Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

Sept. 2

AGENDA

- **Mike Watson, Opening & Welcome Remarks**
- **David Raymond, Virginia Cyber Range**
- **Peter Smith, Zscaler**
- **Milty Brizan, Amazon Web Services**

Virginia Cybersecurity Education – Leading the Nation!

VIRGINIA CYBER RANGE

David Raymond, Ph.D.
Director, Virginia Cyber Range
draymond@virginiacyberrange.org

Cybersecurity Talent Shortfalls

CyberSeek™

National level

TOTAL CYBERSECURITY JOB OPENINGS

504,316

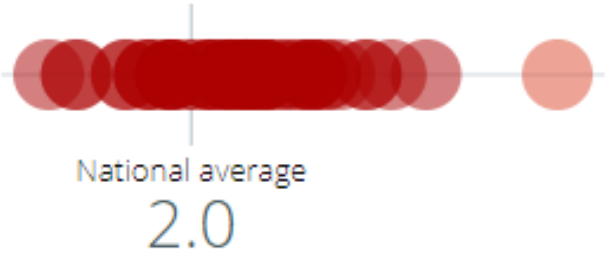
TOTAL EMPLOYED CYBERSECURITY WORKFORCE

997,058

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO



Cybersecurity Talent Shortfalls

CyberSeek™

Virginia

TOTAL CYBERSECURITY JOB OPENINGS

49,669

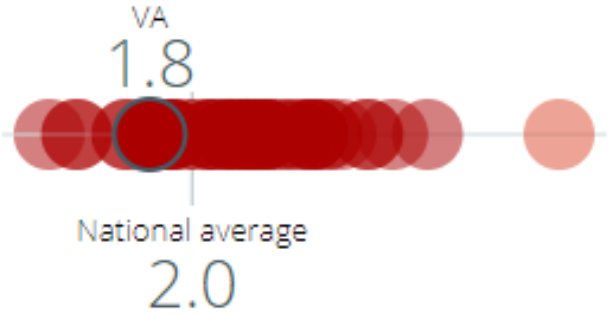
TOTAL EMPLOYED CYBERSECURITY WORKFORCE

88,166

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO



How do we solve this?

Making Virginia a National Resource for Cybersecurity Education

VIRGINIA
CYBER RANGE

Virginia Higher Ed Cybersecurity Education: Recent Developments

- Rapid increase in NSA-certified Centers for Academic Excellence in Cybersecurity Education (CAE)
  - Virginia has doubled the number of CAEs since 2016, from 11 to 22
- George Mason University Cybersecurity Engineering Department
  - Unique in the nation!
- Radford IMPACT program
  - Online, competency-based programs in cybersecurity
  - Workforce development for cybersecurity and geospatial intelligence
  - Includes cybersecurity certificate program for Virginia K12 teachers

Commonwealth Cyber Initiative

- Collaborative effort among academia and industry, started in 2018
  - 21 Universities; 320 Faculty
  - $99M+ in sponsored research
  - 5G Testbed
  - AI Assurance research
- $20M annual investment from the state
- Led by Virginia Tech
  - Dr. Luiz DaSilva – Executive Director

Four Regional Nodes

- Northern Virginia
  - GMU
- Central Virginia
  - VCU
- Coastal Virginia
  - ODU
- Southwest Virginia
  - VT

"Building an engine for research, innovation, and commercialization of cybersecurity technologies"

VDOE Cybersecurity Career Pathway Courses

Career Pathways[1]
Coherent Sequence (Concentration[2]) of State-Approved Courses

Year I Course* (Grade 9, 10, or 11)	Year 2 Course (Grade 10, 11, or 12)	Year 3 Course (Grade 10, 11, or 12)	Year 4 Course (Grade 12)
Programming & Software Development Pathway[1] **Cybersecurity Fundamentals** (Course Code 6302)	**Cybersecurity Software Operations** (Couse Code 6304)	**Cybersecurity Software Operations, Advanced** (Course Code 6306)	*To be developed*
Health & Medical Sciences Pathway[1] **Cybersecurity Fundamentals** (Course Code 6302)	**Health Informatics** (Course Code 8338)	*To be developed*	*To be developed*
STEM/Pre-Engineering Technology Pathway[1] **Cybersecurity Fundamentals** (Course Code 6302)	**Cybersecurity in Manufacturing** (Course Code 8499)	*To be developed*	*To be developed*
Network Systems Pathway[1] **Cybersecurity Fundamentals** (Course Code 6302)	**Cybersecurity Systems Technology** (Course Code 8628)	**Cybersecurity Systems Technology, Advanced** (Course Code 8629)	**Cybersecurity Network Systems** (Course Code 8630)

**The Cybersecurity Fundamentals course (Year 1) serves as the "core" for all Year 2 courses in the coherent sequence.*

6302: Cybersecurity Fundamentals
6304: Cybersecurity Software Operations
8338: Health Informatics
8628: Cybersecurity Systems Technology
8499: Cybersecurity in Manufacturing
6306: Cybersecurity Software Operations, Advanced
8629: Cybersecurity Systems Technology, Advanced
8630: Cybersecurity Network Systems
8000: Cybersecurity in Food and Agriculture Industry
8200: Cybersecurity in Family and Work Life
8100: Cybersecurity in Digital Marketing

Virginia Cyber Range

What is a *Cyber Range*?

- ❑ Isolated network
  - Activity will appear malicious
  - Actual malware sometimes used
- ❑ Usually virtualized
  - Allows for maximum configurability
  - Scripted network environment creation
- ❑ Used for:
  - Hands-on cybersecurity training
    - Defensive AND offensive
    - Classroom exercises
    - Capture-the-flag and red/blue CTFs
  - Device and software testing

VIRGINIA
CYBER RANGE

Virginia Cyber Range: Background

- Recommended by the Virginia Cyber Security Commission in Aug. 2015
- Funded by Commonwealth of Virginia on July 1st, 2016
- *The only state-wide effort of its kind*

2016 Executive Budget Document, Item 224, Paragraph J:

"Out of this appropriation, [two years of funding will be] ***designated to support a cyber range platform*** *to be used for cyber security training by students in* ***Virginia's public high schools, community colleges, and four-year institutions.*** *Virginia Tech shall form a* ***consortium among participating institutions****, and shall serve as the coordinating entity for use of the platform. The* ***consortium should initially include all Virginia public institutions with a certification of academic excellence*** *from the federal government."*

VIRGINIA
CYBER RANGE

Governance: Executive Committee

- Danville Community College
- George Mason University
- Germanna Community College
- James Madison University
- Longwood University
- Lord Fairfax Community College
- Norfolk State University
- Northern Virginia Community College
- Old Dominion University
- Radford University
- Southwest Virginia Community College
- Thomas Nelson Community College
- Tidewater Community College
- University of Virginia
- Virginia Commonwealth University
- Virginia Tech
- Virginia Western Community College

VIRGINIA CYBER RANGE

Leveraging the Public Cloud

Design Requirements:

- ❑ Scale to support thousands of students
- ❑ Up and running quickly
- ❑ Completely automatable
- ❑ Cost effective
- ❑ Short-term surge capacity
- ❑ Available state-wide (or anywhere?)
- ❑ Web portal for access to content
  - Role-based access
  - Login to see user-specific content
  - Students just need a web browser and internet connection!

aws

Why the Cloud?

- ***Unlimited scalability!***
- Quick start-up phase
- Low capital investment
- Rapid scalability
- Surge capacity
- Location independent
- Highly automated
- Available anywhere

VIRGINIA CYBER RANGE

Courseware Repository

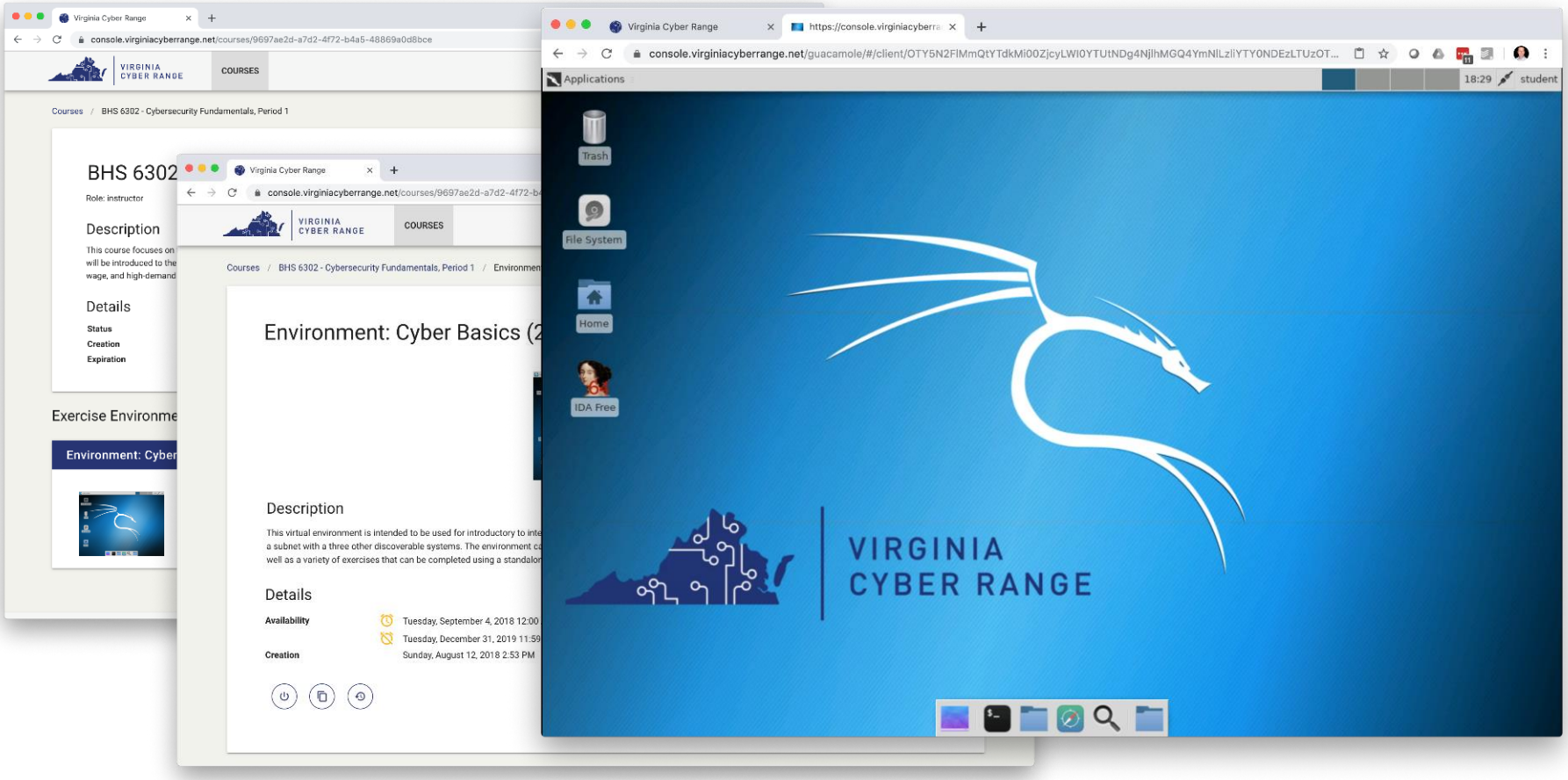
- Courses, modules, and exercises for use in HS, CC, and university cybersecurity curricula
  - Instructors/professors can select course content in full or *a la carte*
- Grants offered for courseware development

Exercise Area

- Menu of per-student, isolated exercise environments for use in cybersecurity courses
- Instructors provision for their students – no delays waiting for administrators
- Capture-the-Flag infrastructure for cybersecurity competitions

Community of Purpose

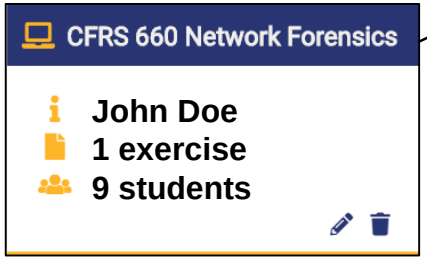
- Consortium governance
- Convene workshops and conferences to "teach the teachers" and share best practices
- Helping to expand NSA/DHS CAE certification among Virginia colleges and universities



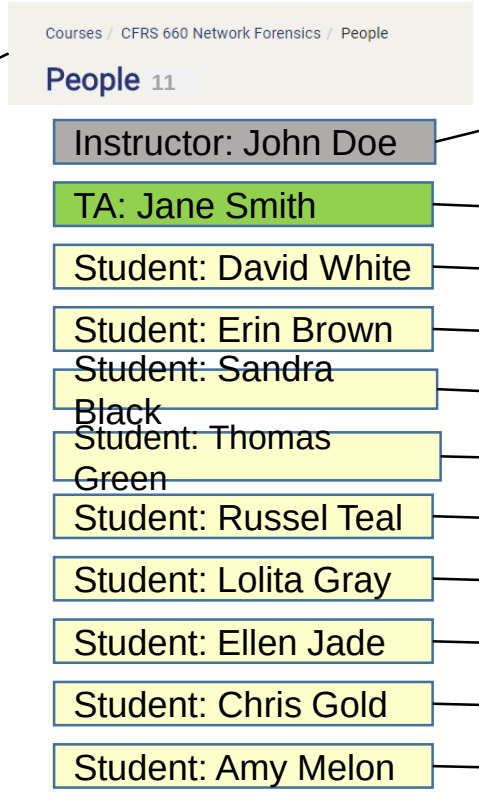
Making Virginia a National Resource for Cybersecurity Education

