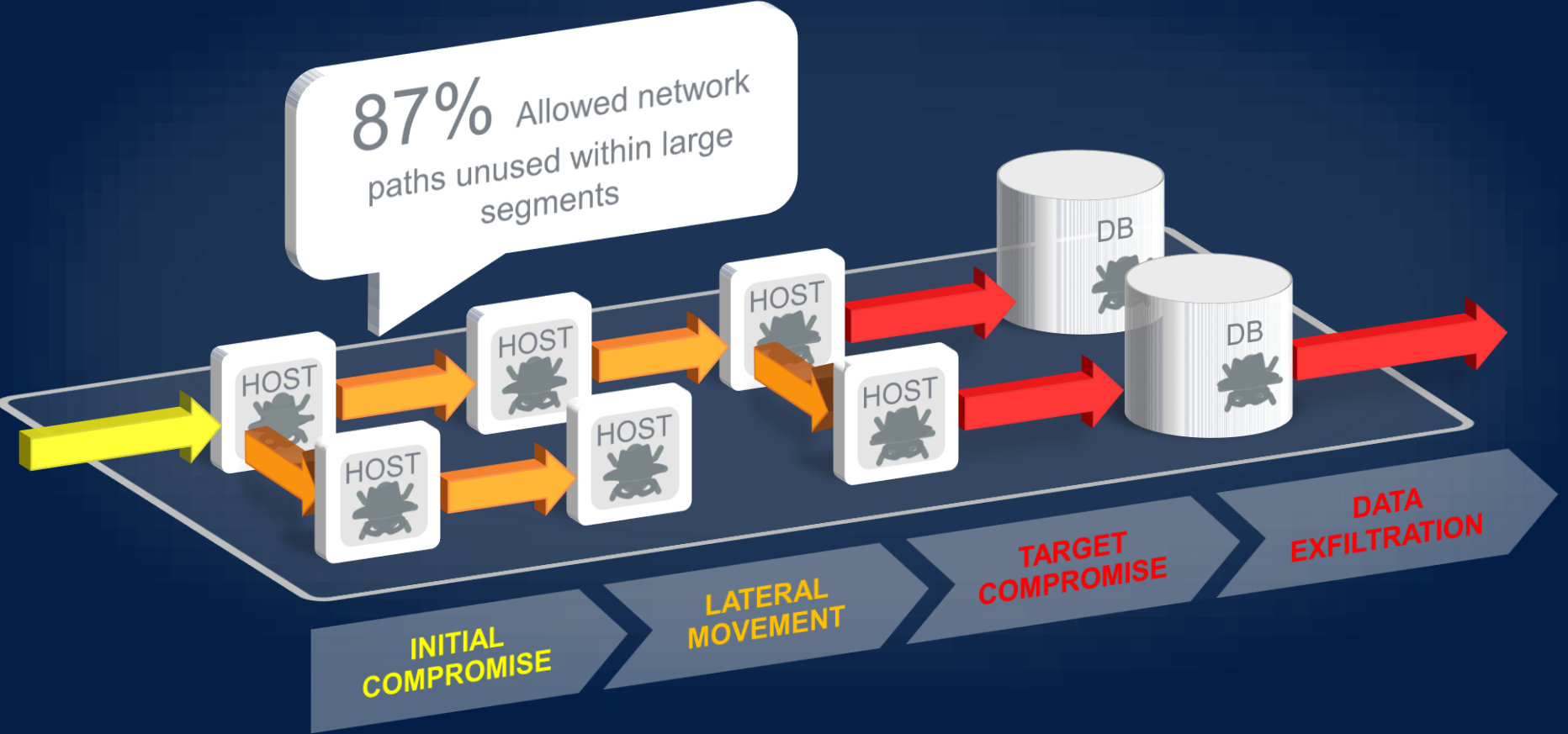
A new approach based on zero trust and automation

Demo

Q&A

# Flat Networks Allow Too Many Attack Paths

87% Allowed network paths unused within large segments



# Experts Recommend Improve Segmentation And Use Zero Trust

THREAT	IMPACT	EXPERTS RECOMMEND
<b>Nation State</b> (Gov. agency)	21.5M PII records	<b>“Zero trust model”</b> <small>US-HCOGR</small>
<b>APT</b> (Financial services)	146M PII records	<b>“Enhance network segmentation”</b>
<b>Ransomware</b> (Logistics co.)	\$300M, 29k systems	<b>“... least privilege”</b> <small>US CERT</small>
<b>Insider Threat</b> (Healthcare co.)	18K PHI records	<b>“Network segmentation”</b> <small>SecurityMetrics</small>

---

**Gartner:** “Identity-based segmentation” is a core protection strategy for cloud workloads.

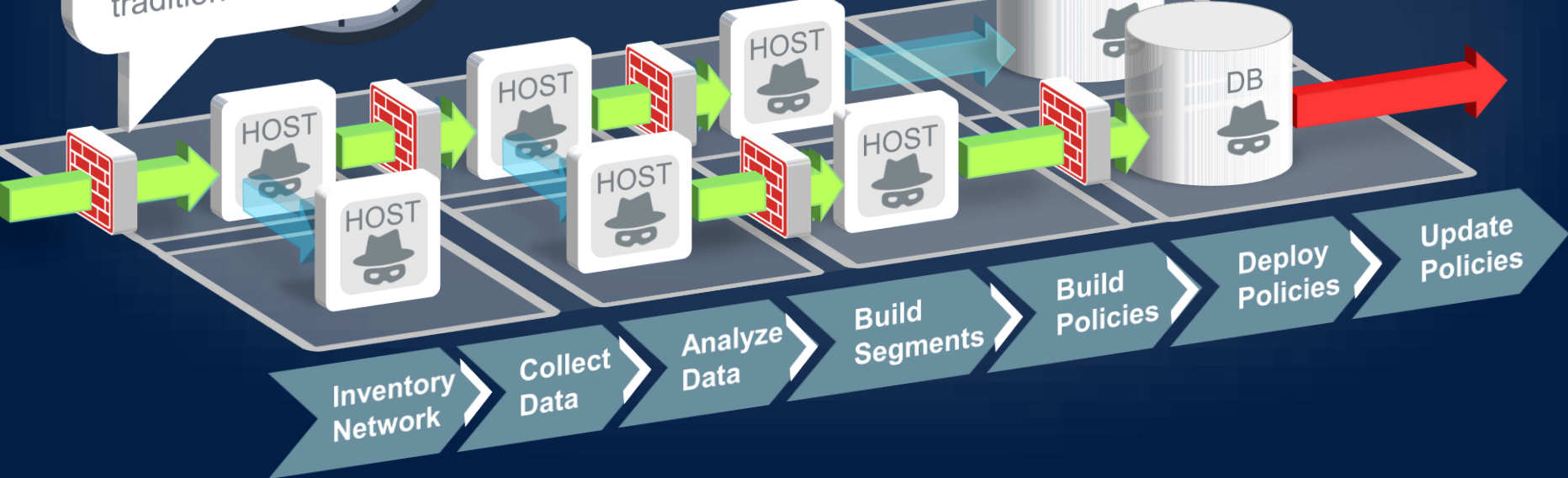
# Shrinking Segments Is Complex and Time Consuming



# Shrinking Segments Is Complex and Time Consuming

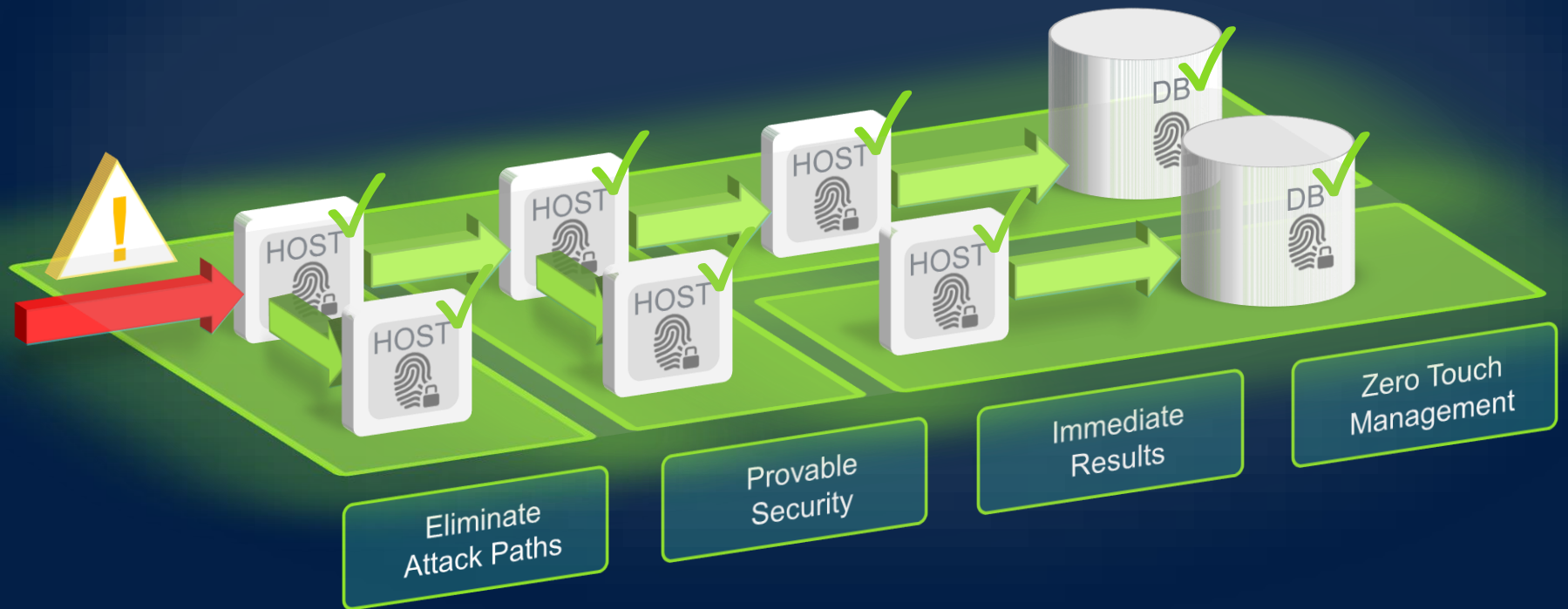
Despite your investment, threats continue to move laterally through traditional controls.

**MONTH**  
TOTAL PROJECT TIME



# Automating Segmentation Using Zero Trust

Impossibly simple microsegmentation with Zero Trust security



# Automating Segmentation Using Zero Trust

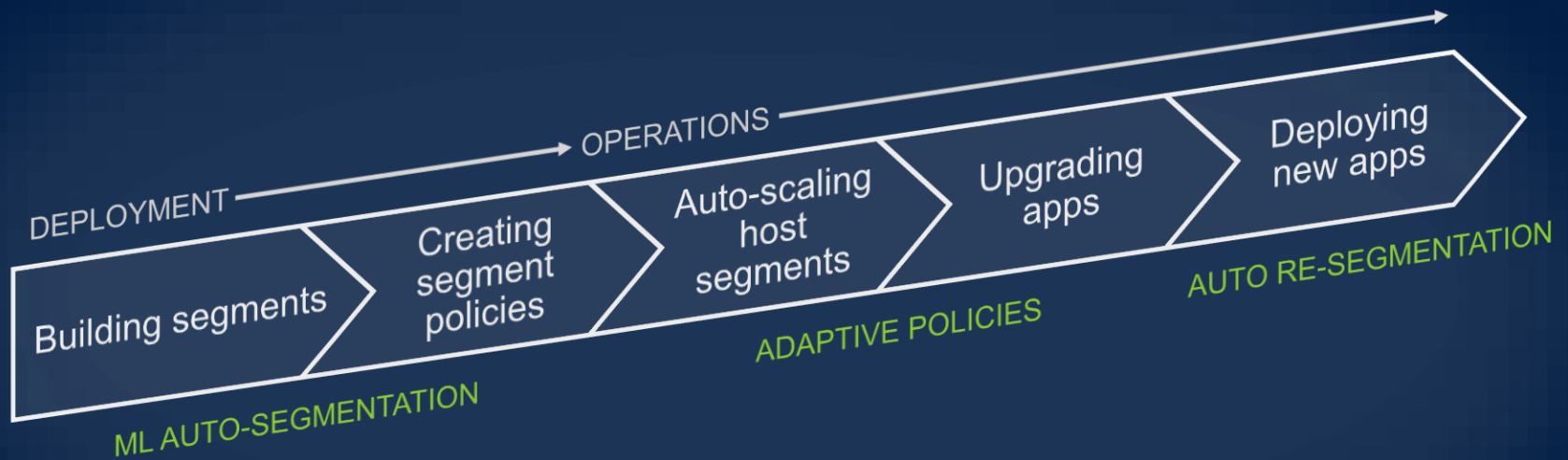
Impossibly simple microsegmentation with Zero Trust security