VIRGINIA
CYBER RANGE

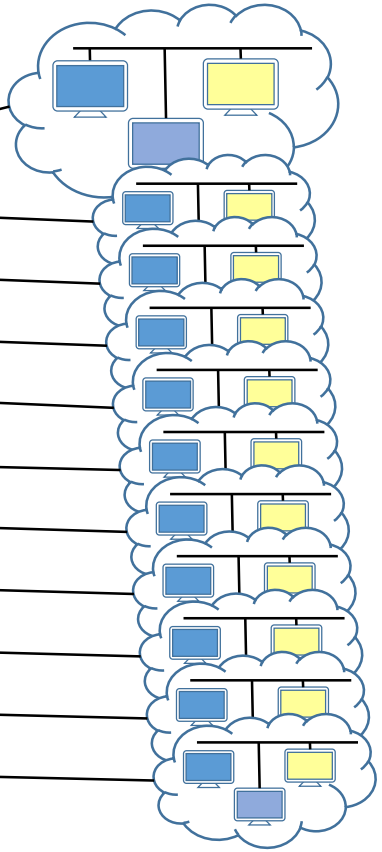
Step 1: Create Course

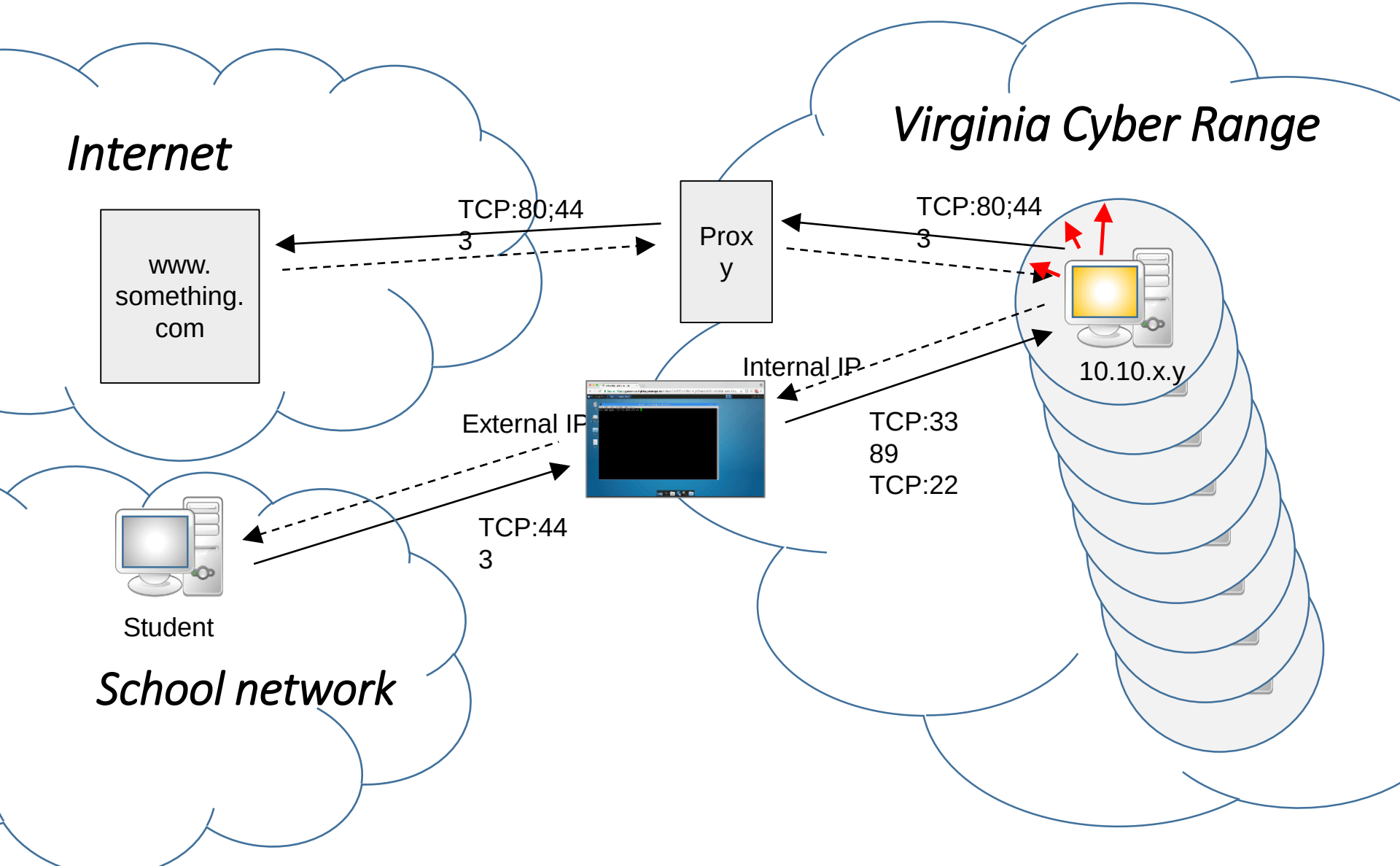


Step 2: Enroll Students



Step 3: Provision Environments




Internet
www. something. com
TCP:80;443
Prox y
TCP:80;443
Virginia Cyber Range
10.10.x.y
Internal IP
External IP
TCP:3389
TCP:22
TCP:443
Student
School network

Capture the Flag!

- Just deployed new **CloudCTF** platform to the Virginia Cyber Range
- Players solve "challenges" across a variety of categories, including networking, cryptography, web, exploitation, and reconnaissance.
- Great to introduce newbies to cybersecurity, and to challenge experts!
- Used for:
  - In-class gamification and topic reinforcement
  - Cybersecurity clubs and teams
  - Conferences and other outreach events

VIRGINIA
CYBER RANGE

Cloud CTF

vacybereducon.ctf.virginiacyberrange.org/challenges/forensics

CLOUD CTF

CHALLENGES MY TEAM SCOREBOARD ADMINS

D

Challenges

AWS CIRCADENCE CRYPTO FORENSICS LINUX MALWARE NCI NETWORKING PROOFPOINT RECONNAISSANCE REVERSING AND EXPLOITATION WEB

Beneath The Surface	Variability	Secret Zip	Ephemeral
25	40	60	75

Rank	Team	Scores
1	Team Robert Marmorstein	1809
2	Team Maureen Lawrence-Kuether	1644
3	Team Kristi Rice	986

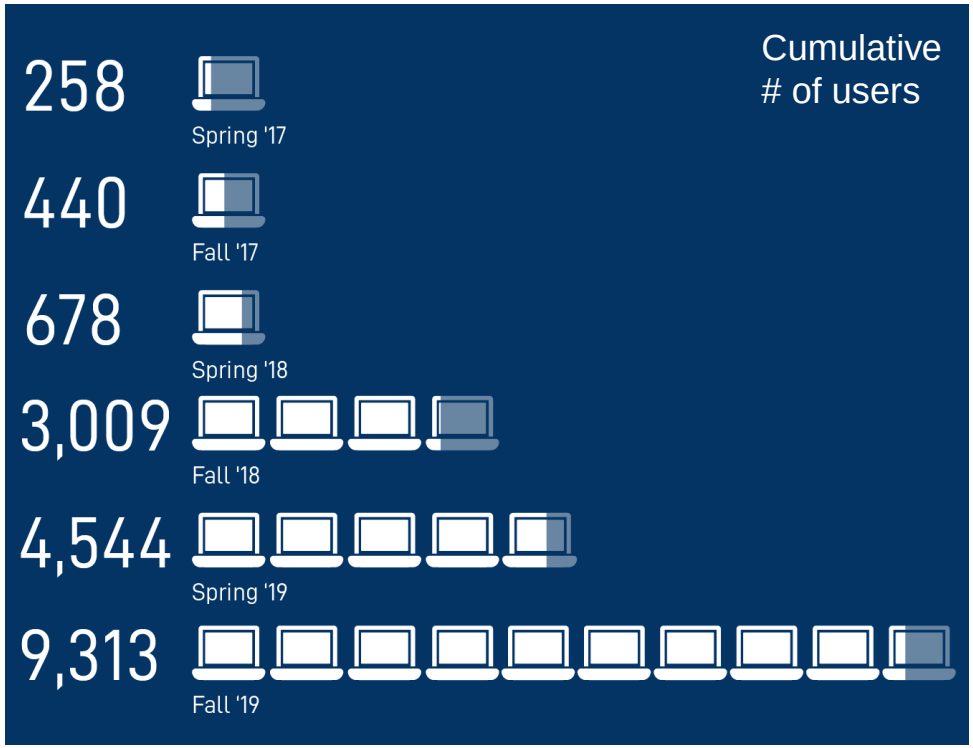
Time	Activity
Aug 31, 3:44 Pm	Team Maureen Lawrence-Kuether has captured Nuclear Crypto Shark.
Aug 31, 3:36 Pm	Team Ellen Test has captured Variability.
Aug 31, 2:22 Pm	Team Maureen Lawrence-Kuether has captured Ephemeral.