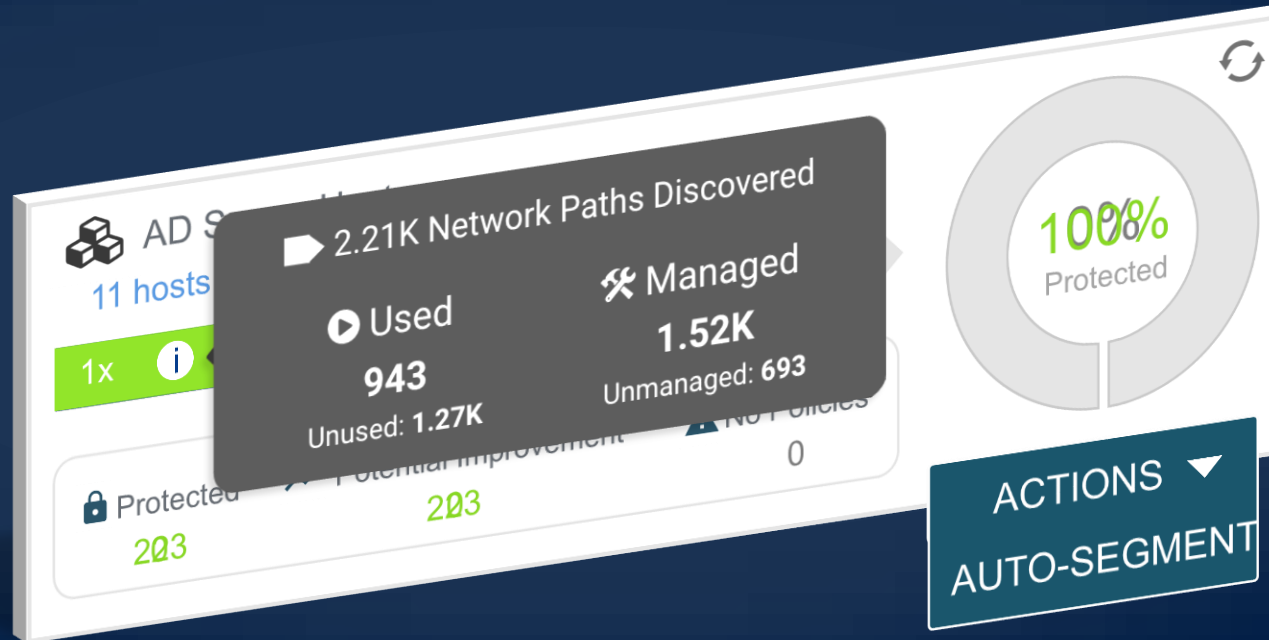
# Fully Automated Microsegmentation

All policy management tasks automated to radically simplify operations



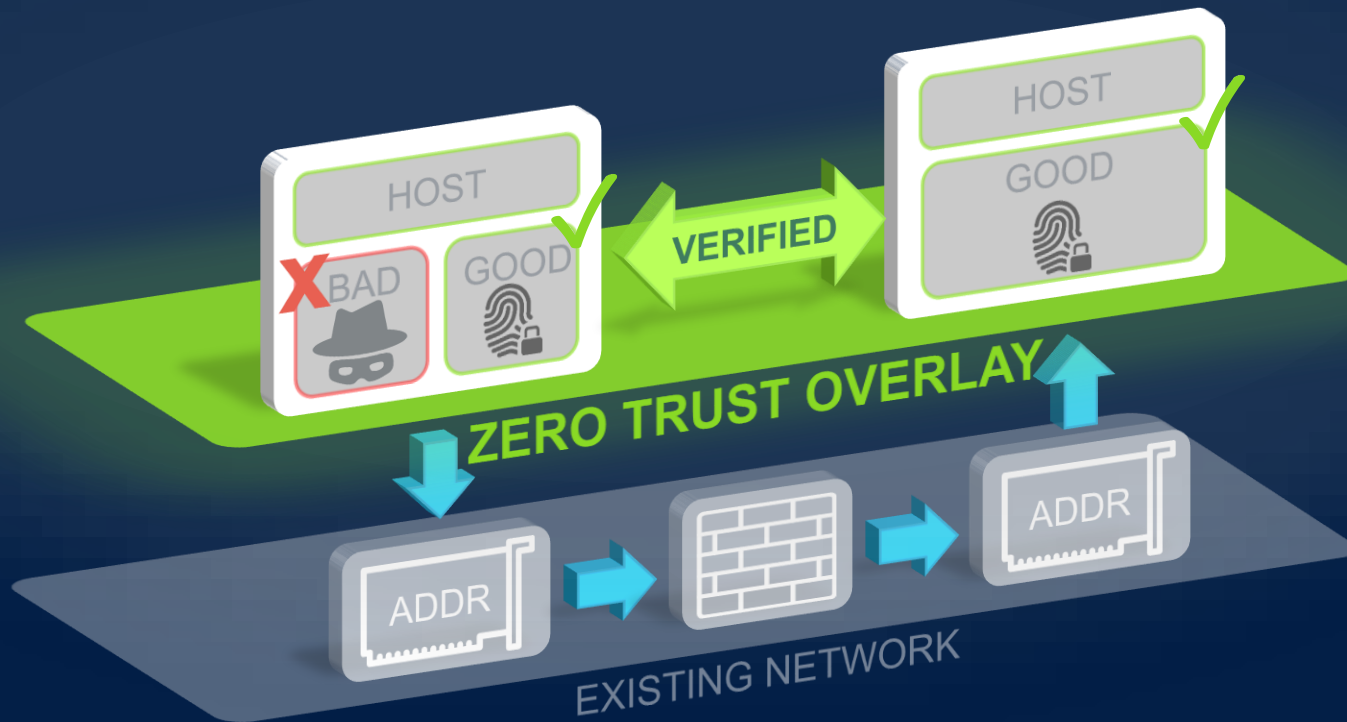
# 1-Click Simplicity → Provable Outcomes

Measurable return on your security investment



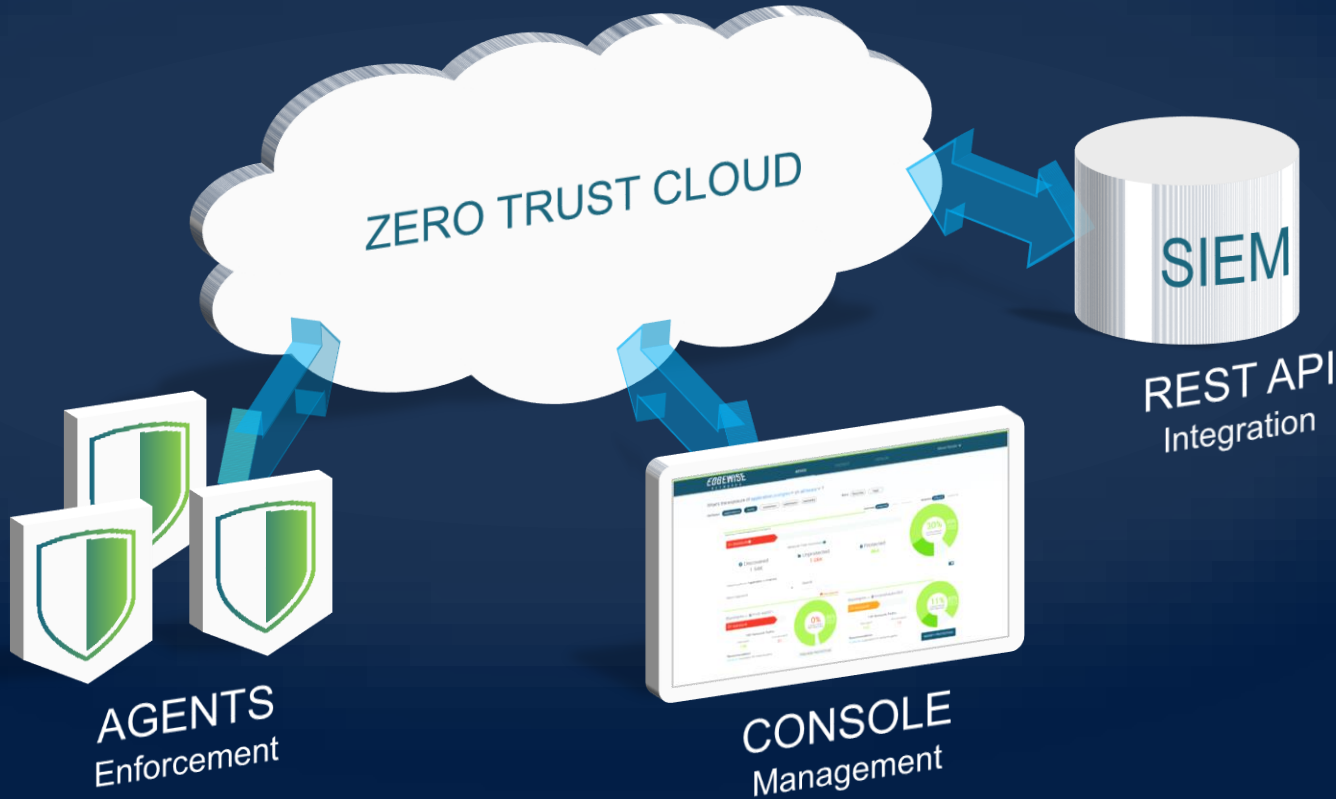
# Don't Change Your Network, Change Your Security

Overlay microsegmentation delivers identity-based protection with no change to your network



# Microsegmentation as a Service

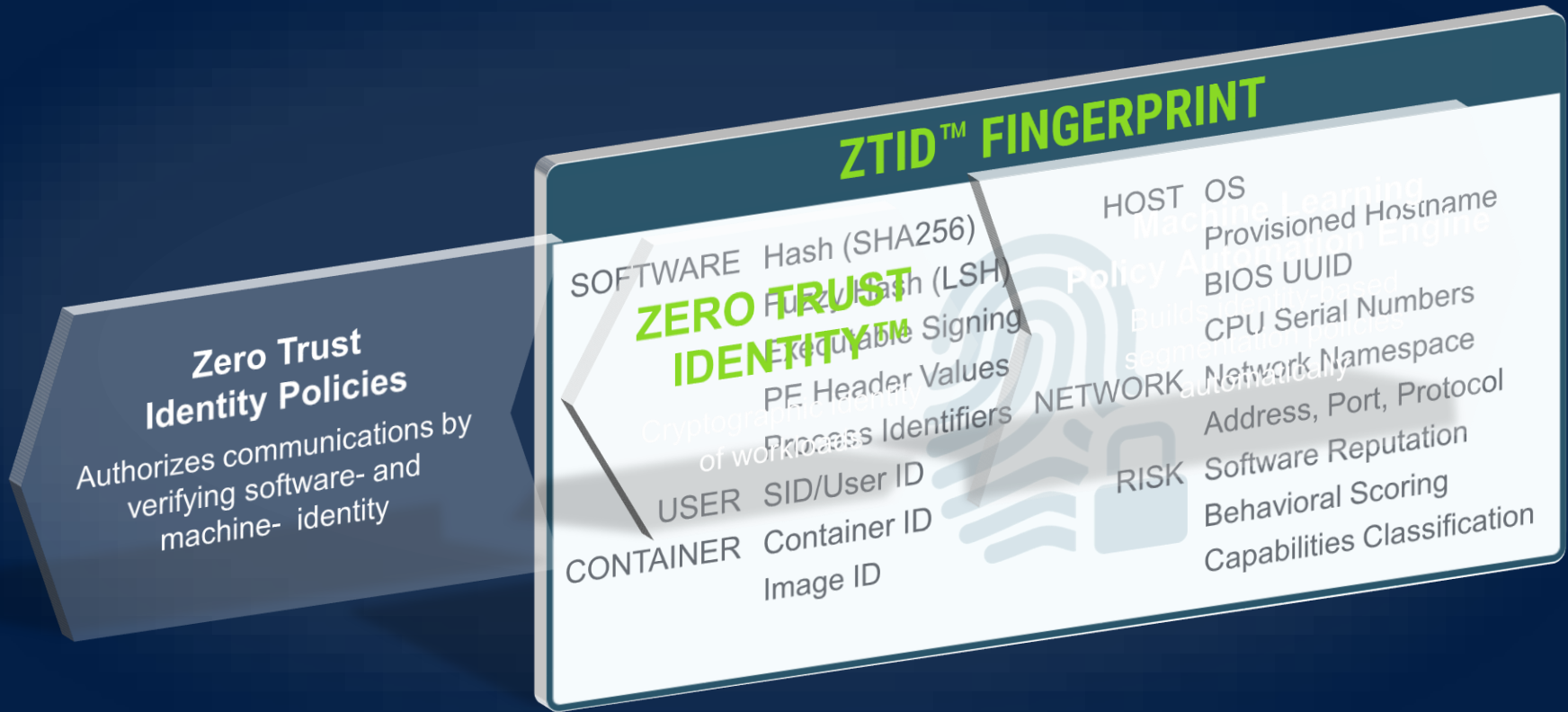
Simple Deployment. Secure Delivery. Scalable Protection. Cloud Delivered



# Zero Trust Identity

# Zero Trust Identity

Patented technology driving Zero Trust Auto-Segmentation



# Zero Trust Identity Verification

Delivering secure, trusted networks

 **RESILIENT IDENTITY**  
ZT Identities are resilient to software upgrades and CI/CD deployments

 user\_mgr.jar  winusrmgr01

**ZTID FINGERPRINT**

Software  
**SHA256:** BA7816BF8F01CFEA41440DE...  
**LSH:** 50FDE99373B04363727400AE98A...  
**PE Signer:** Demo Company, Co.  
**PE Product Name:** User Manager  
**PE Original Name:** user\_mgr.jar  
**Reputation:** Good  
**Capabilities:** Single Function

Host  
**Hostname:** winusrmgr01.prod.company.co  
**BIOS UUID:** 75D64596-53F8-426C-903BA...  
**CPU Serials Hash:** 18EE24150DCB1D967...



 sqlsrvr.exe  winusrdb01

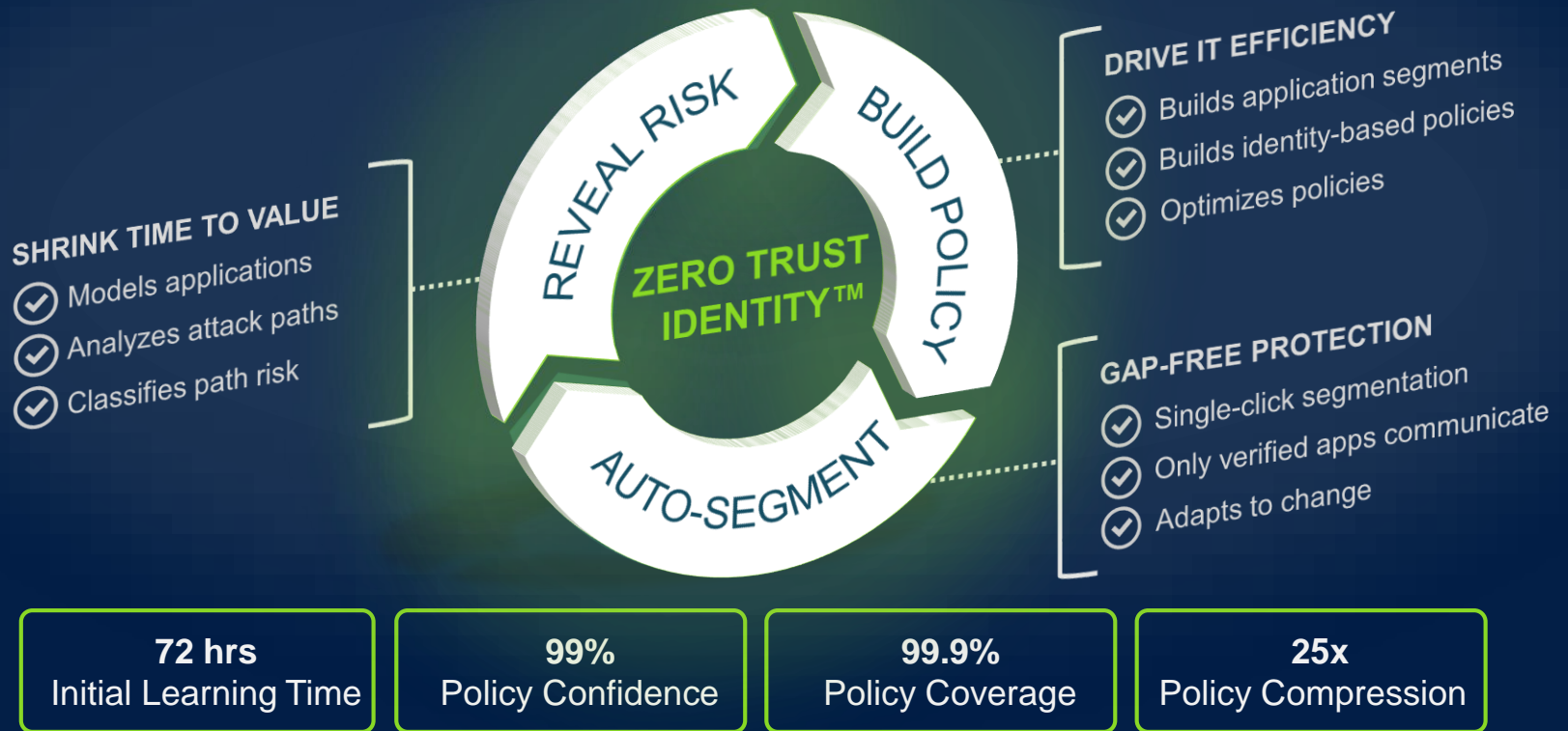
**ZTID FINGERPRINT**

Software  
**SHA256:** ED2456914E48C1E17B7BD922...  
**LSH:** BF6FF9792B2A5EAA331426E8523...  
**PE Signer:** Microsoft Corporation  
**PE Product Name:** MS SQL Server 2016  
**PE Original Name:** sqlsrvr.exe  
**Reputation:** Good  
**Capabilities:** Single Function

Host  
**Hostname:** winusrdb01.prod.company.co  
**BIOS UUID:** 062fef0f-4b04-4d17-a638-d...  
**CPU Serials Hash:** 32CFAD293016DFF08...

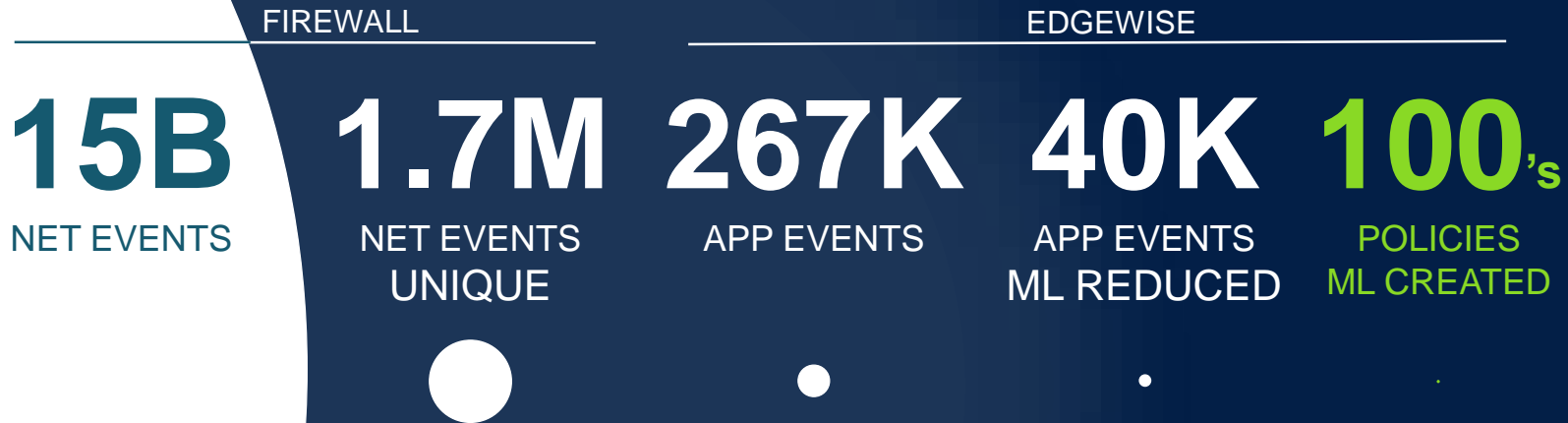
# Policy Automation Engine

Machine Learning generated policies for identity-based protection and 1-click simplicity





# The Machine Learning Advantage



## ML REDUCED APPLICATION EVENTS

Evaluating network vs. application identity attributes for automated rule generation.

- ✓ Compresses data by >6 orders of magnitude
- ✓ Reduces computational time
- ✓ Increases policy accuracy

# Demo



# Fully Automated Microsegmentation

All policy management tasks automated to radically simplify operations

1. BUILDING SEGMENTS
2. CREATING POLICIES FOR COMMUNICATION
3. ADDING/REMOVING HOSTS
4. UPGRADING APPLICATIONS
5. DEPLOYING NEW APPLICATIONS

# One Platform, Complete Zero Trust Protection

Protection made easy for workloads. No changes to applications or the network

## Deploy in minutes

Lightweight agents automatically installed

## Measure network exposure risk

Visualize app topology and attack paths, and quantify reduction in risk

## Simulate microsegmentation

Segments and policies automatically built by machine learning

## Enforce policies & manage updates

Zero trust protection that adapts to changes in the environment

Thank you. Q&A



# Managing Security on AWS

Milty Brizan

Solutions Architect, WWPS, State and Local Government, AWS

# Security is our top priority



Designed for  
security



Constantly  
monitored



Highly  
automated



Highly  
available



Highly  
accredited

# Benefits of AWS Security



Keep Your  
Data Safe



Meet  
Compliance  
Requirements



Save  
Money



Scale  
Quickly



# AWS Security Tools & Features



Identity & Access Control



Data Encryption



Infrastructure Security



Monitoring & Logging



Inventory & Configuration



AWS Partner Solutions

# Economies of Scale Apply to Security and Compliance



The stringent demands of a few...

**NASDAQ**



Set a higher standard for everyone



Tough scrutiny, robust capabilities, constant improvements, and a world-class AWS security team benefit the whole client community.

**Everyone's Systems and Applications**

**NASDAQ**

REQUIREMENTS



REQUIREMENTS



REQUIREMENTS

**Amazon Web Services Security Infrastructure**

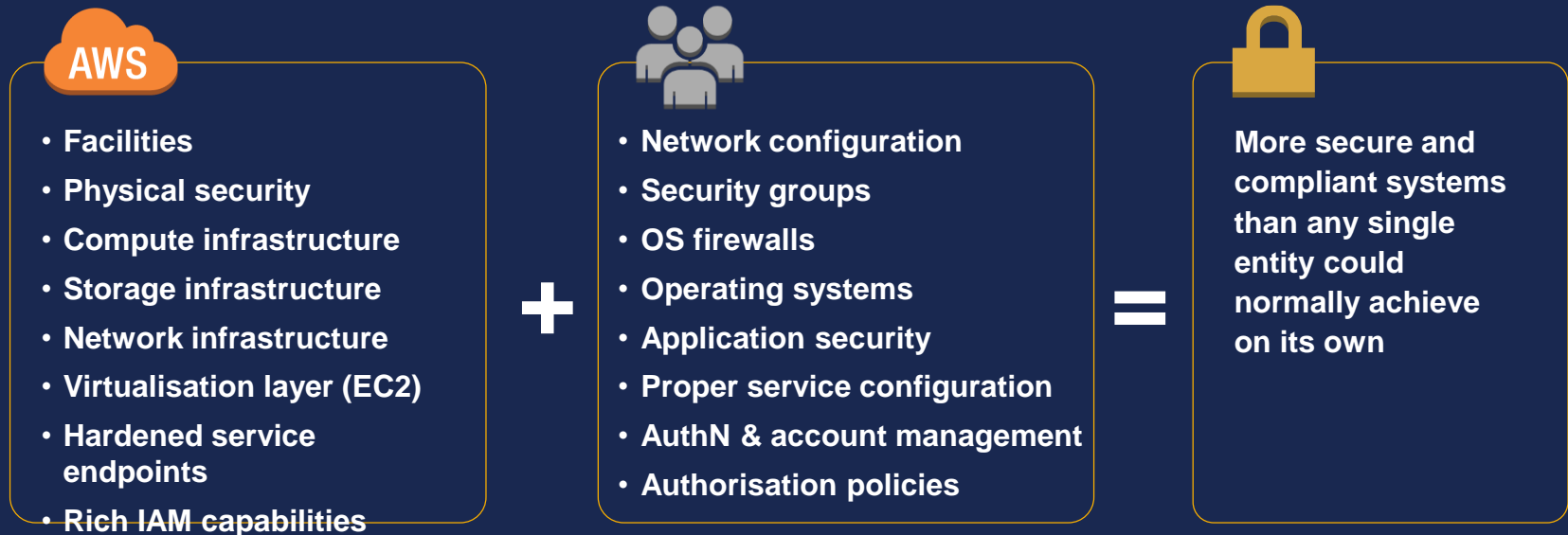
# What does this mean?

- 📦 You benefit from an environment built for the most security sensitive organisations
- 📦 AWS manages a multitude of security controls **so you don't have to**
- 📦 You get to define the right security controls for your workload sensitivity
- 📦 You always have full ownership and control of your data

# AWS Shared Responsibility Model

# With AWS, Security Is a Shared Responsibility

Customers concentrate on systems and apps while AWS manages infrastructure.



Security expertise is a scarce resource; AWS oversees the big picture, letting your security team focus on a subset of overall security needs.

# AWS Shared Responsibility Model

- Will one model work for all services?