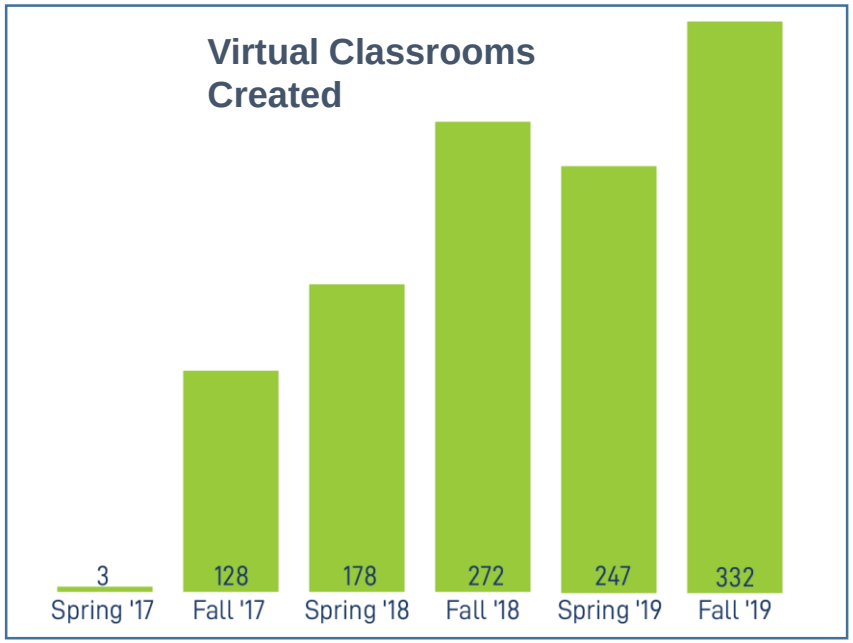
Ends in

29 : 21 : 41 : 58

days hours minutes seconds

Exercise Area Stats

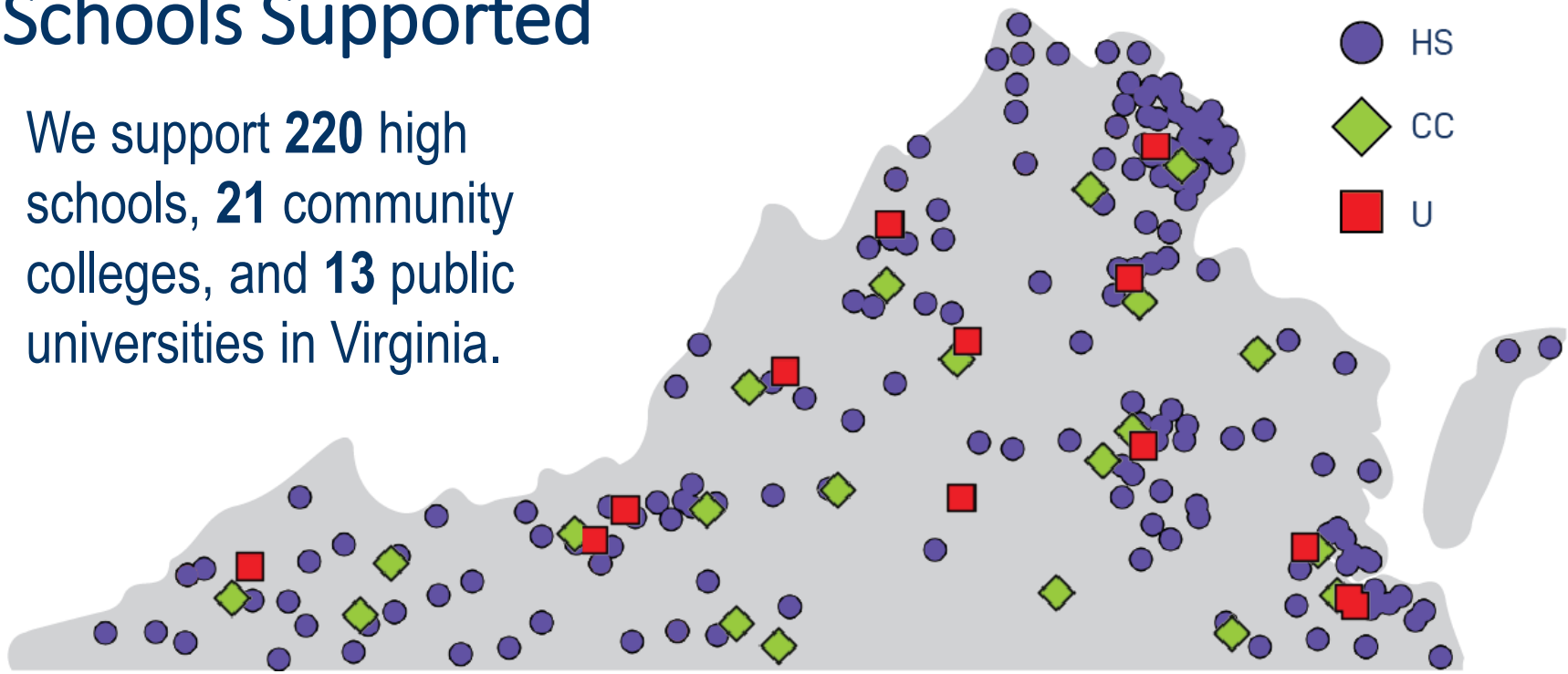




20,000 Virtual Machines Provisioned in Fall 2018

Schools Supported

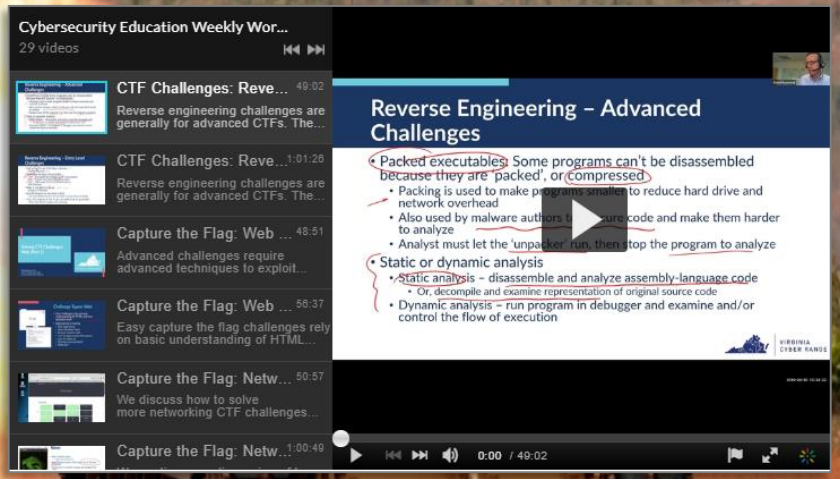
We support **220** high schools, **21** community colleges, and **13** public universities in Virginia.



* Each dot represents a different Virginia high school, community college, or university.

Community

Teacher Camps and Live Conference Workshops



Online Weekly Workshops' (Recorded)

VIRGINIA CYBER RANGE

Annual Virginia Cybersecurity Education Conference

- 2 Days in July/Aug
  - Day 1: Workshops and keynote
  - Day 2: Talks and panels

2018 VIRGINIA CYBERSECURITY EDUCATION CONFERENCE

2019 VIRGINIA CYBERSECURITY EDUCATION CONFERENCE

VIRTUAL VIRGINIA CYBERSECURITY EDUCATION CONFERENCE 2020

NCI OPPORTUNITY. GROWTH. SUCCESS.

SyCom Connected.

SANS

aws

proofpoint

ISACA Virginia Chapter

VIRGINIA TECH.

GEORGE MASON UNIVERSITY Volgenau School of Engineering

ABS TECHNOLOGY

IEEE

LFCC Lord Fairfax Community College

VIRGINIA CYBER RANGE

US Cyber Range

- Providing Cyber Range as a Service
  - Schools outside of Virginia
  - Private schools in Virginia
  - Government and industry nationwide
  - 33 Customers in 20 states
- Customer organizations contract with Virginia Tech
  - "Service Center" within the university
  - Cost reimbursement model
- Students and teachers access cloud-based network infrastructure and CTFs via web portal

U.S. CYBER RANGE

VIRGINIA
CYBER RANGE

How Can *You* Help?

- Partner with Commonwealth Cyber Initiative and other orgs to support and expand cyber education in Virginia
  - More info here: https://cyberinitiative.org/
- Support continued high school cybersecurity courses in your district
  - Reach out to Career and Technical Education (CTE) departments and offer your expertise
- Be a CyberPatriot team mentor
  - Go to https://www.uscyberpatriot.org/ to register

“The Virginia Cyber Range has enabled me to teach a Cybersecurity class without needing expensive hardware and software.”

“Without this environment, my students would have only learned theory and seen pictures of what a professional might use in this work.”

“The Virginia Cyber Range is a definite game changer!”

“There are a variety of big-ticket range products out there that are just unwieldy and hard to implement. This is quick, easy, and to the point!”

VIRGINIA
CYBER RANGE

Questions?

VIRGINIA CYBER RANGE

Making Virginia a national resource for cybersecurity education.

CONNECT WITH US

@VaCyberRange

virginiacyberrange.org

Microsegmentation Powered By Zero Trust

Peter Smith

VP, Zscaler Workload Segmentation

Agenda

Why microsegmentation?