Infrastructure  
Services



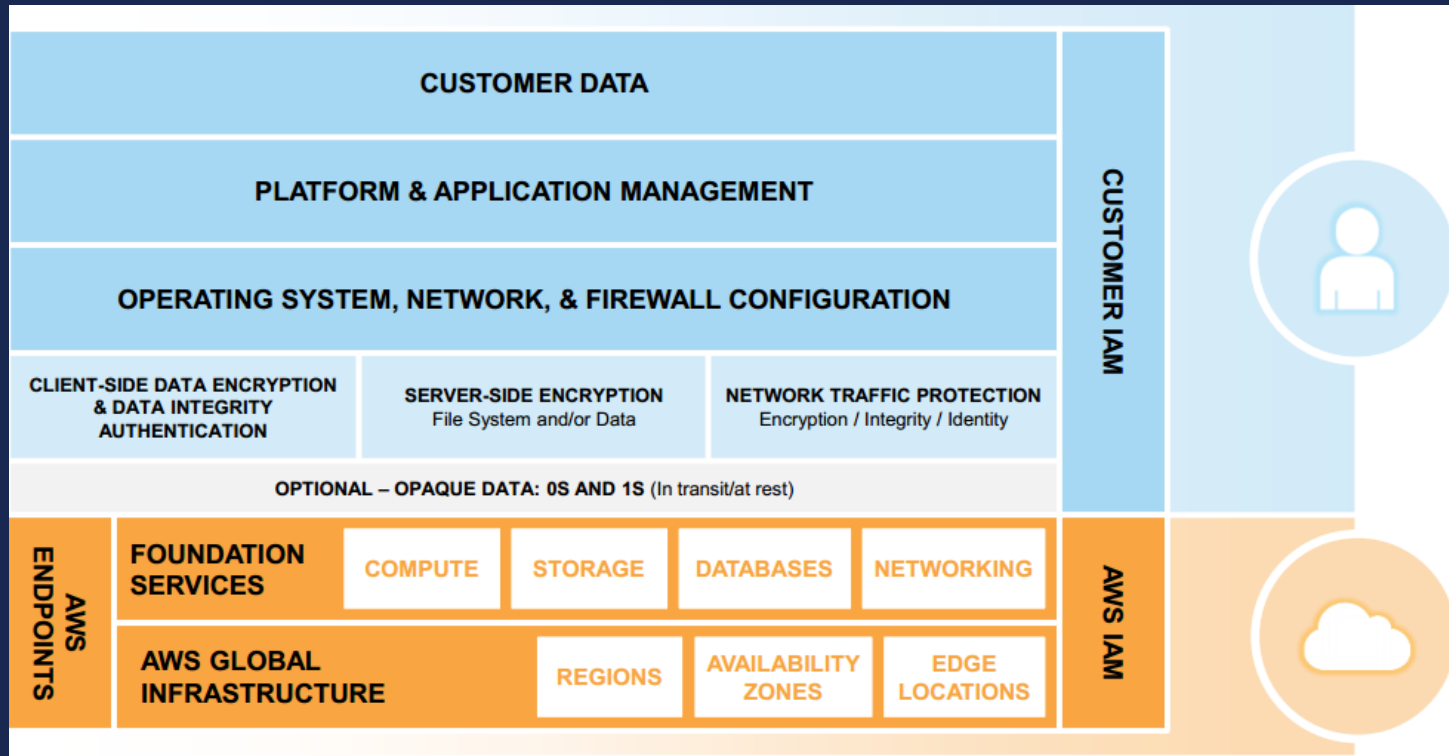
Container  
Services



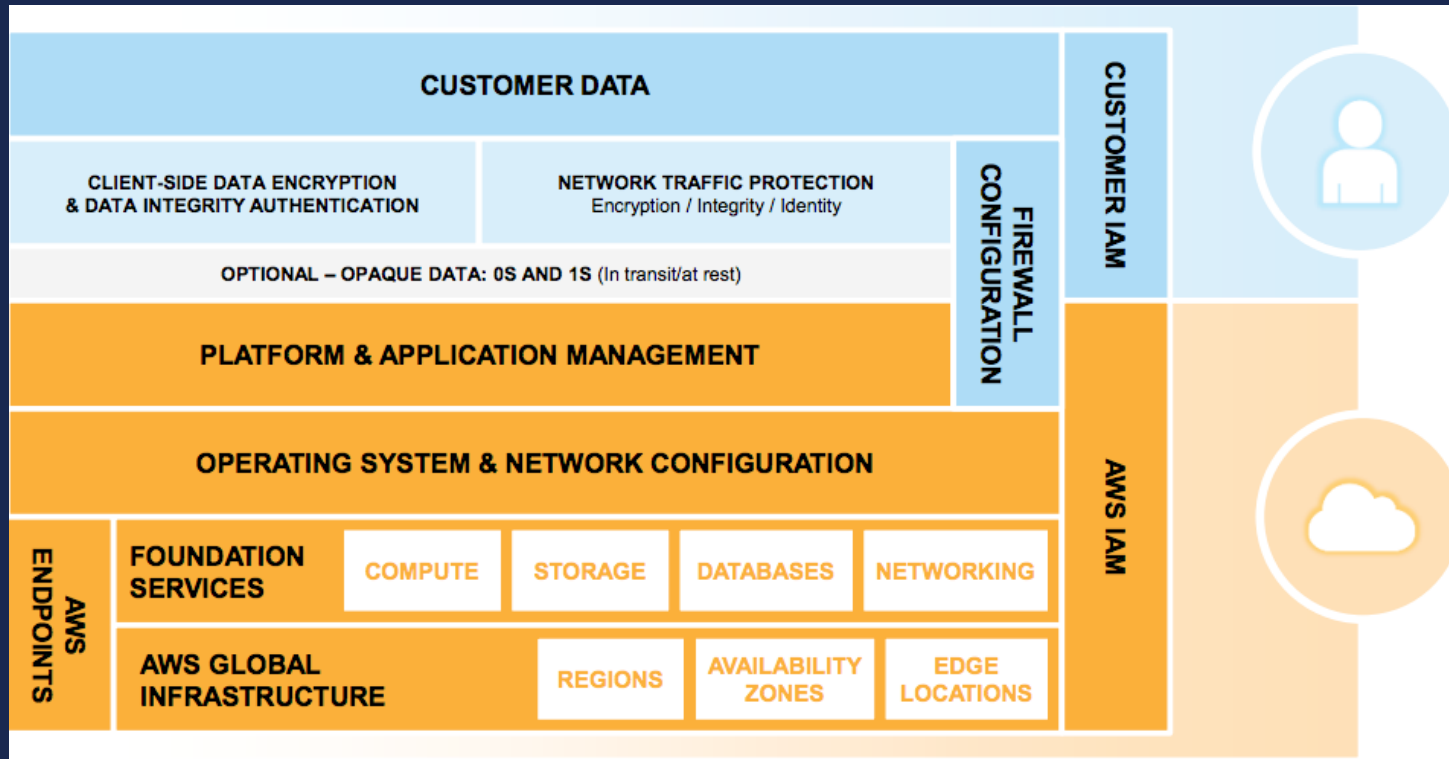
Abstract  
Services



# Shared Responsibility Model - Infrastructure

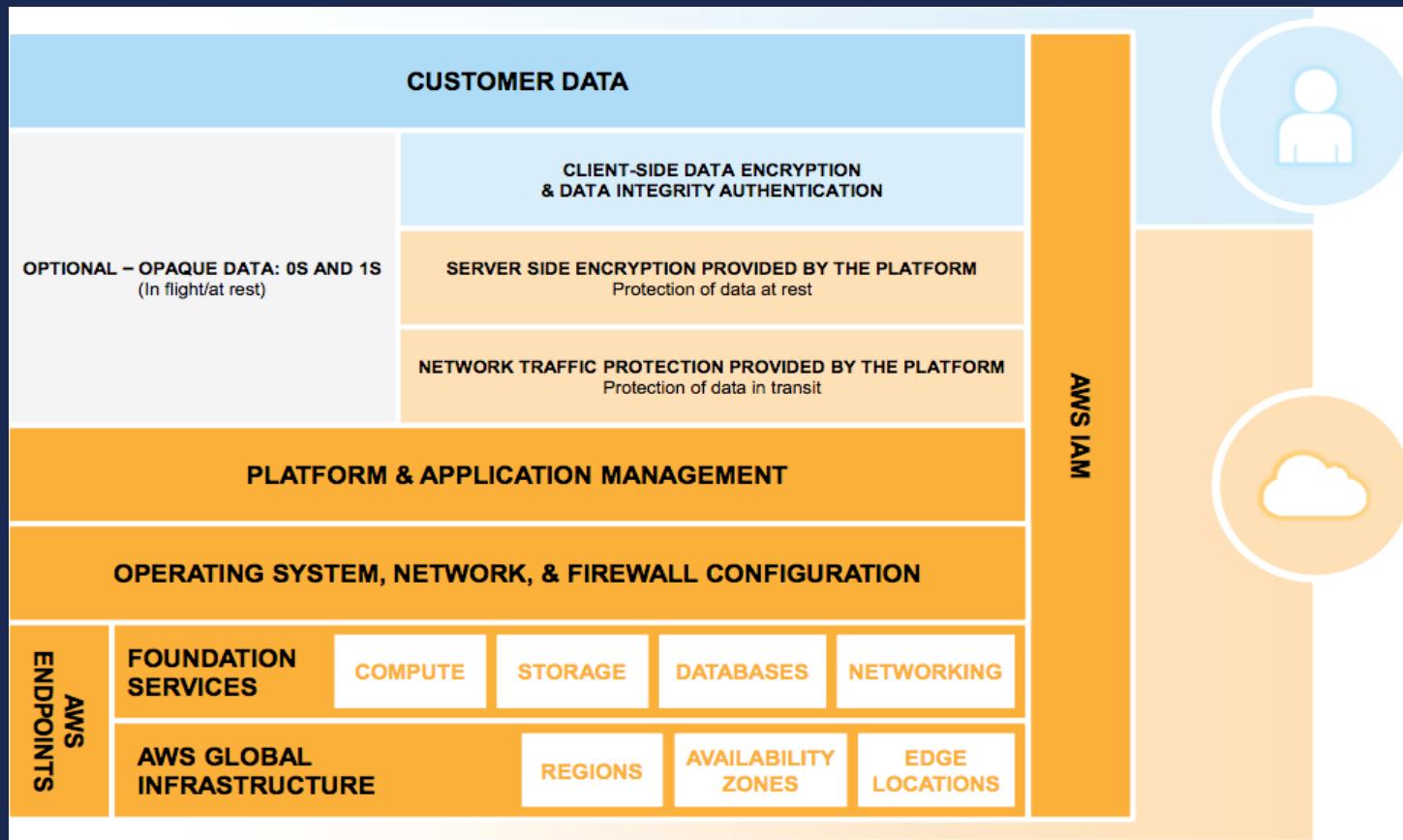


# Shared Responsibility – Container Services





# Shared Responsibility – Abstracted Services



Managed by  
AWS Customers

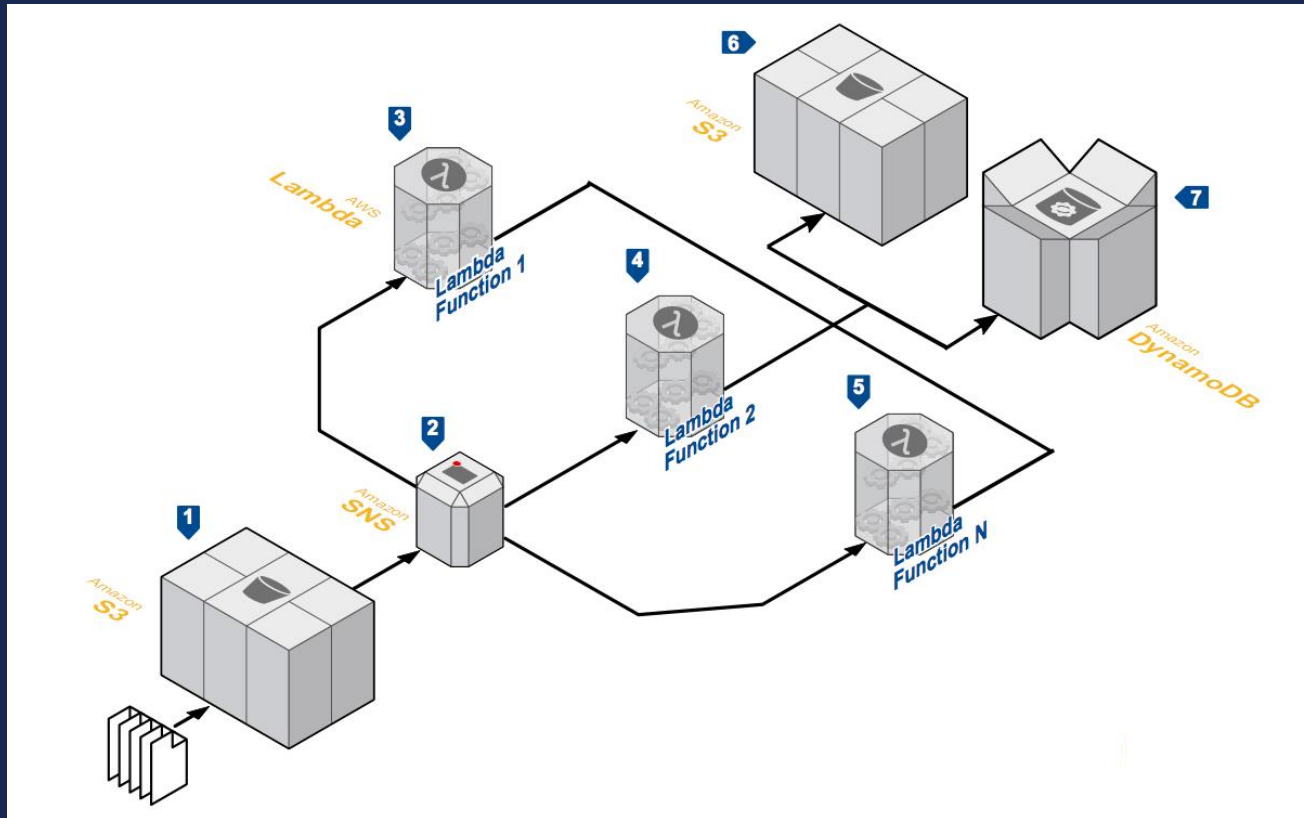
Managed by  
Amazon Web  
Services

# Benefiting from Abstracted Services: Serverless Architectures

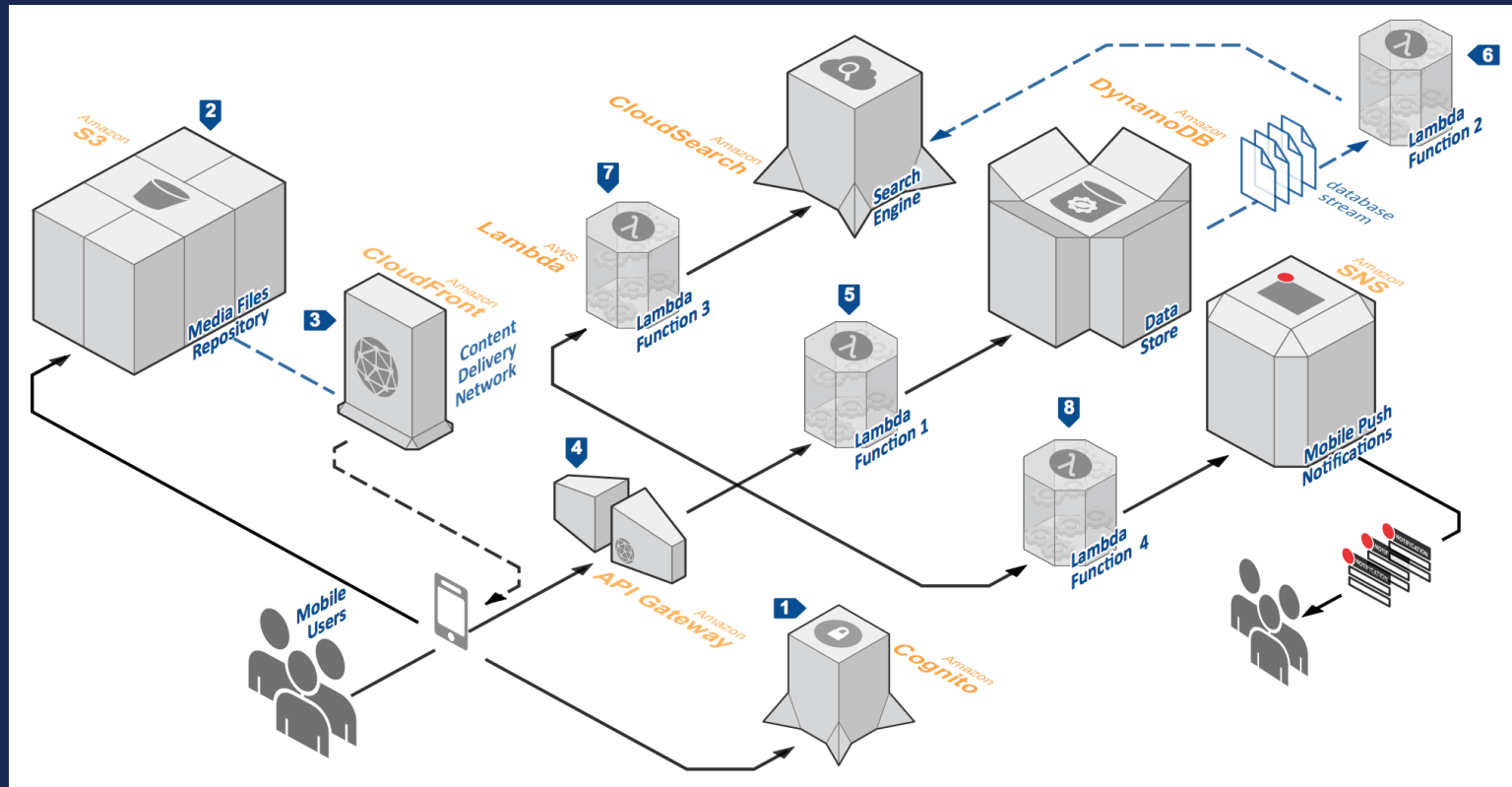
# Benefits of Serverless Architectures

- Developers can focus on their core product
  - No server management
  - Flexible scaling
  - Automated high availability
- Let AWS manage the security of the underlying services
  - We do the undifferentiated heavy lifting
- Reduced overhead lets developers reclaim time and energy that can be spent on developing great products

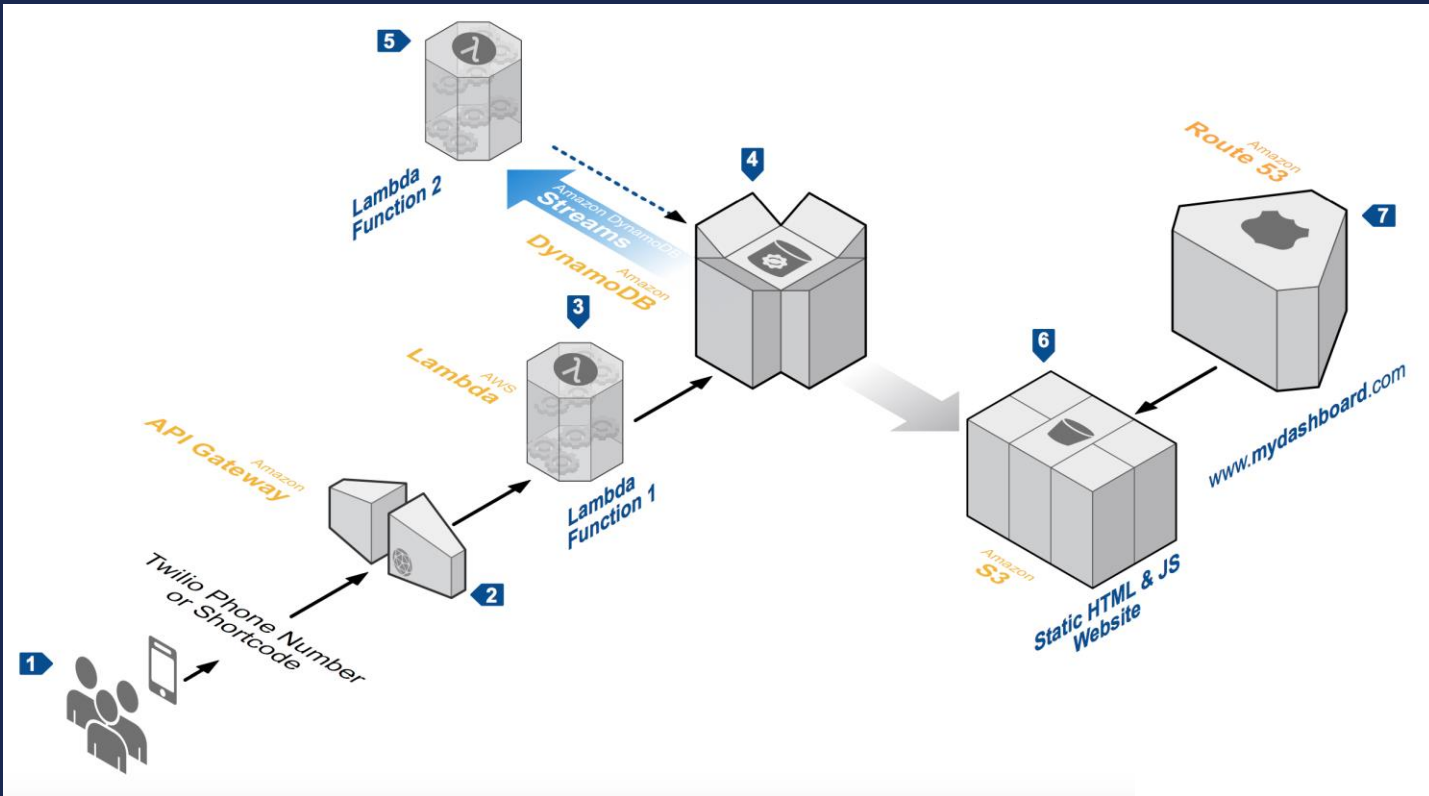
# Real-time File Processing



# Mobile Back-end



# AWS Lambda: Real-time voting application



# Applying the Shared Responsibility Model

- **Security of the cloud**
  - Security measures that **AWS** implements and operates
  - AWS security standards shown by **certifications & attestations**
- **Security in the cloud**
  - Security measures that the **customer** implements and operates
  - **Certifications** and **attestations** can be used by customers when undertaking risk assessments or using **frameworks**

# Security OF the Cloud

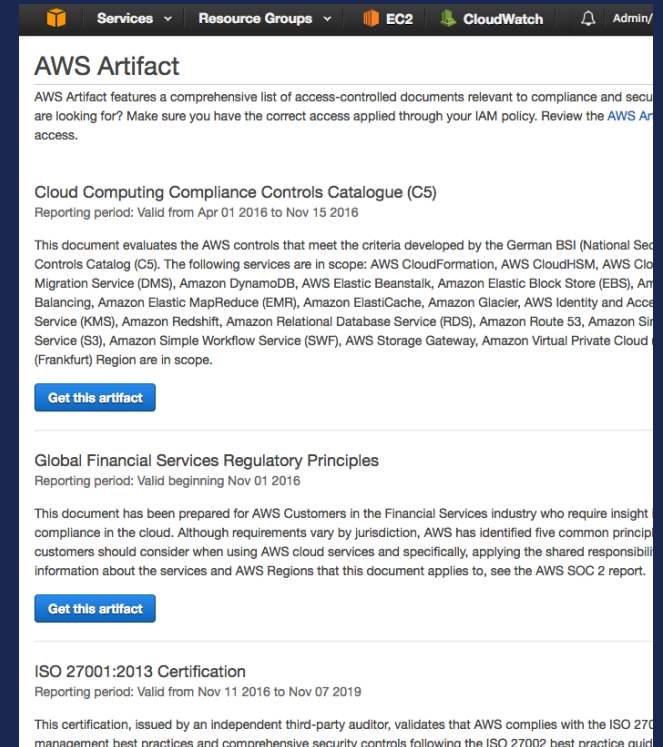


# AWS Compliance

- Compliance **certifications** and **attestations** are assessed by a third-party, independent auditor and result in a **certification**, **audit report**, or **attestation of compliance**.

# Accessing AWS Compliance Reports

- AWS Artifact:
  - On-demand access to AWS' compliance reports
  - Globally available
  - Easy identification
  - Quick assessments
  - Continuous monitoring
  - Enhanced transparency



The screenshot displays the AWS Artifact console interface. At the top, there is a navigation bar with icons for Services, Resource Groups, EC2, CloudWatch, and Admin. The main content area is titled "AWS Artifact" and contains three report entries, each with a "Get this artifact" button.

**AWS Artifact**  
AWS Artifact features a comprehensive list of access-controlled documents relevant to compliance and security. Make sure you have the correct access applied through your IAM policy. Review the AWS Artifact access.

**Cloud Computing Compliance Controls Catalogue (C5)**  
Reporting period: Valid from Apr 01 2016 to Nov 15 2016