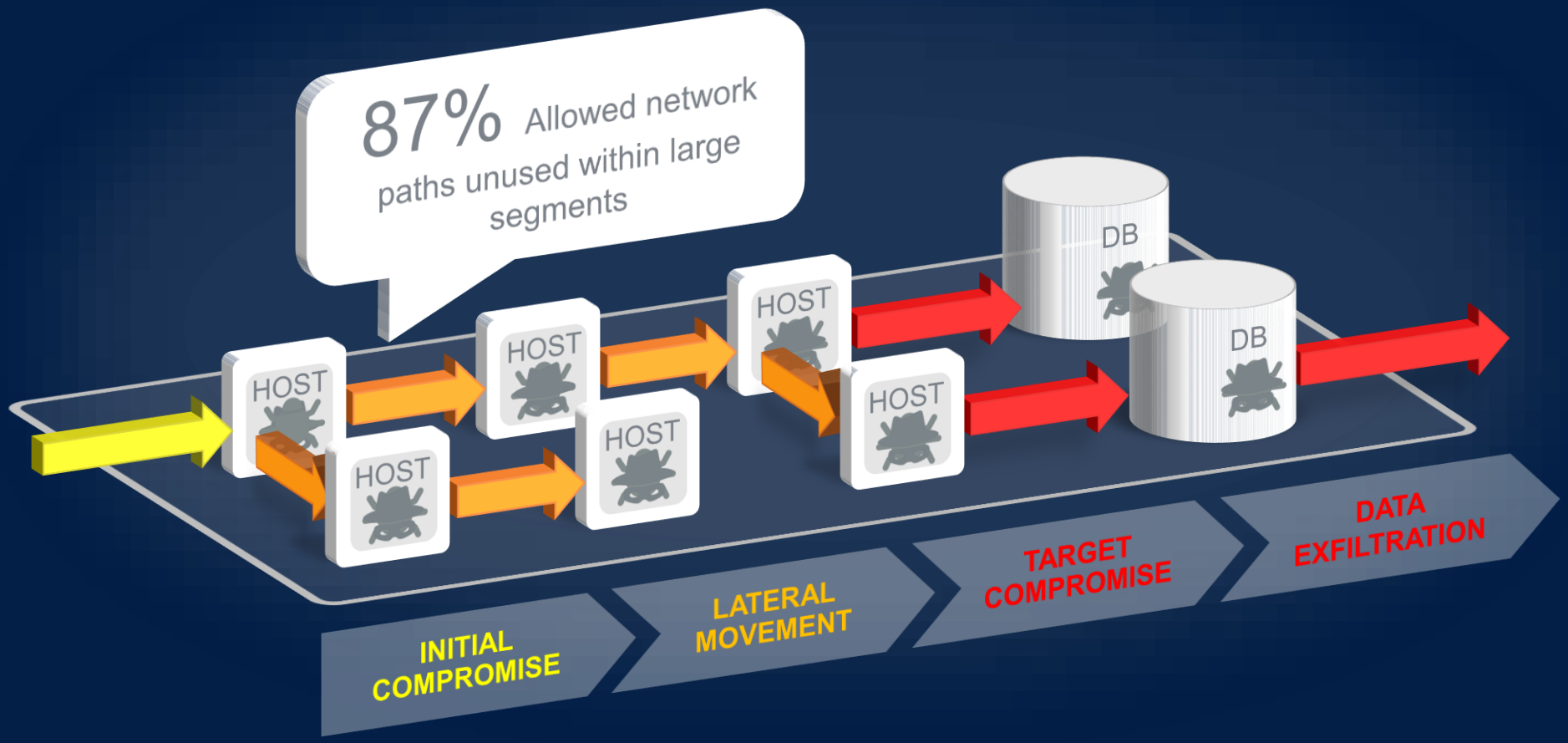
Limitations of existing approaches

A new approach based on zero trust and automation

Demo

Q&A

Flat Networks Allow Too Many Attack Paths

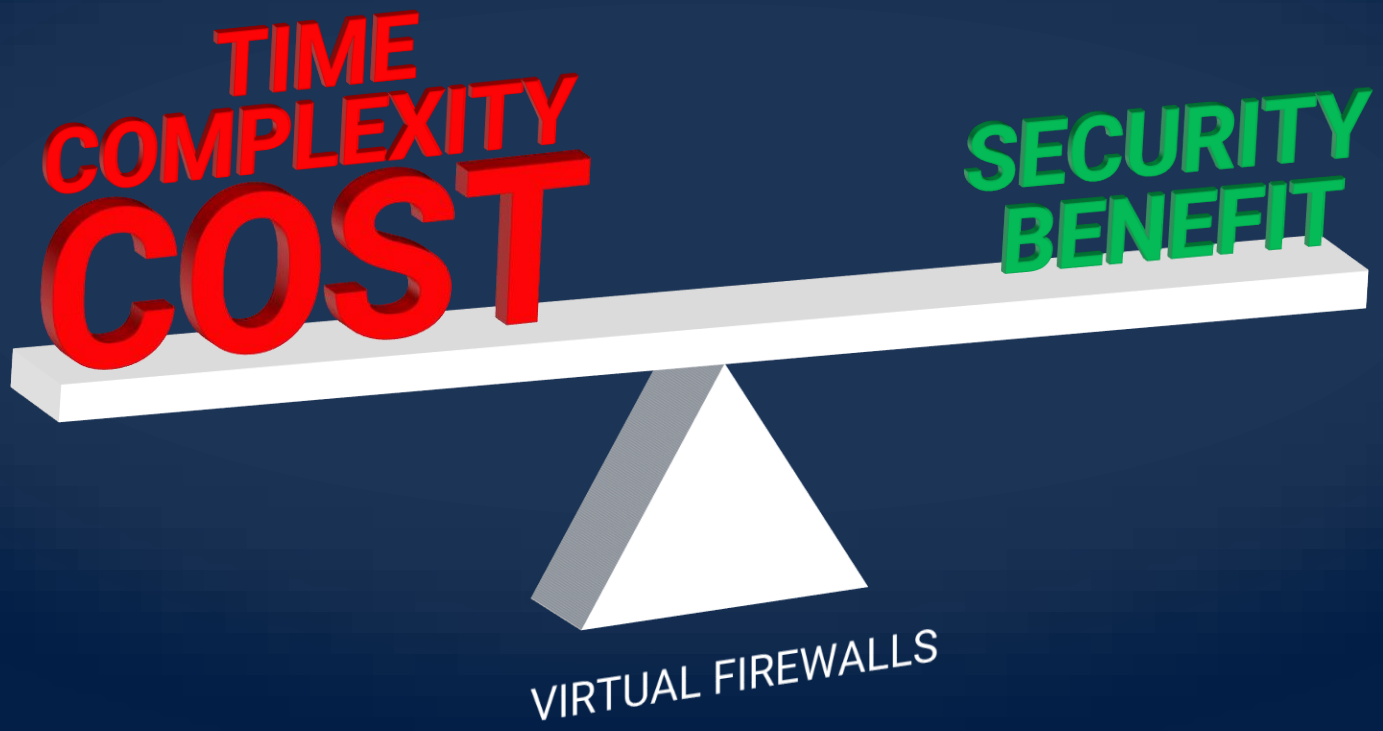


Experts Recommend Improve Segmentation And Use Zero Trust

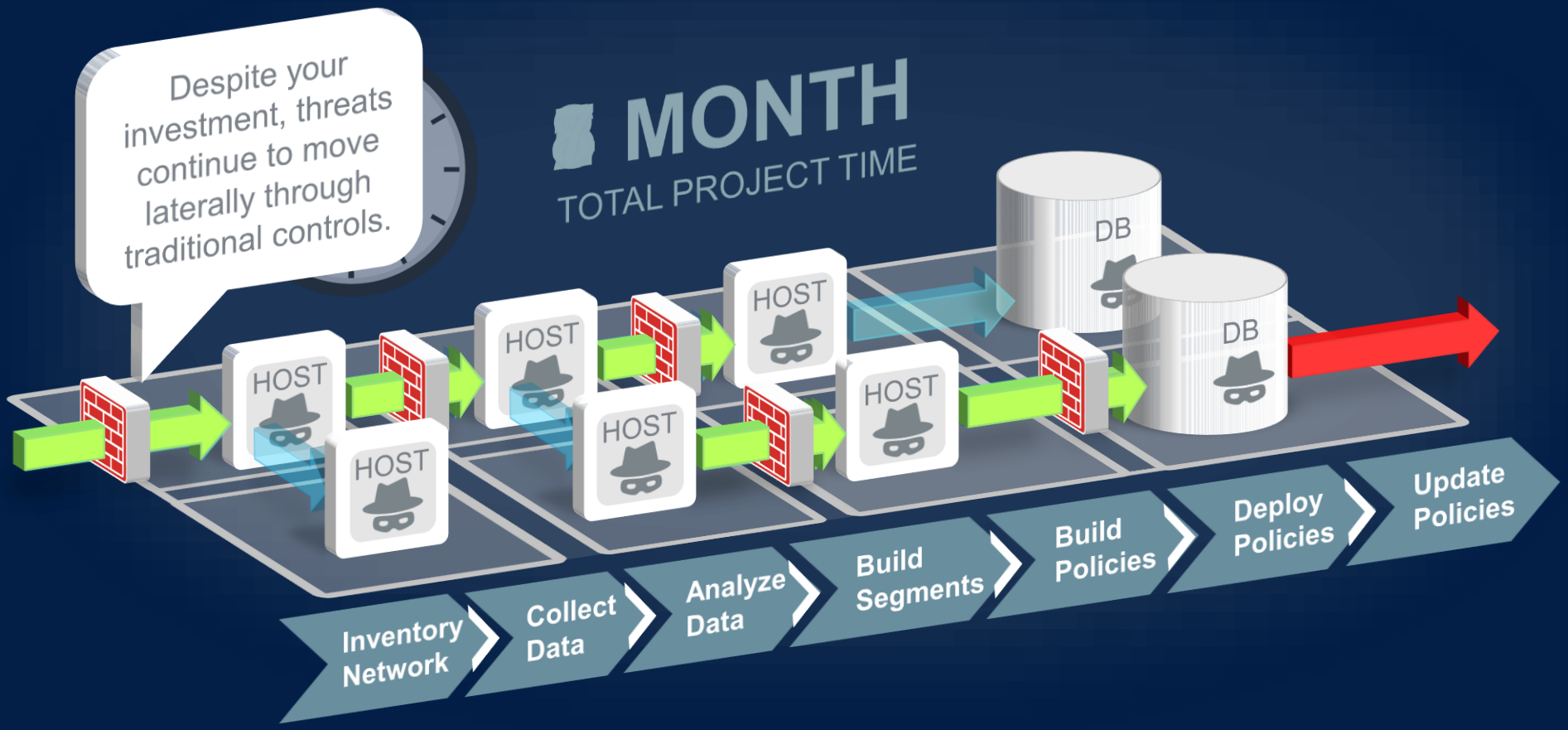
THREAT	IMPACT	EXPERTS RECOMMEND
Nation State (Gov. agency)	21.5M PII records	"Zero trust model" US-HCOGR
APT (Financial services)	146M PII records	"Enhance network segmentation"
Ransomware (Logistics co.)	$300M, 29k systems	"... least privilege" US CERT
Insider Threat (Healthcare co.)	18K PHI records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

Gartner: "Identity-based segmentation" is a core protection strategy for cloud workloads.