This document evaluates the AWS controls that meet the criteria developed by the German BSI (National Security Controls Catalog (C5). The following services are in scope: AWS CloudFormation, AWS CloudHSM, AWS Cloud Migration Service (DMS), Amazon DynamoDB, AWS Elastic Beanstalk, Amazon Elastic Block Store (EBS), Amazon ElastiCache, Amazon Elastic MapReduce (EMR), Amazon ElastiCache, Amazon Glacier, AWS Identity and Access Management (IAM), Amazon Key Management Service (KMS), Amazon Redshift, Amazon Relational Database Service (RDS), Amazon Route 53, Amazon Simple Storage Service (S3), Amazon Simple Workflow Service (SWF), AWS Storage Gateway, Amazon Virtual Private Cloud (VPC) (Frankfurt) Region are in scope.

**Global Financial Services Regulatory Principles**  
Reporting period: Valid beginning Nov 01 2016

This document has been prepared for AWS Customers in the Financial Services industry who require insight into compliance in the cloud. Although requirements vary by jurisdiction, AWS has identified five common principles that all financial services customers should consider when using AWS cloud services and specifically, applying the shared responsibility model. For more information about the services and AWS Regions that this document applies to, see the AWS SOC 2 report.

**ISO 27001:2013 Certification**  
Reporting period: Valid from Nov 11 2016 to Nov 07 2019

This certification, issued by an independent third-party auditor, validates that AWS complies with the ISO 27001:2013 information management best practices and comprehensive security controls following the ISO 27002 best practice guide.

# Assurance Programmes - Global



**CSA**  
Cloud Security  
Alliance Controls



**ISO 9001**  
Global Quality  
Standard



**ISO 27001**  
Security Mgmt  
Controls



**ISO 27017**  
Cloud Specific  
Controls



**ISO 27018**  
Personal Data  
Protection



**PCS DSS Level  
1**  
Payment Card  
Standards



**SOC 1**  
Audit Controls  
Report



**SOC 2**  
Security, Availability &  
Confidentiality Report



**SOC 3**  
General Controls  
Report

# Assurance Programmes - Europe



**C5 (Germany)**  
Operational  
Security  
Attestation



**Cyber  
Essentials Plus  
(UK)**  
Cyber Threat  
Protection



**ENS High  
(Spain)**  
Spanish Govt  
Standards



**G-Cloud (UK)**  
UK Govt  
Standards



**IT-Grundschutz  
(Germany)**  
Baseline  
Protection  
Methodology

*And many more...*

<https://aws.amazon.com/compliance/>

Certifications / Attestations	Laws, Regulations, and Privacy	Alignments and Frameworks
C5 [Germany]	CISPE	CIS
Cyber Essentials Plus [UK]	DNB [Netherlands]	CJIS
DoD SRG	EU Model Clauses	CSA
FedRAMP	FERPA	ENS [Spain]
FIPS	GLBA	EU-US Privacy Shield
IRAP [Australia]	HIPAA	FISC [Japan]
ISO 9001	HITECH	FISMA
ISO 27001	IRS 1075	G-Cloud [UK]
ISO 27017	ITAR	GxP (FDA CFR 21 Part 11)
ISO 27018	My Number Act [Japan]	ICREA
MLPS Level 3 [China]	U.K. DPA - 1988	IT Grundschutz [Germany]
MTCS [Singapore]	VPAT / Section 508	MITA 3.0
PCI DSS Level 1	EU Data Protection Directive [EU]	MPAA
SEC Rule 17-a-4(f)	Privacy Act [Australia & New Zealand]	NIST
SOC 1	PDPA - 2010 [Malaysia]	PHR
SOC 2	PDPA - 2012 [Singapore]	Uptime Institute Tiers
SOC 3	PIPEDA [Canada]	UK Cloud Security Principles
	Spanish DPA Authorization	

# Inherit controls from AWS



Control #	Control Name	Control #	Control Name	Control #	Control Name
A.11.1.1	Physical security perimeter	A.11.2.1	Equipment siting and protection	A.11.2.7	Secure disposal or reuse of equipment
A.11.1.2	Physical entry controls	A.11.2.2	Supporting utilities	A.11.2.8	Unattended user equipment
A.11.1.3	Securing offices, rooms and facilities	A.11.2.3	Cabling security	A.11.2.9	Clear desk and clear screen policy
A.11.1.4	Protecting against external and environmental threats	A.11.2.4	Equipment maintenance	A.17.2.1	Availability of information processing facilities
A.11.1.5	Working in secure areas	A.11.2.5	Removal of assets	A.13.1.2	Communications security
A.11.1.6	Delivery and loading areas	A.11.2.6	Security of equipment and assets off-premises		

# Security IN the Cloud

# Access a deep set of cloud security tools

## Networking & Security



Amazon GuardDuty



Amazon VPC



AWS Direct Connect



VPN connection



Security Groups



Flow logs



AWS Shield



AWS WAF



Route table



AWS Firewall Manager

## Compliance & Governance



AWS Service Catalog



AWS Trusted Advisor



AWS CloudFormation



AWS CloudTrail



AWS Systems Manager



Amazon CloudWatch



AWS Config



AWS Artifact



Amazon Inspector



AWS OpsWorks

## Identity



Amazon Cognito



IAM



AWS Directory Service



AWS Organizations



Active Directory integration

AWS Single Sign-on



Temporary Security credential



SAML Federation



## Encryption



AWS KMS



AWS Secrets Manager



AWS CloudHSM



Client-side encryption



AWS Certificate Manager



# Asset Inventory / Management

## Knowing, at every point in time, what's running, where, and why

- **Everything is an API call**
  - Authenticated, signed, logged, whether it's the GUI, CLI, or SDK
  - All resources are listed in the console and, for CLI users, one API call away
- **AWS Service Catalog**
  - Asset inventory, ownership, responsibility, and access management
- **AWS Systems Manager**
  - Asset inventory, management and automation (including on premises assets)
  - Manage VMs without logging in (RunCommand): immutable infrastructure
  - Patch Management, and configuration checks

# Network Segmentation

- **Virtual Private Cloud (VPC)**
  - **Multi-dimensional defense-in-depth**
    - Private and Public subnets
    - Security Group and NACLs
    - VPC Flow Logs for network monitoring and analysis
- **Range of connectivity options**
  - Internet access
  - IPsec VPN (over Internet)
  - Private Network Connectivity (Direct Connect)
- **Infrastructure as code**



# Configuration and Change Management

- **AWS Config and Aws Config Rules**  
**Controlled, monitored, and managed change – in an Agile context**
  - Configuration history and Security rules enforcement
  - Extensive set of built-in rules and you can create your own (security as code)
- **CloudFormation**
  - Configuration management, with a unique source of truth
- **AWS Inspector and AWS Trusted Advisor**
  - Best practices and vulnerability management
- **AWS CloudWatch Events**
  - Respond quickly to notifications from AWS resources delivered in near-real-time



# Security by Design

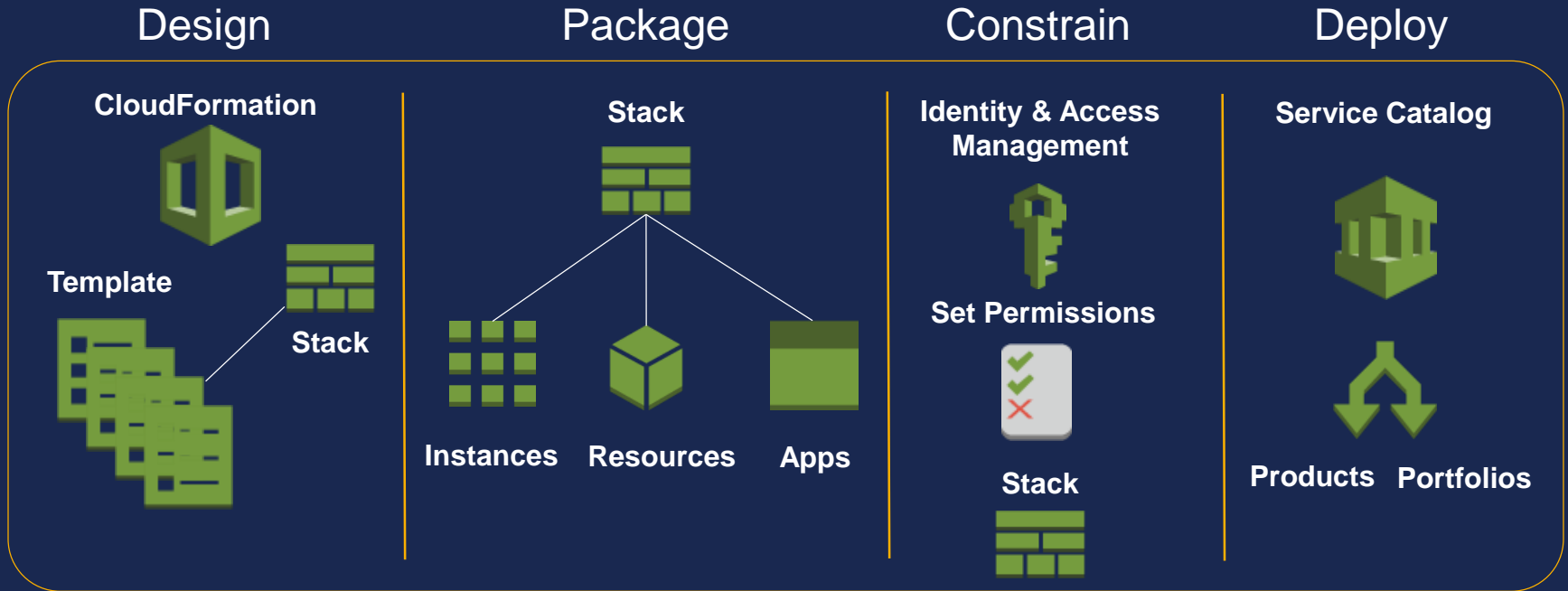
Security by Design (SbD) is a security assurance approach that formalises AWS account design, automates security controls, and streamlines auditing.

Instead of relying on auditing security retroactively, SbD provides security control built in throughout the AWS IT management process.

<https://aws.amazon.com/compliance/security-by-design/>



# Automate Security Operations



**Security by Design** allows you to automate deployments, provisioning, and configurations of AWS environments

# Advantages to the API

- **Authoritative** – the interface to, and between, AWS services
- **Auditable** – always know what, and who, is doing what
- **Secure** – verified integrity, and no covert channels
- **Fast** – can be read and manipulated in sub-second time
- **Precise** – defines the state of all infrastructure and services
- **Evolving** – continuously improving
- **Uniform** – provides consistency across disparate components
- **Automatable** – enables some really cool capabilities

# Automated Remediation: Amazon CloudWatch Events

# Automated Remediation: Example

- Customer wants to make sure that there is no Internet access available within a secure VPC
  - IAM policies should provide the first defense
  - The customer would like to be notified in the event that an Internet Gateway does get attached
- Automated remediation: automatically remove the Internet Gateway attachment at the same time as sending the notification
- How could we do this?



# Amazon CloudWatch Events

- Delivers a **near real-time** stream of **system events** that **describe changes** in Amazon Web Services (AWS) resources
  - Use simple rules to match events and route them to target function(s)
  - Schedule automated actions that self-trigger at certain times using cron or rate expressions
- Common **use cases** for CloudWatch Events
  - Responding to operational changes
  - Sending notifications
  - Automating corrective actions

# Key concepts

- Event: **indicates a change** in your AWS environment
  - Generated from other AWS services
  - Generated on a schedule
  - Generated from custom application-level events
- Target: **processes events**
  - Example targets include AWS Lambda, Kinesis Streams, Step Functions
- Rule: **matches incoming events** and **routes them** to targets for processing
  - Single rule can match to multiple targets
  - Rules are processed in parallel

# Amazon CloudWatch event bus

- Allows **the sending of CloudWatch Events to other AWS account(s)**
  - Allows for centralised CloudWatch Events within/between organisations
- Receiving accounts can **receive events from**
  - Whitelisted AWS accounts, or
  - Any AWS account
- Some additional **points to consider**
  - Chained events aren't supported (e.g. Acct A → Acct B → Acct C)
  - The sending account is charged for the event; the receiving account is not
  - Rules can be scoped to specific AWS account(s)

# Implementation

- Create an **Amazon CloudWatch event rule**:
  - Trigger the event when an `ec2:AttachInternetGateway` API call is made
  - Target an SNS topic to notify the security team when this happens
- **Test** the CloudWatch Events rule
  - Navigate to the VPC console, Internet Gateways section
  - Attach the unattached IGW to the Data VPC
  - You should receive an email notification within 5 minutes
- Automated remediation: hook up a **custom Lambda function** as a second trigger to CloudWatch Events, to detach the IGW automatically

# CloudWatch Events Rule

**Step 1: Create rule**

Create rules to invoke Targets based on Events happening in your AWS environment.

### Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

Event Pattern ⓘ  Schedule ⓘ

**Build event pattern to match events by service**

Service Name: EC2

Event Type: AWS API Call via CloudTrail

For AWS API call events, CloudWatch Events supports the same read/write APIs as CloudTrail does. Read-only APIs, such as those that begin with **List**, **Get**, or **Describe** are not supported by CloudWatch Events. [See more details](#) about which services are supported by CloudTrail.

Any operation  Specific operation(s)

AttachInternetGateway

**Event Pattern Preview** [Copy to clipboard](#) [Edit](#)

```
"aws.ec2"
],
"detail-type": [
  "AWS API Call via CloudTrail"
],
"detail": {
  "eventSource": [
    "ec2.amazonaws.com"
  ],
  "eventName": [
    "AttachInternetGateway"
  ]
}
```

### Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

**SNS topic**

Topic\*: alerts

Configure input

**Lambda function**

Function\*: testFunction

Configure version/alias

Configure input

**Add target\***

# Where to start?

# So many services... where do I start?

- AWS provides:
  - Continuous innovation of products and services
  - AWS Quick Starts
  - AWS Answers
  - AWS blogs
  - Comprehensive documentation
  - Extensive partner network

# Continuous Innovation



# AWS Certificate Manager – Private CA

## Create CA

- Step 1: Select CA type**
- Step 2: Configure CA subject name
- Step 3: Configure CA key algorithm
- Step 4: Configure revocation
- Step 5: Review

## Certificate authority (CA) type

ACM helps you create a private subordinate CA.

**Subordinate CA** Create a subordinate CA. Choose this option if you want to make a CA

## Certificates

[Request a certificate](#) [Import a certificate](#) [Actions](#)

**Success**  
Your certificate was requested successfully.

	Name	Domain name	Additional names	Status	Type
<input checked="" type="checkbox"/>		secure.internal	*.secure.internal	Issued	Private

- Delete
- Export (private certificates only)
- Resend validation email
- Reimport certificate

# AWS Firewall Manager

## AWS Firewall Manager

AWS Firewall Manager simplifies your AWS WAF administration and maintenance tasks across multiple accounts and resources. With AWS Firewall Manager, you create a policy and set up your firewall rules just once. The service automatically applies your rules across your accounts and resources, even as you add new resources. [Learn more](#)

### Prerequisites for using AWS Firewall Manager

- ✓ Your AWS account must be part of full feature set enabled. [Learn more](#)
- ✓ This AWS account must be enabled

[Create policy](#)

### Define policy scope

Specify condition to identify which resources to protect

**Region**

US East (N. Virginia)

**Select resource types that will be protected\***

- CloudFront distribution
- ELB Application Load Balancer

Use tags to include/exclude resources (optional)

**Apply policy?**

- Create and apply this policy to existing and new resources. ⓘ
- Create but do not apply this policy to existing or new resources. ⓘ

\* Required [Cancel](#) [Previous](#) [Next](#)

### Choose an option

- Create an AWS Firewall Manager policy and add existing rule groups.
- Create an AWS Firewall Manager policy and add a new rule group.

### Choose a region

The service will create the policy and any associated conditions, rules, and rule groups that you choose. The policy will protect only the resources in that region.

**Region\*** US East (N. Virginia)

If the policy will apply to CloudFront distributions, choose Global (CloudFront).

[Cancel](#) [Next](#)

Status
! Noncompliant
! Noncompliant
! Noncompliant

# AWS Secrets Manager

AWS Secrets Manager > Secrets > Store a new secret

## Store a new secret

Select secret type [Info](#)

Credentials for RDS database  Credentials for other database  Other type of secrets (e.g. API key)

Specify the user name and password to be stored for this secret. [Info](#)

User name:

Password:

Show password

Select the encryption key [Info](#)

Select the AWS KMS key to use to encrypt your secret information. You can encrypt key that AWS Secrets Manager creates on your behalf or a customer master key (CMK).

DefaultEncryptionKey

[Add new key](#)

Select which RDS database this secret will access [Info](#)

DB instance	DB Engine	Status	Creation date
<input checked="" type="radio"/> twitterapp2	aurora	available	04/02/2018
<input type="radio"/> twitterapp2-us-east-1a	aurora	available	04/02/2018

AWS Secrets Manager > Secrets > Store a new secret

## Store a new secret

Step 1 Secret type

Step 2 Name and description

Step 3 Configure rotation

Step 4 Review

### Secret name and description [Info](#)

Secret name

Give the secret a name, that enables you to find and manage it easily.