Shrinking Segments Is Complex and Time Consuming

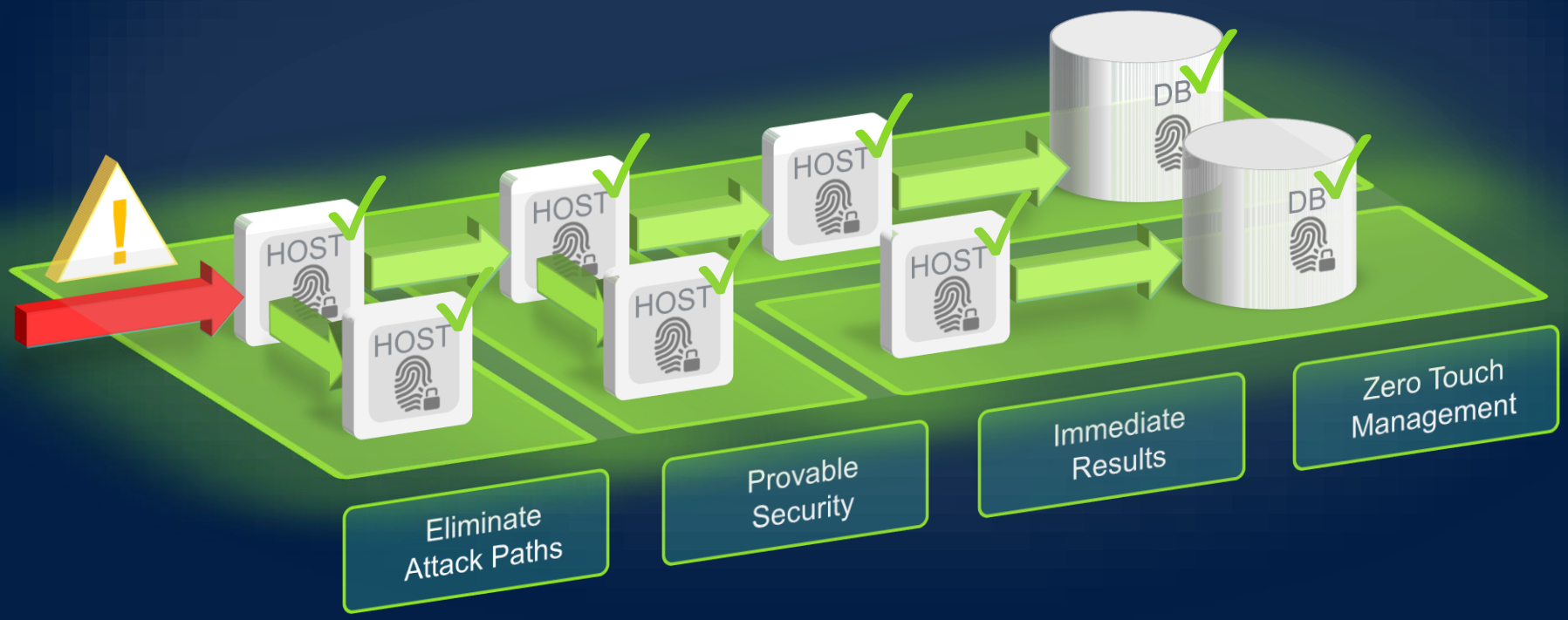


Shrinking Segments Is Complex and Time Consuming



Automating Segmentation Using Zero Trust

Impossibly simple microsegmentation with Zero Trust security

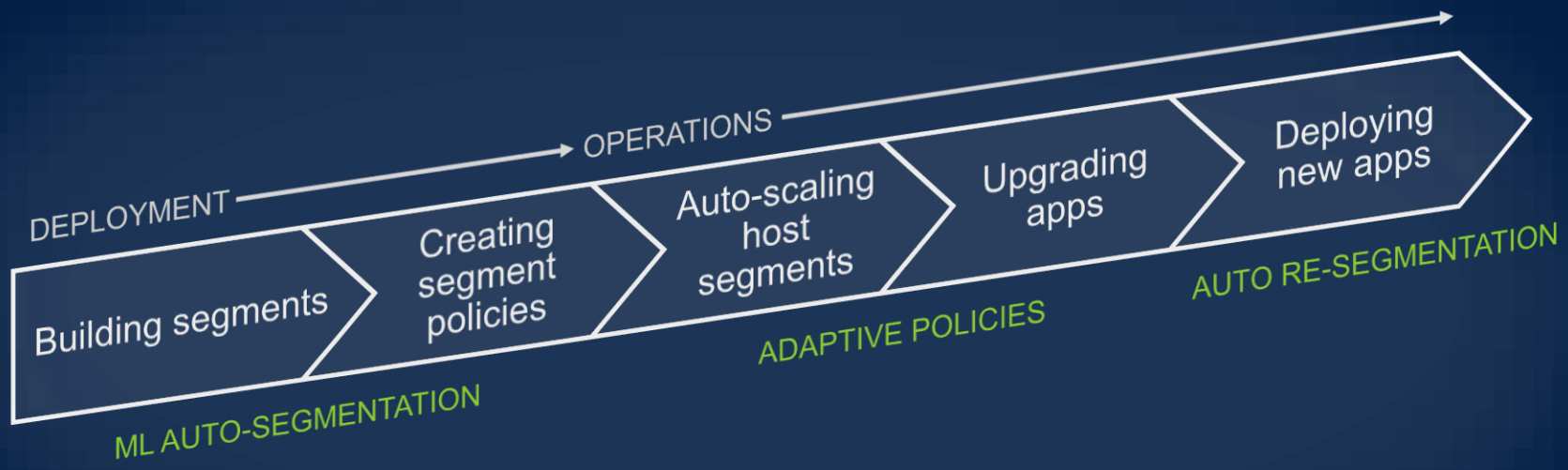


Automating Segmentation Using Zero Trust

Impossibly simple microsegmentation with Zero Trust security

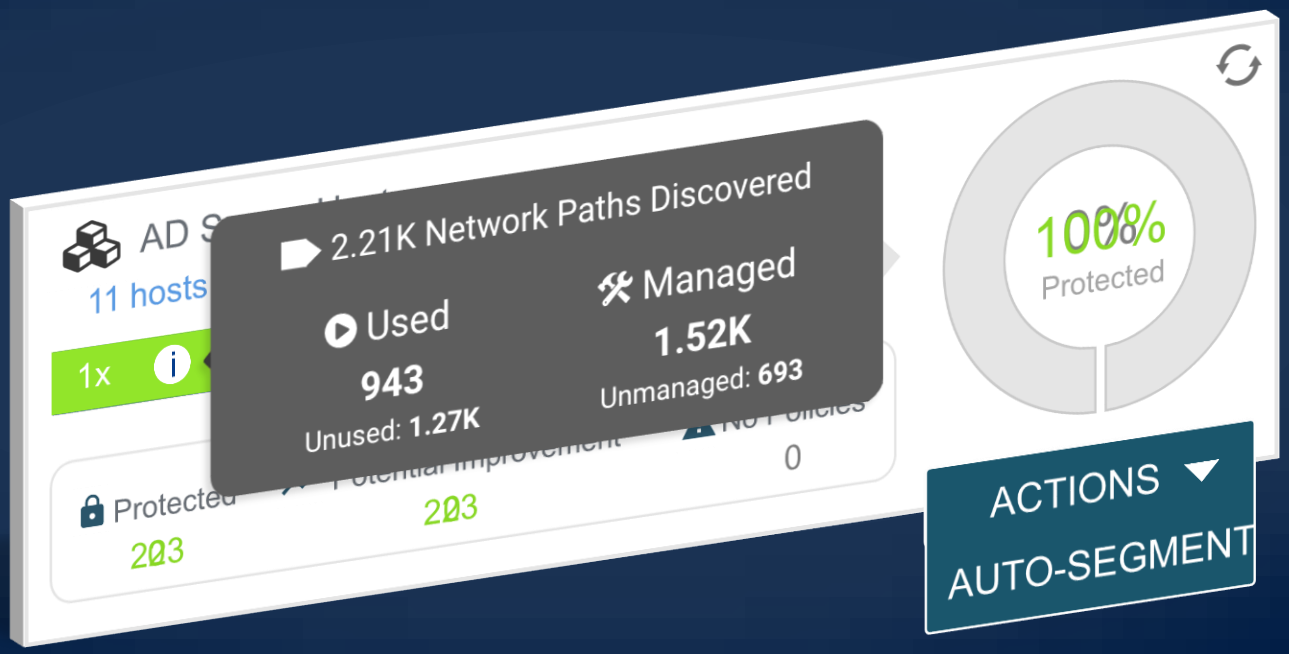
Fully Automated Microsegmentation

All policy management tasks automated to radically simplify operations



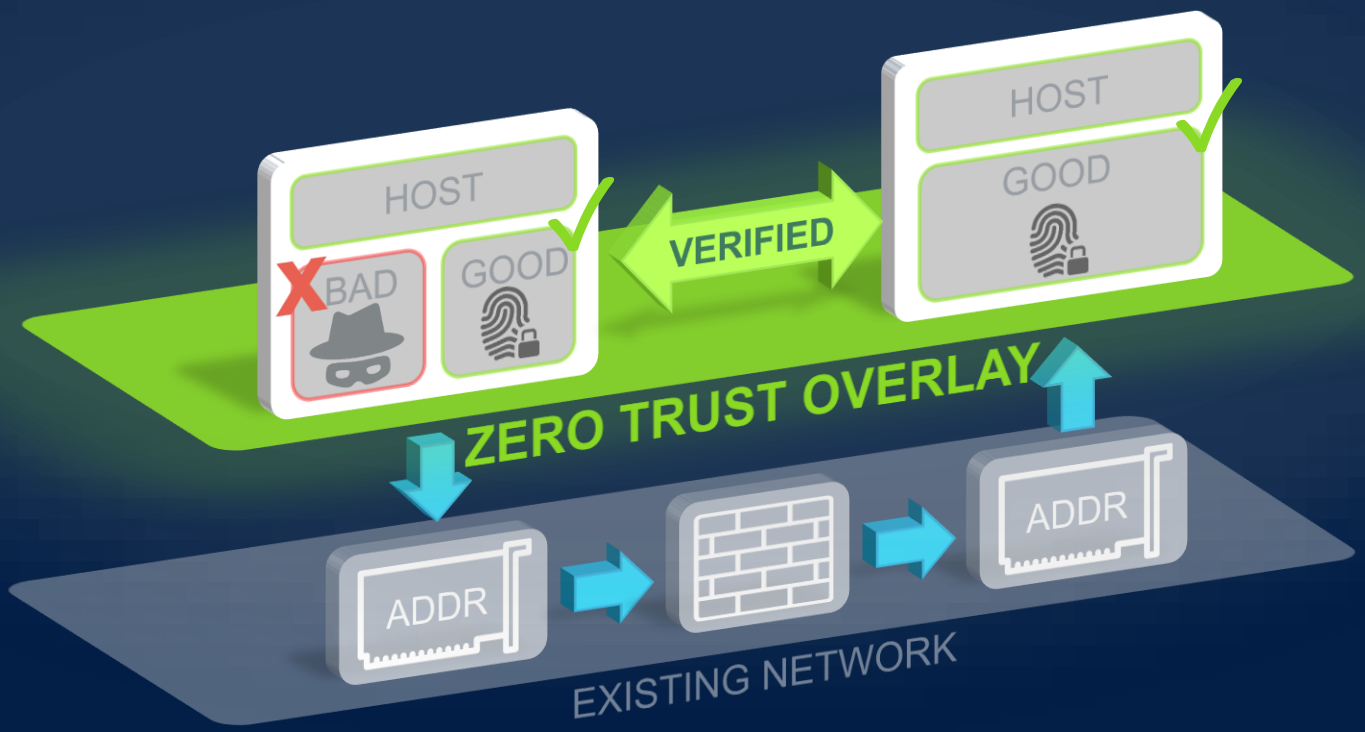
1-Click Simplicity ➔ Provable Outcomes

Measurable return on your security investment



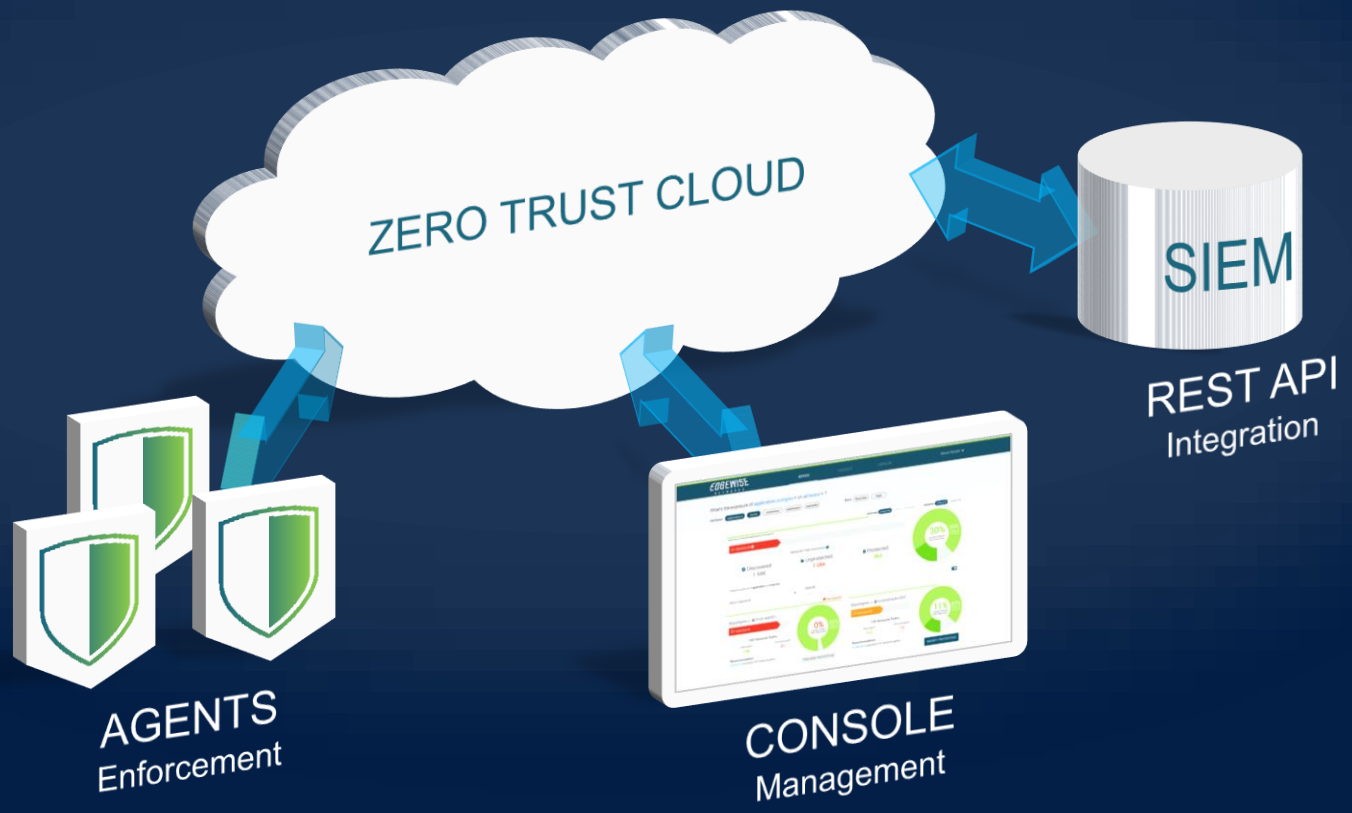
Don’t Change Your Network, Change Your Security

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



Microsegmentation as a Service

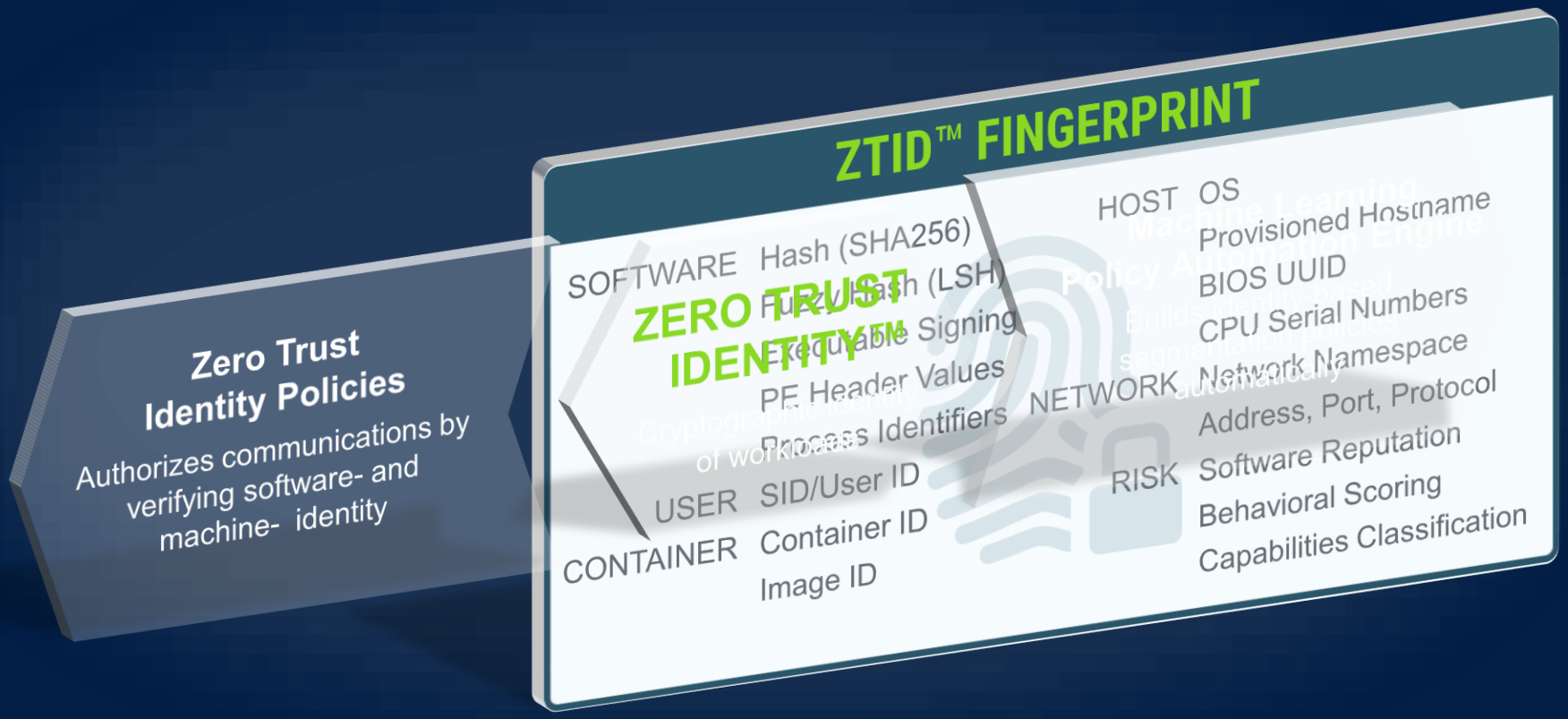
Simple Deployment. Secure Delivery. Scalable Protection. Cloud Delivered



Zero Trust Identity

Zero Trust Identity

Patented technology driving Zero Trust Auto-Segmentation



Zero Trust Identity Verification

Delivers the [illegible] usted 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…

VERIFIED

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

SHRINK TIME TO VALUE
- Models applications
- Analyzes attack paths
- Classifies path risk

DRIVE IT EFFICIENCY
- Builds application segments
- Builds identity-based policies
- Optimizes policies

GAP-FREE PROTECTION
- Single-click segmentation
- Only verified apps communicate
- Adapts to change

72 hrs Initial Learning Time	**99%** Policy Confidence	**99.9%** Policy Coverage	**25x** Policy Compression

The Machine Learning Advantage

FIREWALL	EDGEWISE			
15B	**1.7M**	**267K**	**40K**	**100's**
NET EVENTS	NET EVENTS UNIQUE	APP EVENTS	APP EVENTS ML REDUCED	POLICIES ML CREATED

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

aws PUBLIC SECTOR SUMMIT

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.

AWS

- Facilities
- Physical security
- Compute infrastructure
- Storage infrastructure
- Network infrastructure
- Virtualisation layer (EC2)
- Hardened service endpoints
- Rich IAM capabilities

+

- Network configuration
- Security groups
- OS firewalls
- Operating systems
- Application security
- Proper service configuration
- AuthN & account management
- Authorisation policies

=

More secure and compliant systems than any single entity could normally achieve on its own

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

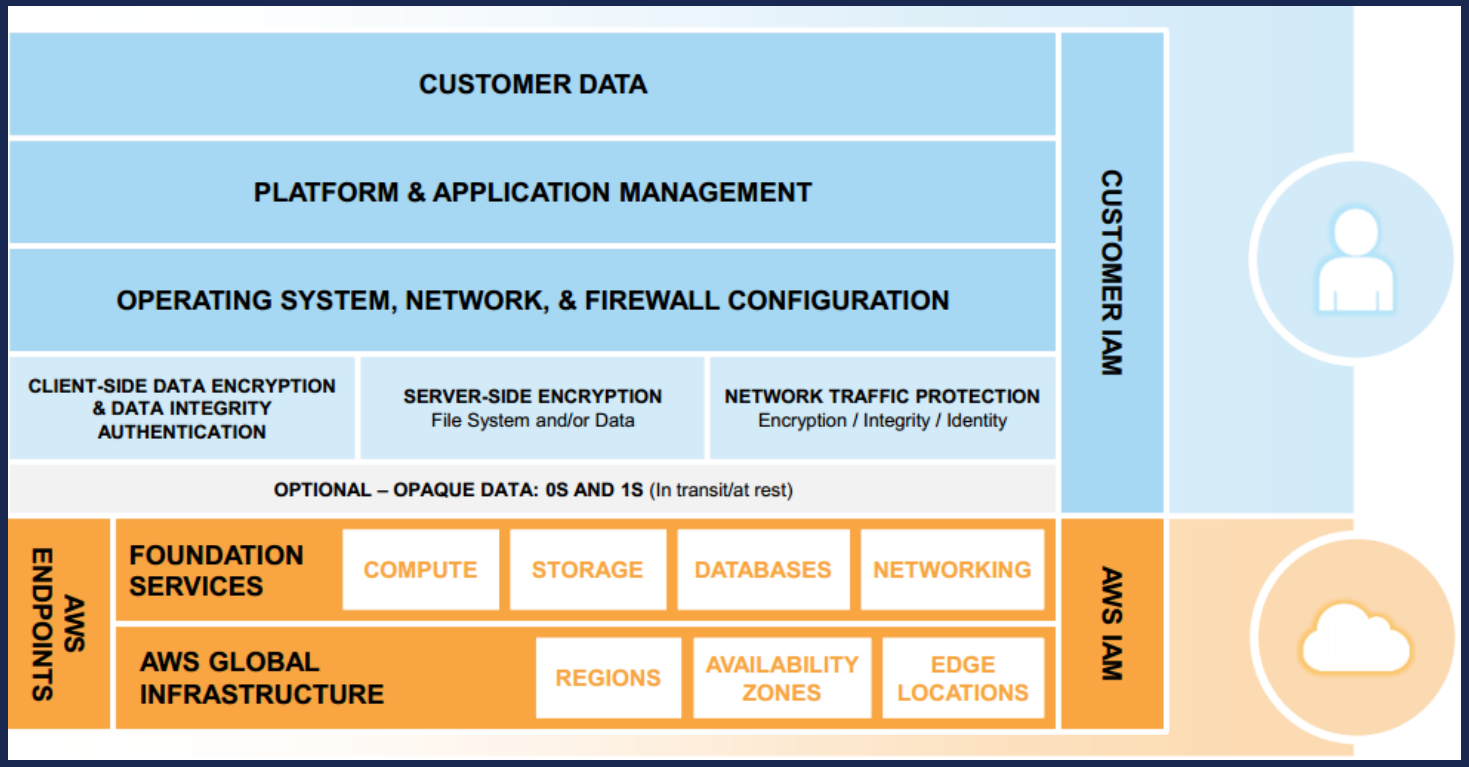
- Will one model work for all services?