Secret name can contain alphanumeric characters and the characters `./_+@-`

Description - optional

Maximum 250 characters

AWS Secrets Manager > Secrets > Store a new secret

## Store a new secret

Step 1 Secret type

Step 2 Name and description

Step 3 Configure rotation

**!** If you enable automatic rotation, the first rotation will happen immediately when you store this secret. If this secret is already in use, you must update your applications to retrieve it from AWS Secrets Manager. Read the [getting started guide on rotation](#).

### Configure automatic rotation - optional [Info](#)

Configure AWS Secrets Manager to rotate this secret automatically. Read the [getting started guide on rotation](#).

Disable automatic rotation  
Recommended when your applications are using this secret and have not been updated to use AWS Secrets Manager.

Enable automatic rotation  
Recommended when your applications are not using this secret yet.

Select rotation interval [Info](#)

This secret will be rotated based on the schedule you determine.

Custom  days

Maximum 365 days

Select which secret will be used to perform the rotation [Info](#)

Use the secret that I provided in step 1  
Use this option if you are storing a super user.

Use a secret that I have previously stored in AWS Secrets Manager  
Use this option if you are storing a user who will access the database programmatically. ASM will use a previously stored super user to execute rotation.

# AWS Config Rules aggregation



### Aggregated view

Aggregator: MyAgg | Region: All regions | Account: All accounts

Note: Data displayed in the dashboard is received from multiple aggregation sources and is refreshed at different intervals. Data might be delayed by a few minutes.

#### Config rule compliance

11 Noncompliant rule(s)

#### Top 5 noncompliant rules

Rule name	Region	Account	Compliance
cloudwatch-alar...	us-west-2	[blurred]	20 noncompliant resource(s)
iam-user-group-...	us-west-2	[blurred]	7 noncompliant resource(s)
s3-bucket-server...	us-west-2	[blurred]	7 noncompliant resource(s)
restricted-ssh	us-west-2	[blurred]	3 noncompliant resource(s)
approved-amis-b...	us-west-2	[blurred]	2 noncompliant resource(s)

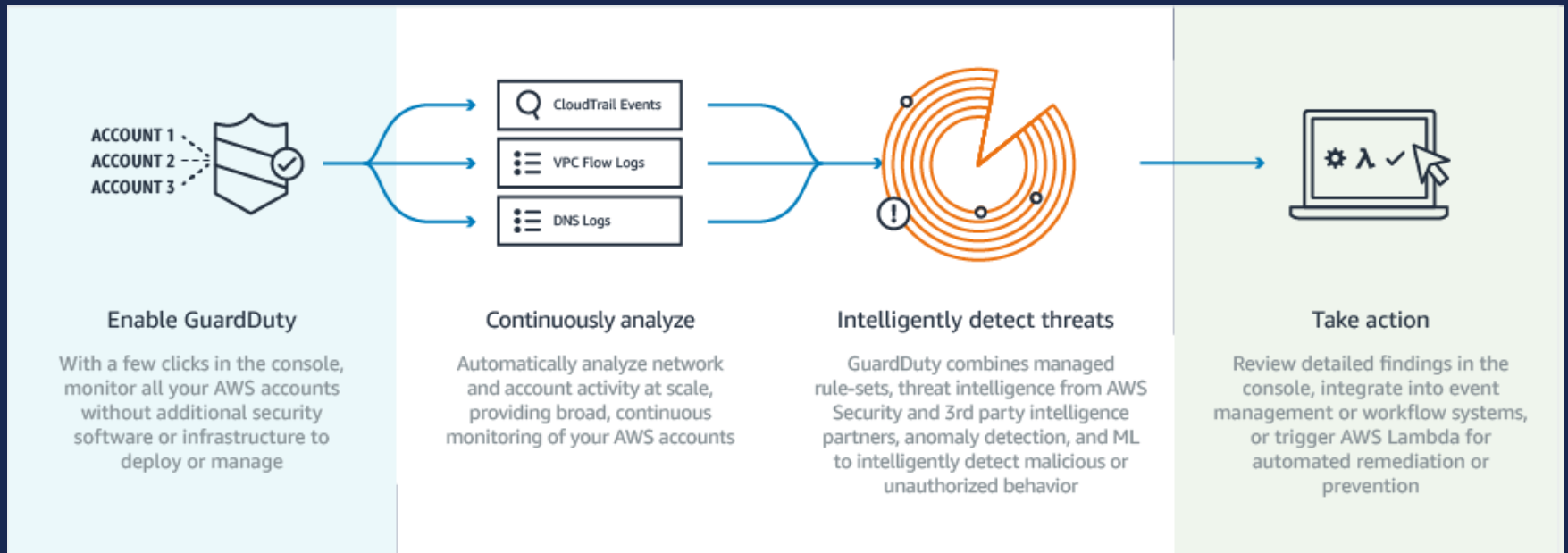
[View all noncompliant rules](#)

#### Accounts by noncompliant rules

Account	Compliance
[blurred]	6 noncompliant rule(s)
[blurred]	5 noncompliant rule(s)

[View all noncompliant rules](#)

# Amazon GuardDuty



# AWS Quick Starts

# What are AWS Quick Starts?

- AWS Quick Starts are:
  - built by AWS solutions architects and partners
  - help you deploy popular solutions on AWS
  - based on AWS best practices for security and high availability
- Covers a wide range of topics
  - DevOps; Security & Compliance
  - Database & Storage; Big Data & Analytics
  - Microsoft & SAP

- <https://aws.amazon.com/quickstart/>

# Security-focused Quick Starts



## HIPAA

Reference architecture that helps support your HIPAA compliance program  
[Learn more](#) | [View guide](#)



## NIST

AWS architecture that helps supports NIST, DoD, FedRAMP standards  
[Learn more](#) | [View guide](#)



## NIST High-Impact

AWS architecture for NIST high-impact controls, featuring Trend Micro  
[Learn more](#) | [View guide](#)



## PCI DSS

Standardized AWS architecture that helps support PCI DSS compliance  
[Learn more](#) | [View guide](#)



## UK-OFFICIAL

AWS architecture that supports the UK's NCSC and CIS security controls  
[Learn more](#) | [View guide](#)



## CIS Benchmark

Security configurations for the CIS AWS Foundations Benchmark  
[Learn more](#) | [View guide](#)



## CJIS Security Policy

Standardized AWS architecture to help support CJIS Security Policy 5.6  
[Learn more](#) | [View guide](#)



## Deep Security

Security solution with intrusion prevention, anti-malware, host firewall  
[Learn more](#) | [View guide](#)



## Sophos web proxy

Sophos UTM and Outbound Gateway for outbound web filtering proxy on AWS  
[Learn more](#) | [View guide](#)



## Symantec Protection Engine

Content scanning, malware and threat detection  
[Learn more](#) | [View guide](#)



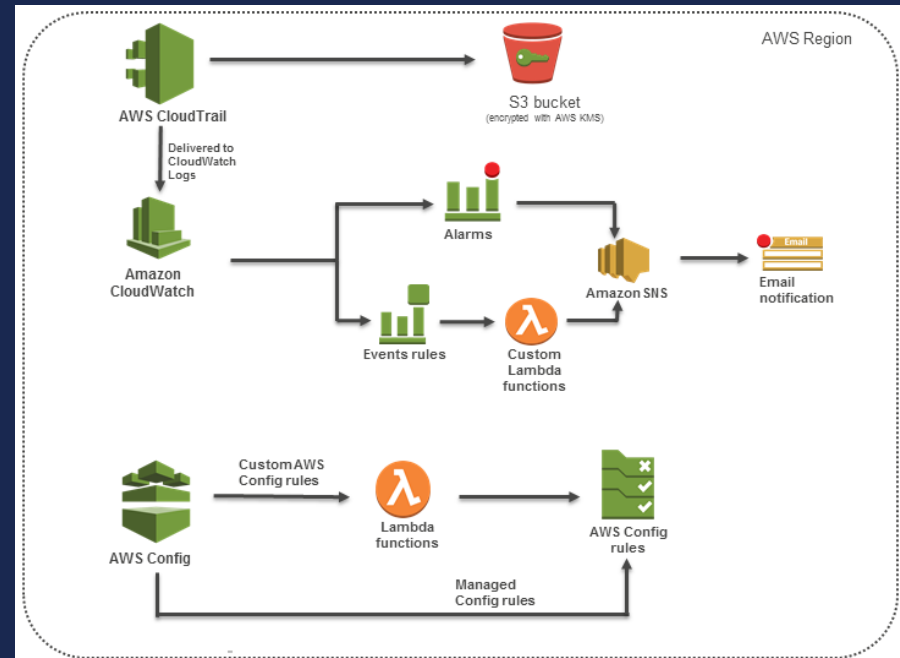
## Security and analytics with Palo Alto Networks and Splunk

Palo Alto Networks VM-Series firewall and Splunk Enterprise on AWS  
[Learn more](#) | [View guide](#)

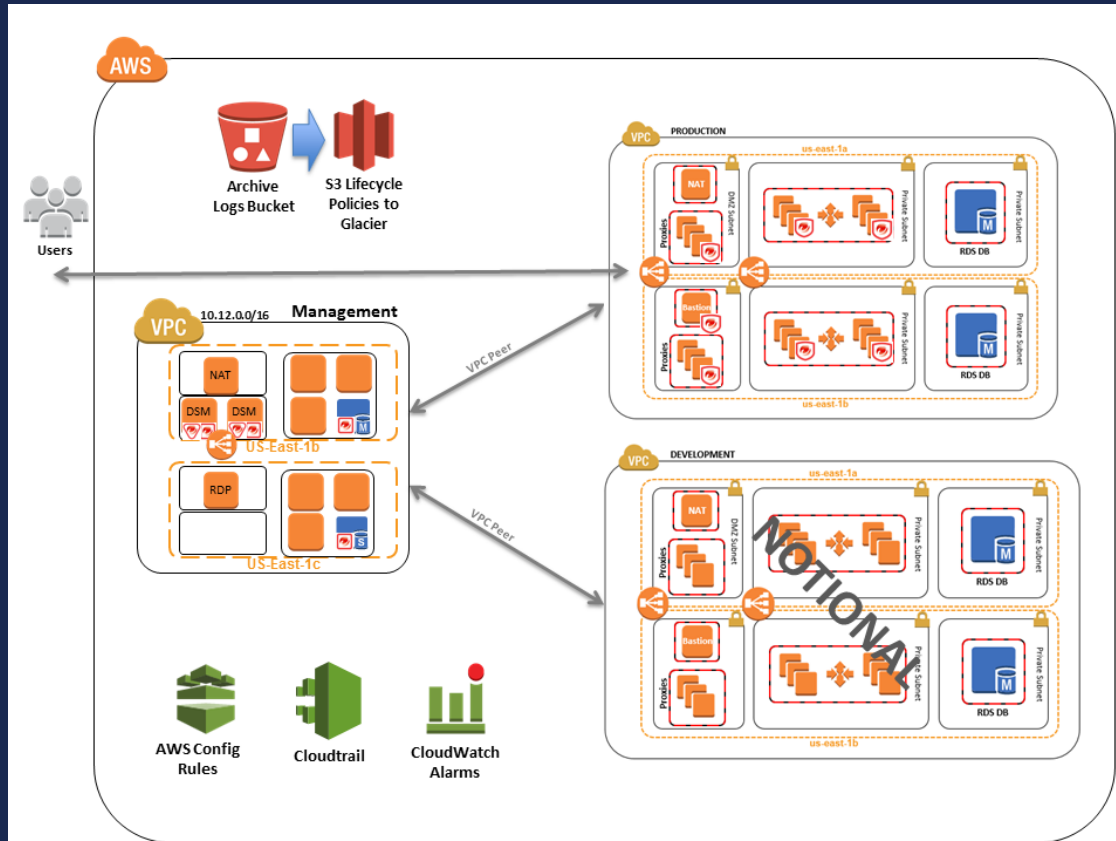


# CIS Benchmark on AWS

- Standardised architecture for the Center for Internet Security (CIS) AWS Foundations Benchmark.
- Deploys the following AWS services
  - AWS Config rules
  - CloudWatch alarms
  - CloudWatch Events
  - Lambda functions
  - AWS CloudTrail
  - AWS Config

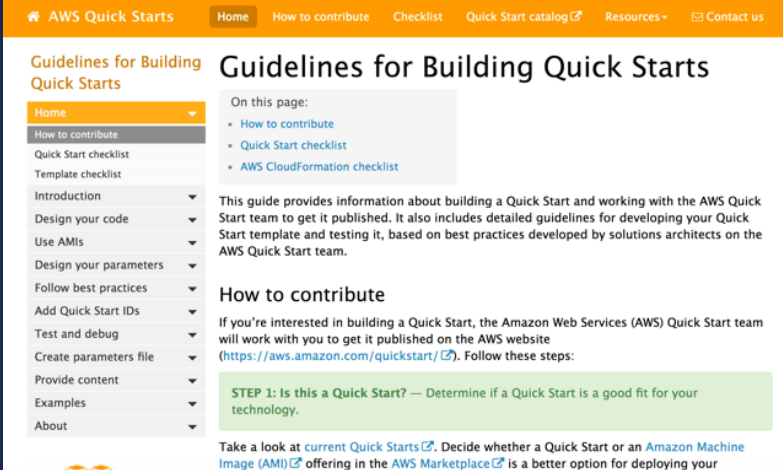


# NIST High-Impact on AWS



# Building your own AWS Quick Start

- <https://aws-quickstart.github.io/>
- Advice on code design & deployment
- AMI configuration and regionalisation
- Parameterising CloudFormation
- Learn about best practices



The screenshot shows the AWS Quick Start website. The navigation bar includes 'AWS Quick Starts', 'Home', 'How to contribute', 'Checklist', 'Quick Start catalog', 'Resources', and 'Contact us'. The main content area is titled 'Guidelines for Building Quick Starts'. On the left, there is a table of contents with a dropdown menu. The 'How to contribute' section is expanded, showing links to 'Quick Start checklist' and 'Template checklist'. The main content area includes a section 'On this page:' with links to 'How to contribute', 'Quick Start checklist', and 'AWS CloudFormation checklist'. Below this is a paragraph explaining the guide's purpose. The 'How to contribute' section is also visible, with a sub-section 'STEP 1: Is this a Quick Start?' and a paragraph about current Quick Starts.

# AWS Answers

# What is AWS Answers?

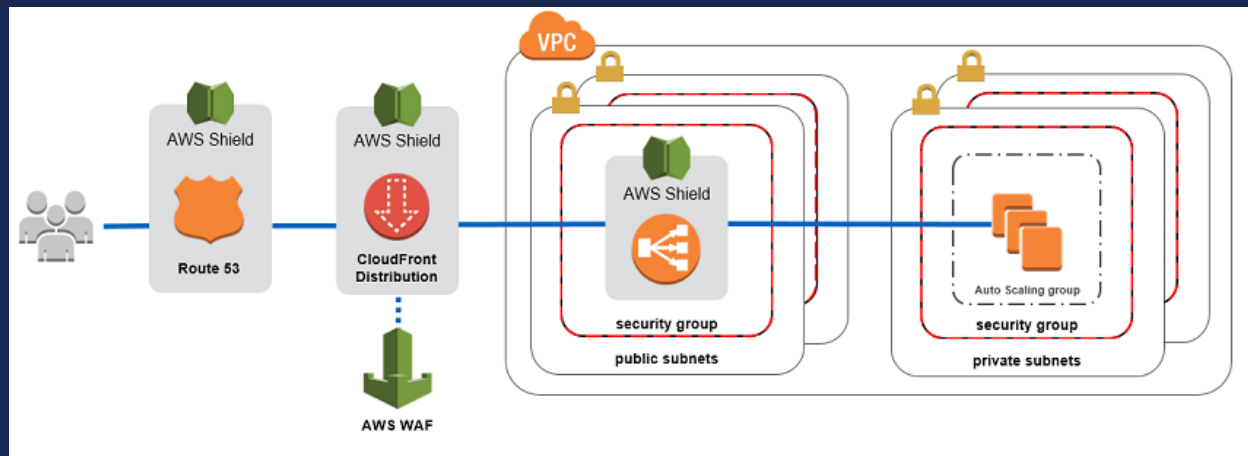
- Offers clear answers to common questions about architecting, building, and running applications on AWS
  - Repository of instructional documents and solutions
  - Outlines AWS best practices & provides prescriptive architectural guidance
- <https://aws.amazon.com/answers/>

# Examples of security-focussed AWS Answers

- Account security
  - How do I ensure I set up my AWS account securely?
  - How do I setup AWS IAM for my organisation?
  - What are the native AWS security-logging capabilities?
- EC2 security
  - What is the recommended EC2 baseline configuration?
  - How do I control OS-level access to my EC2 instances?
- Application security
  - How do I protect my applications from DDoS attacks?

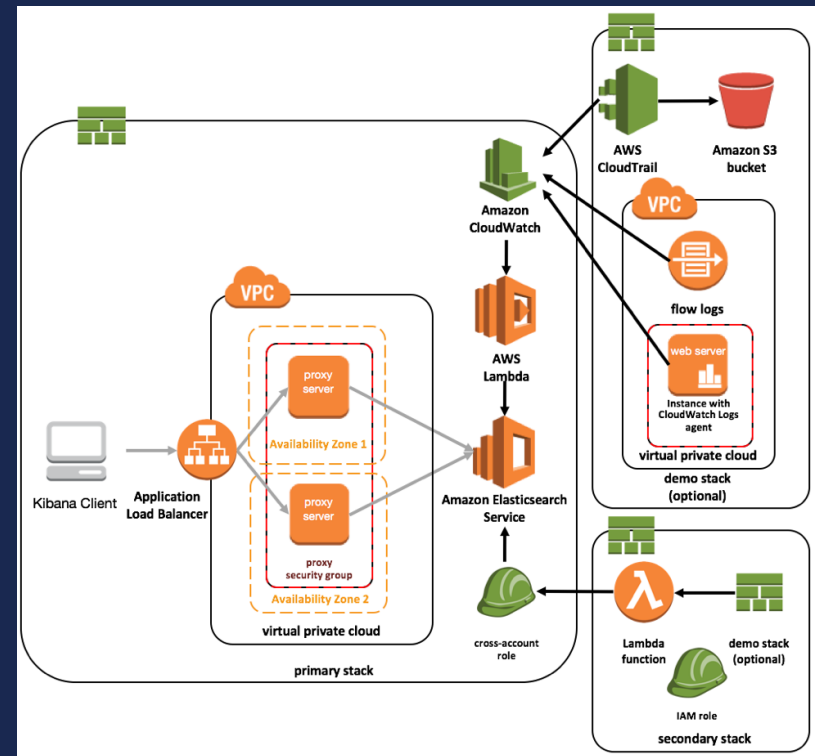
# Protecting web applications from DDoS attacks

- AWS provides flexible infrastructure and services that help customers implement strong DDoS mitigations and create highly available application architectures



# Centralised Logging

- Deploy a centralised logging solution using AWS CloudFormation
- Extend your logging capabilities beyond default AWS service logs.
- Control access to your dashboards
- Simplify data visualisation using built-in Amazon ES support for Kibana



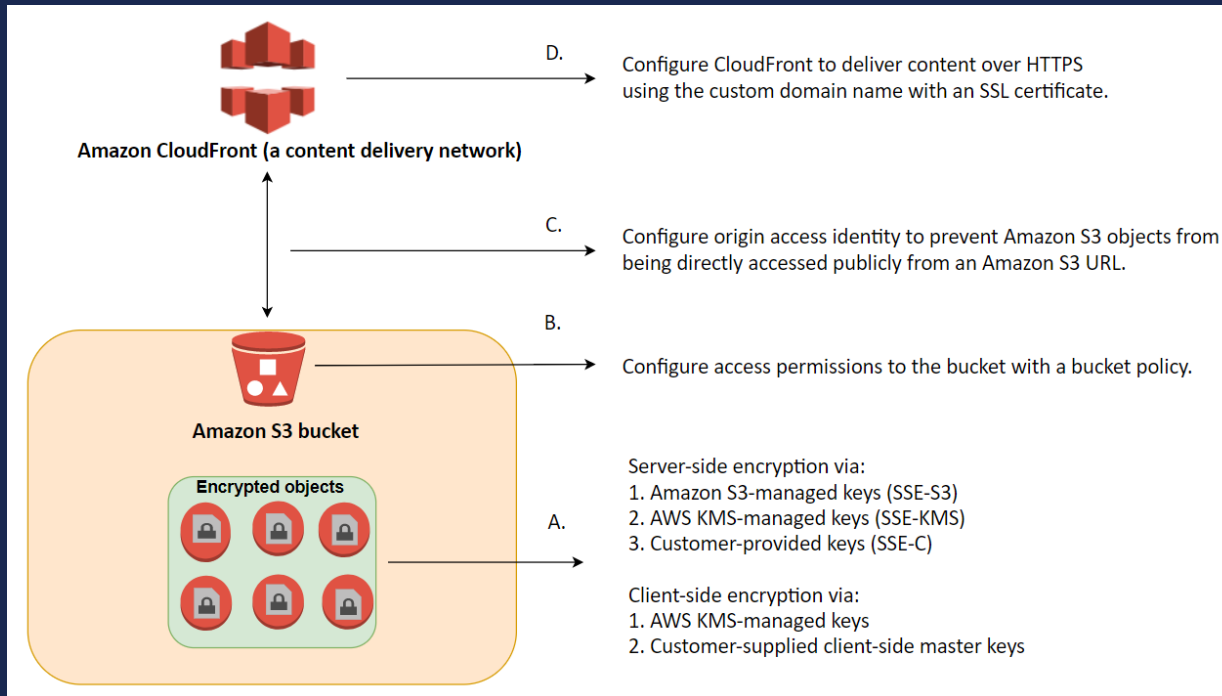


# AWS Blogs

# What are AWS Blogs?

- New service / functionality announcements
- Best practice guidance
- Customer references and case studies
- Key blogs from a security perspective:
  - AWS Security: <https://aws.amazon.com/blogs/security/>
  - AWS Management Tools: <https://aws.amazon.com/blogs/mt/>
  - AWS Architecture: <https://aws.amazon.com/blogs/architecture/>
- <https://aws.amazon.com/blogs/>

# Securing data on S3 using bucket policies



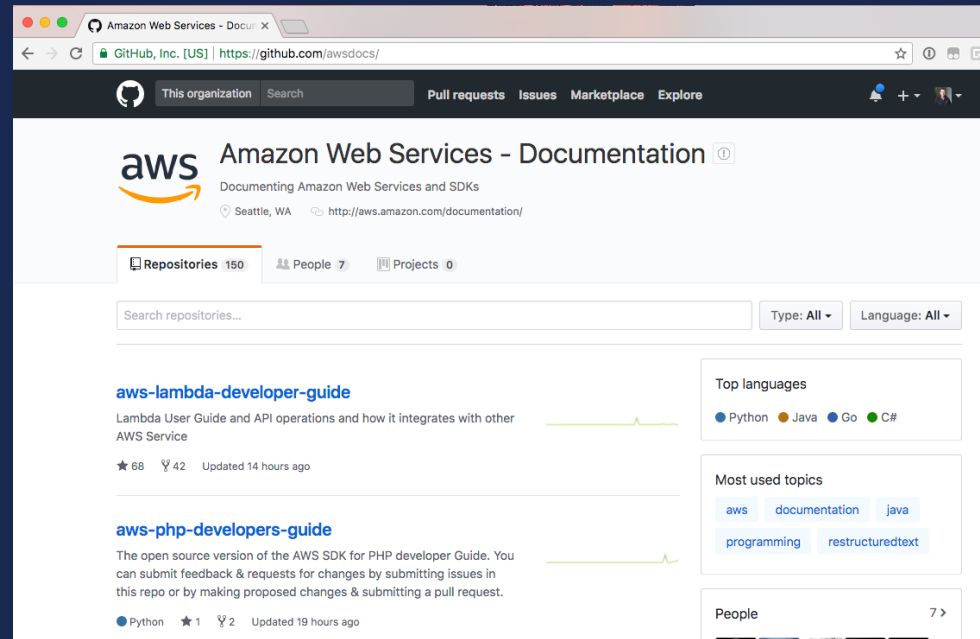
<https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-your-amazon-s3-data/>

# AWS Documentation

# AWS Documentation







- AWS Documentation is now available in GitHub
- Accepting pull requests for content updates, errata, and code samples

<https://github.com/awsdocs/>



# AWS Partners

# AWS Marketplace security partners

Infrastructure Security	Logging and Monitoring	Identity and Access Control	Configuration and Vulnerability Analysis	Data Protection
         	    	    	    	     

# Recap

- In AWS, security is our TOP priority
- Shared Responsibility Model; security...
  - ...**OF the cloud**: build on our security controls
  - ...**IN the cloud**: use our extensive security features
- Use abstracted services to let you focus on applications
- Automation is your friend
- Make use of available AWS resources, docs, and examples



# Key take-aways

- AWS Cloud:
  - Is the **new normal**, and security is **still familiar**
  - **Improves security** for nearly all customers
  - Simplifies the work of **security and compliance**
  - Delivers unprecedented **visibility and control**
  - Enables agility and speed through **automation**

Finally, some links to remember...



- <https://aws.amazon.com/security/>



<https://aws.amazon.com/compliance/>

Thank you!



Virginia Information Technologies Agency

# Upcoming events





# Cybersecurity Awareness Month: Oct. 2020

**DO YOUR PART.**  
**#BECYBERSMART**





## Theme for 2020

*Do Your Part. #BeCyberSmart*

Helping to empower individuals and organizations to own their role in protecting their part of cyberspace.



## Weekly themes

Oct. 1 and 2: Official NCSAM kick-off

Week of Oct. 5 (Week 1): If You Connect It, Protect It

Week of Oct. 12 (Week 2): Securing Devices at Home and Work

Week of Oct. 19 (Week 3): Securing Internet-Connected Devices in Healthcare

Week of Oct. 26 (Week 4): The Future of Connected Devices



# Resources

- <https://staysafeonline.org/cybersecurity-awareness-month/theme/>
- <https://www.cisa.gov/national-cyber-security-awareness-month>
- <https://www.dhs.gov/publication/dhs-speaker-request-form>
- <https://www.cisa.gov/cisa-cybersecurity-resources>
- <https://www.cisa.gov/national-cybersecurity-awareness-month-sample-social-media-posts-and-graphics>





# IS Orientation

IS Orientation

Sept. 30 at 1 p.m.

Presenter: Marlon Cole

Registration Link:

<https://covaconf.webex.com/covaconf/onstage/g.php?MTID=e68b787865f20af9aaa799b14b366af31>



# COVITS 2020

government  
technology

# VIRTUAL COVITS

September 9-10, 2020



## Future ISOAG

**Oct. 7, 2020**

**Speakers:**

**Randy Marchany, VT – Remote Security Threats**

**Dan Han, VCU – Dangers of using Teleconference & Online Classroom Training**

***ISOAG meets the first Wednesday of each month in 2020***

# ADJOURN

## THANK YOU FOR ATTENDING