Infrastructure Services

Container Services

Abstract Services

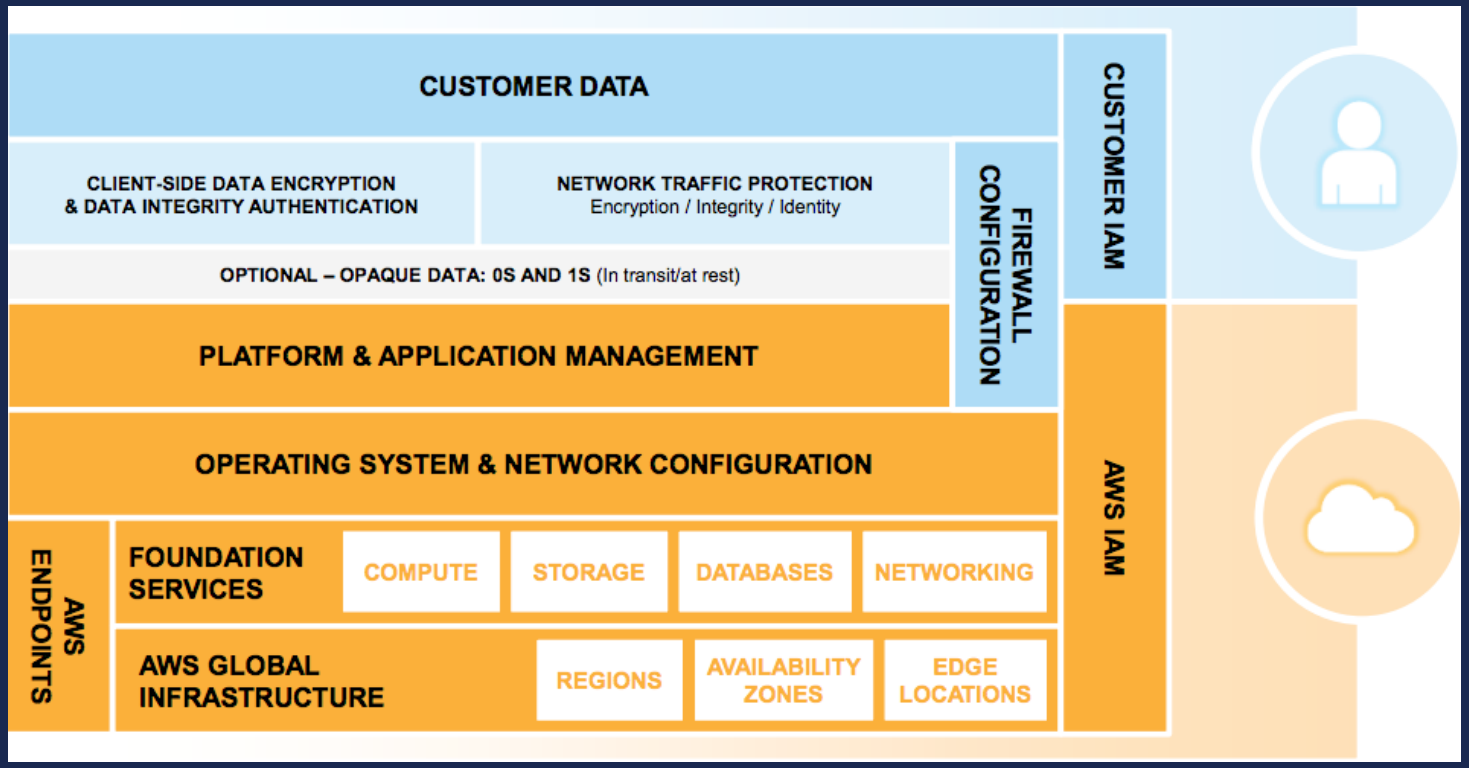
Shared Responsibility Model - Infrastructure



Managed by AWS Customers

Managed by Amazon Web Services

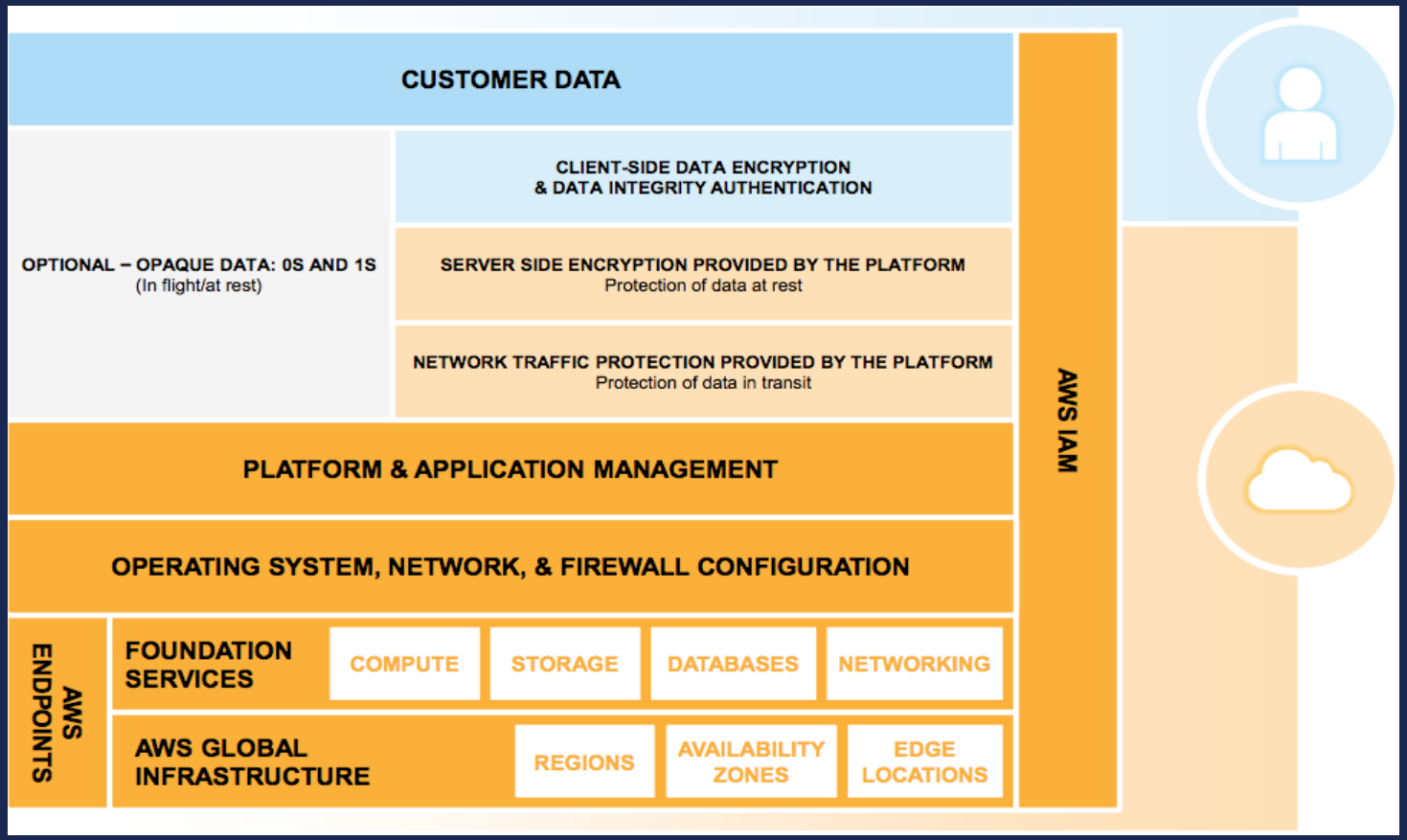
Shared Responsibility – Container Services



Managed by AWS Customers

Managed by Amazon Web Services

Shared Responsibility – Abstracted Services



Managed by AWS Customers

Managed by Amazon Web Services

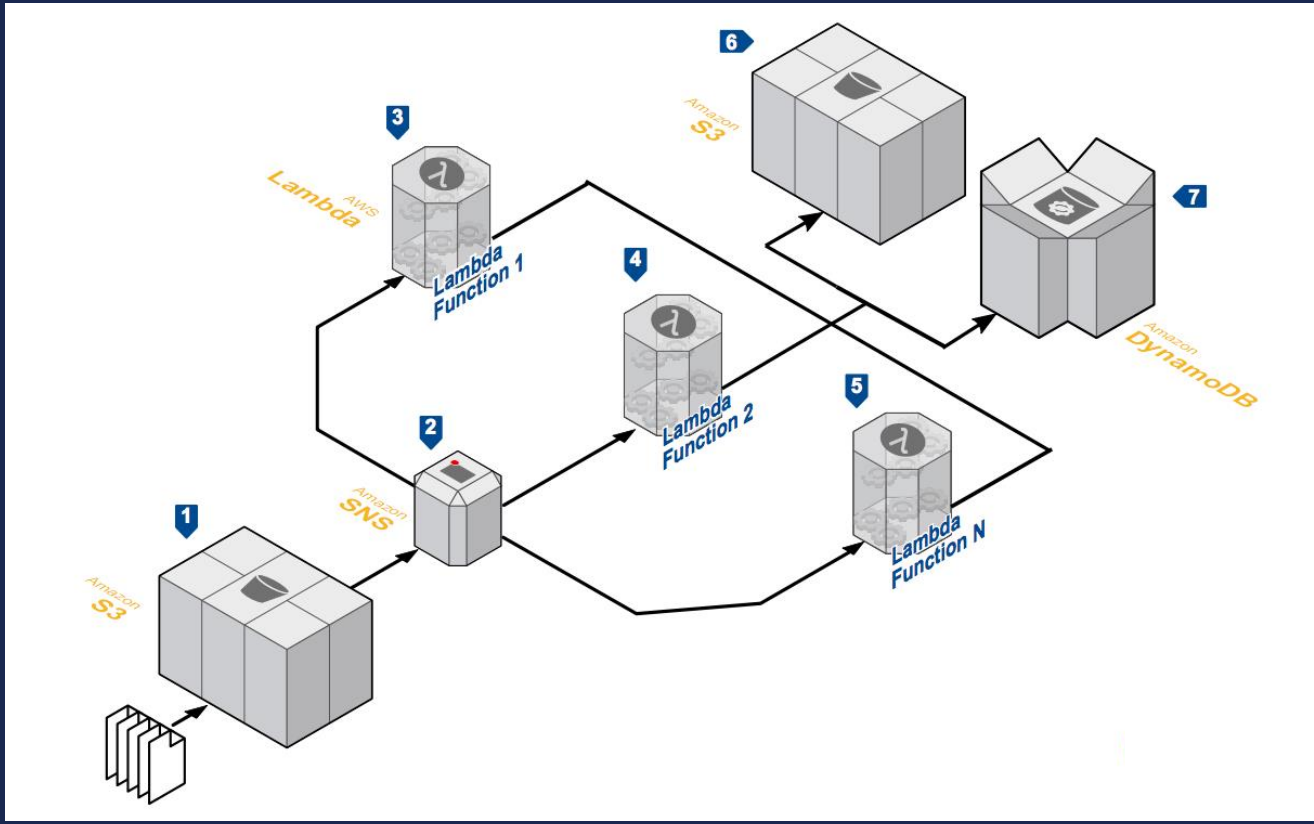
Benefiting from Abstracted Services:

Serverless Architectures

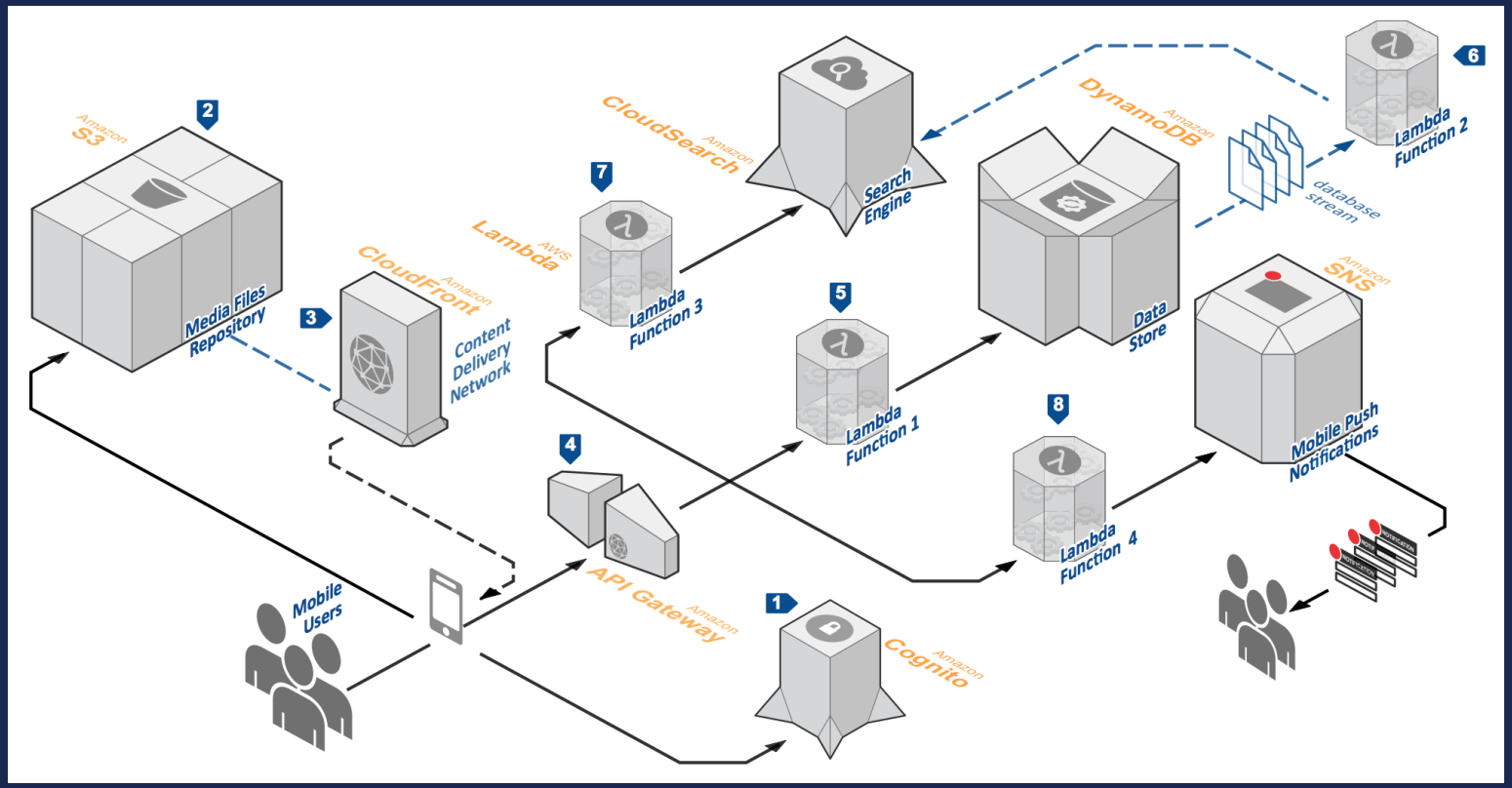
Benefits of Serverless Architectures

- 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

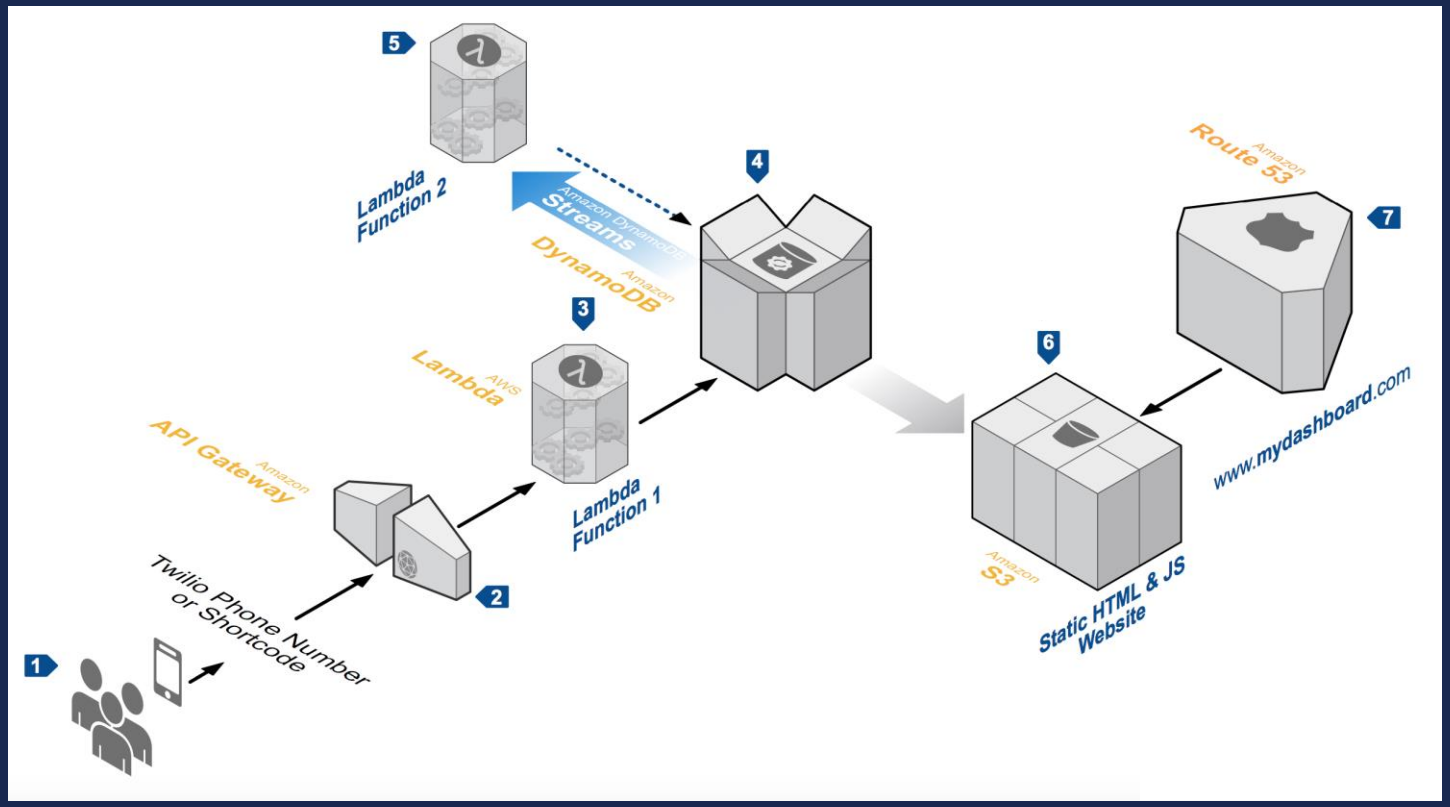
Real-time File Processing



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 a**ttestations** can be used by customers when undertaking risk assessments or using **frameworks**

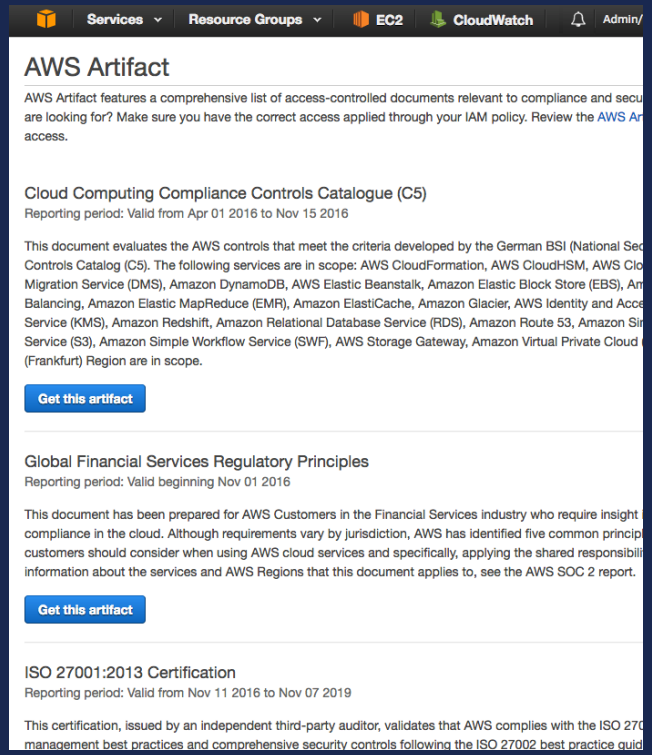
Security OF the Cloud

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



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 (172.16.0.0, 172.16.1.0, 172.16.2.0)
- 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)**
  - Private and Public subnets
  - Security Group and NACLs
  - VPC Flow Logs for network monitoring and analysis

Multi-dimensional defense-in-depth

- **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**
  - Configuration history and Security rules enforcement
  - Extensive set of built-in rules and you can create your own (security as code)

Controlled, monitored, and managed change – in an Agile context

- **CloudFormation**
  - Configuration management, with a unique source of truth

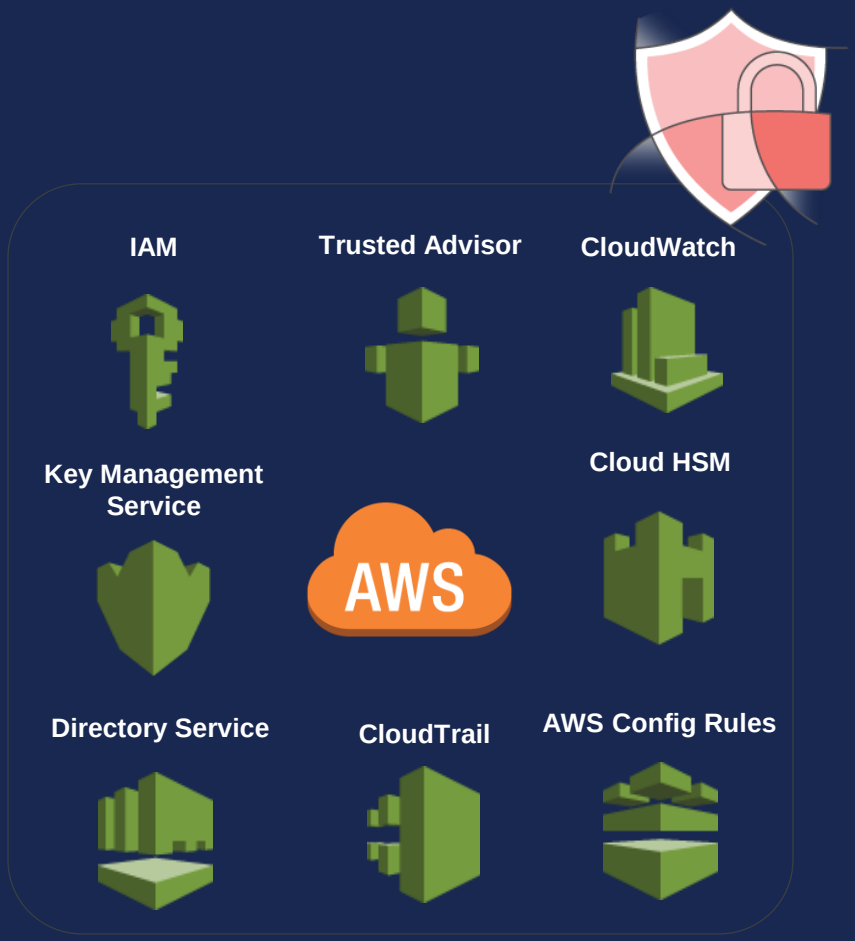
- **AWS Inspector and AWS Trusted Advisor**
  - Best practices and vulnerability management
- **AWS CloudWatch Events**
  - Respond quickly to notifications from AWS resources delivered in near-real-time

Security by Design

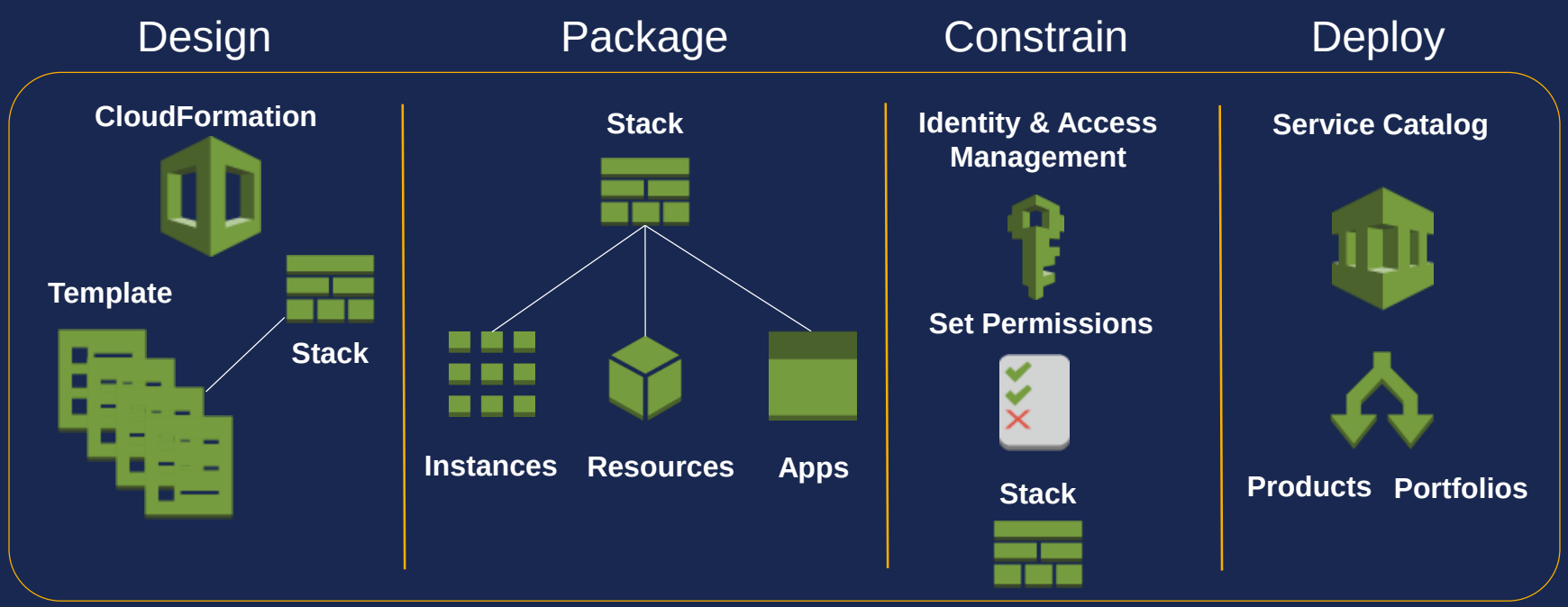
Security by Design (SbD) is a security assurance approach that formalises AWS account design, automates security controls, and streamlines auditing.

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

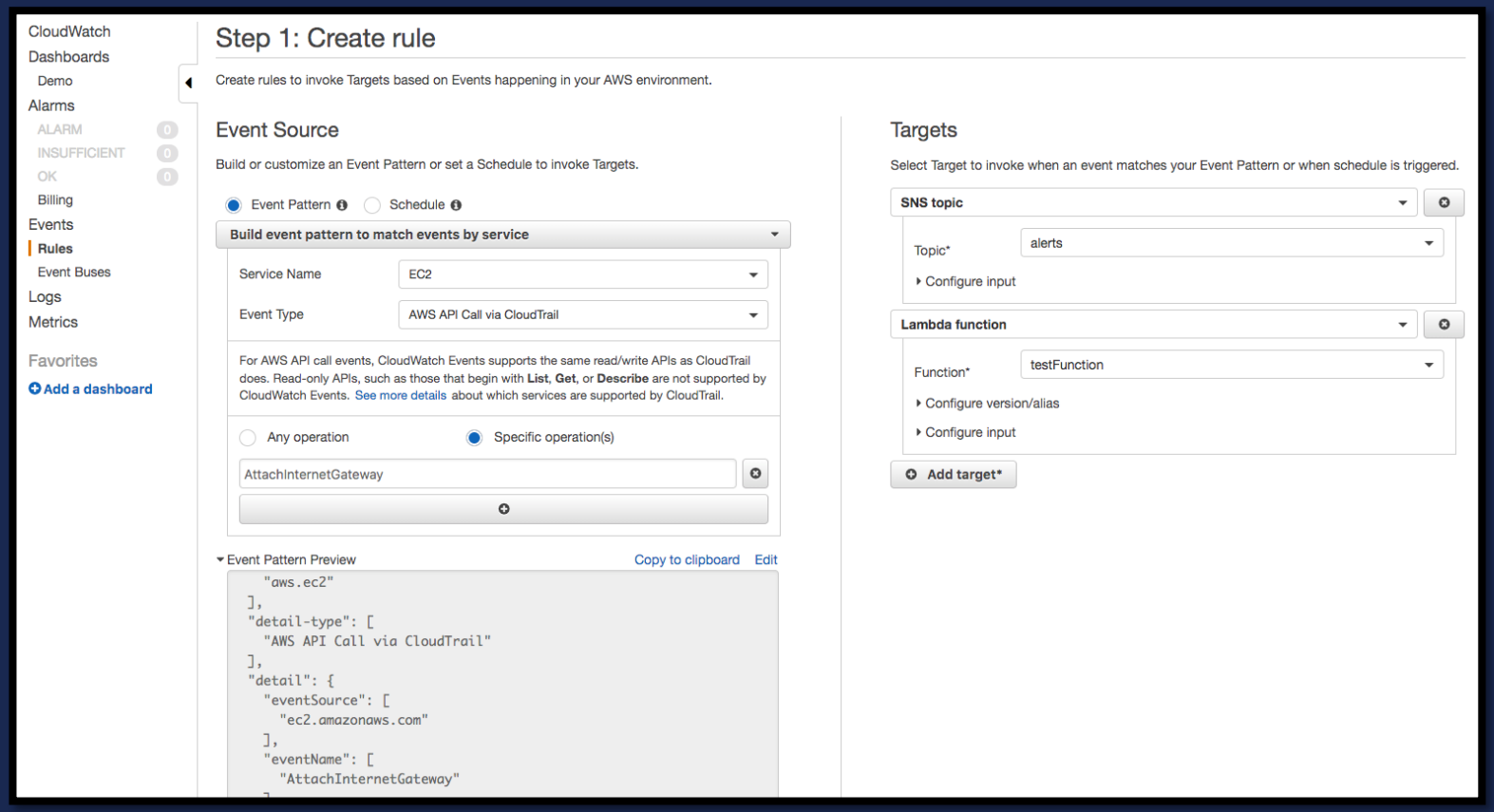
Amazon CloudWatch event bus

- 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



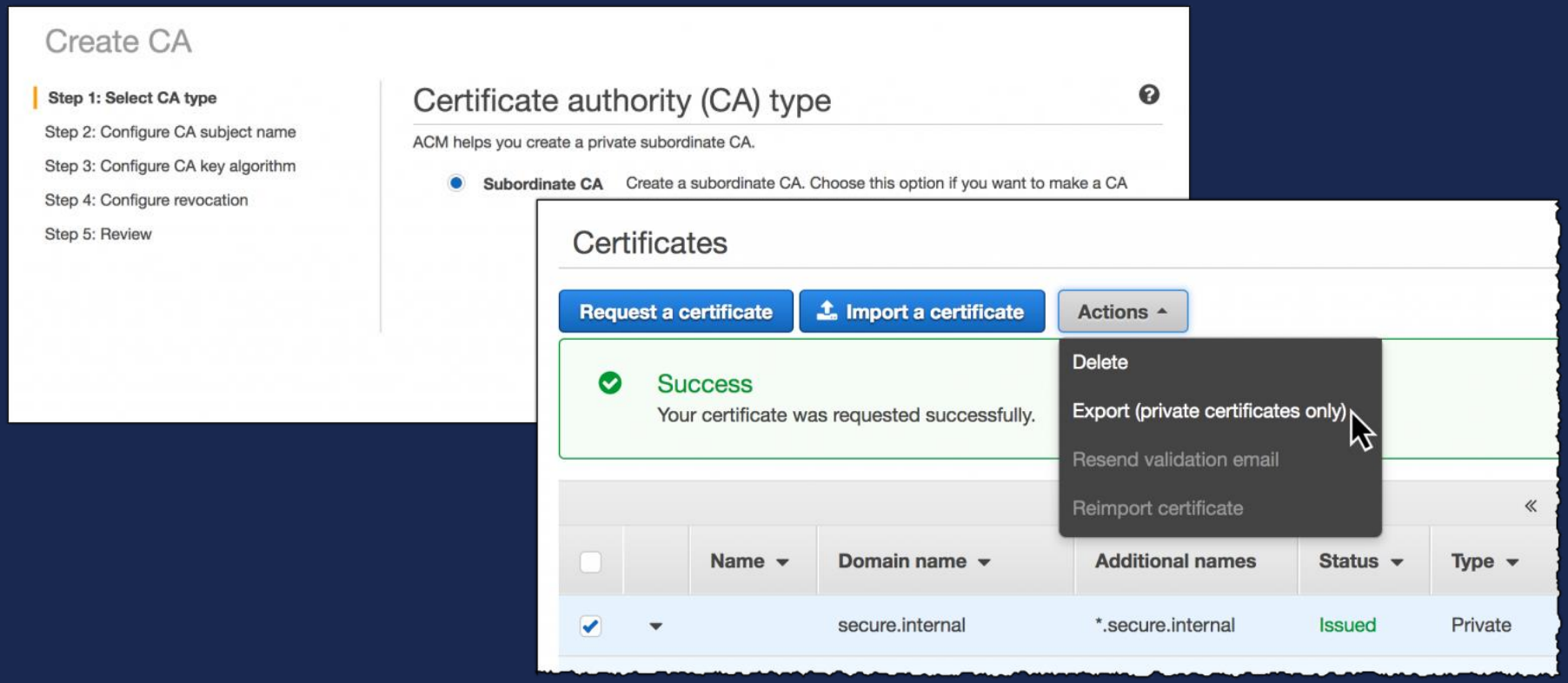
Where to start?

So many services… where do I start?

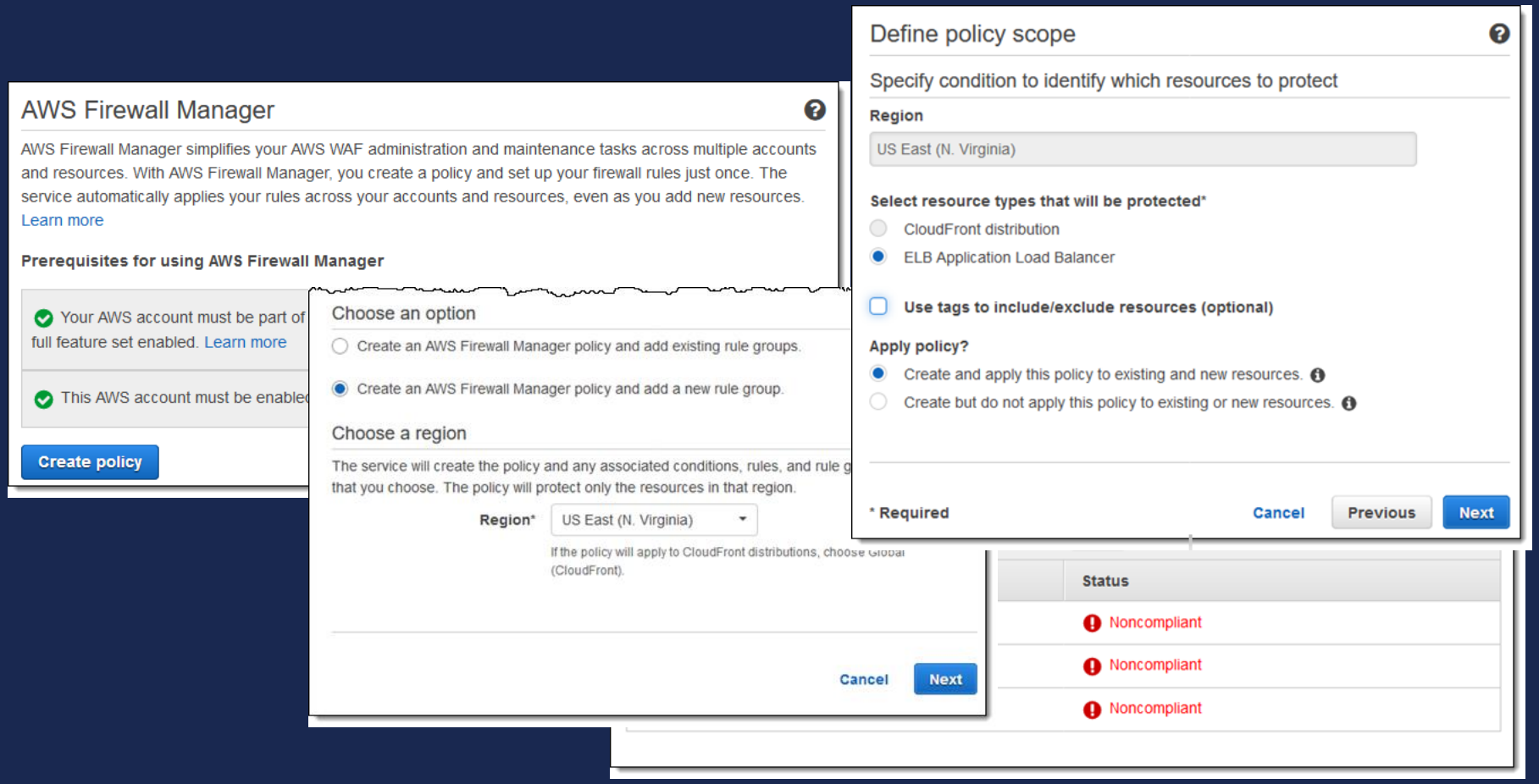
- AWS provides:
  - Continuous innovation of products and services
  - AWS Quick Starts
  - AWS Answers
  - AWS blogs
  - Comprehensive documentation
  - Extensive partner network

Continuous Innovation

AWS Certificate Manager – Private CA



AWS Firewall Manager



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: ranman

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 (C

DefaultEncryptionKey

Add new key

Select which RDS database this secret will access Info

	DB instance	DB Engine	Status	Creation date
◉	twitterapp2	aurora	available	04/02/2018
○	twitterapp2-us-east-1a	aurora	available	04/02/2018

Cancel | Next

Step 1 Secret type
Step 2 **Name and description**
Step 3 Configure rotation
Step 4 Review

AWS Secrets Manager > Secrets > Store a new secret

Store a new secret

Secret name and description Info

Secret name

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

prod/TwitterApp/Database

Secret name can contain alphanumberic characters and the characters /_+=,.@-

Description - *optional*

Connection string info for production twitterapp db

Maximum 250 characters

Cancel | Previous | Next

Step 1 Secret type
Step 2 Name and description
Step 3 **Configure rotation**

AWS Secrets Manager > Secrets > Store a new secret

Store a new secret

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 | 10 | days

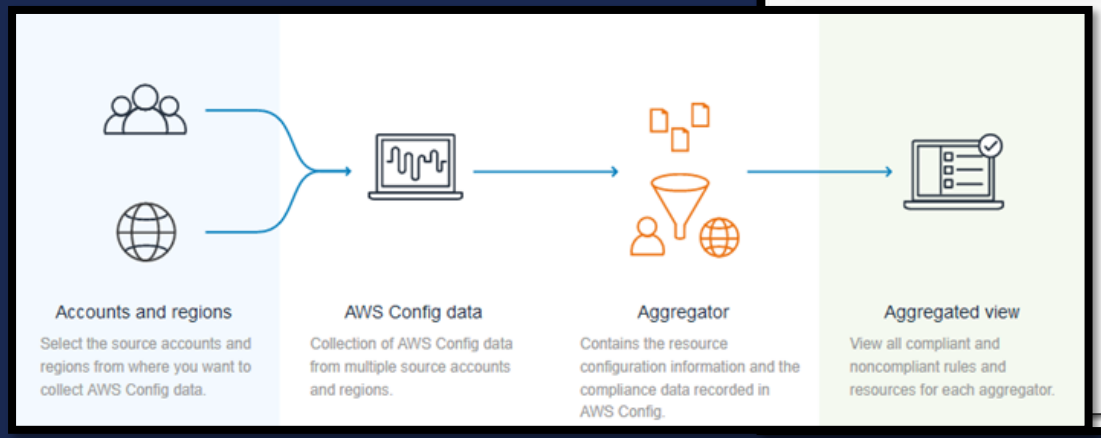
Maximum 365 days

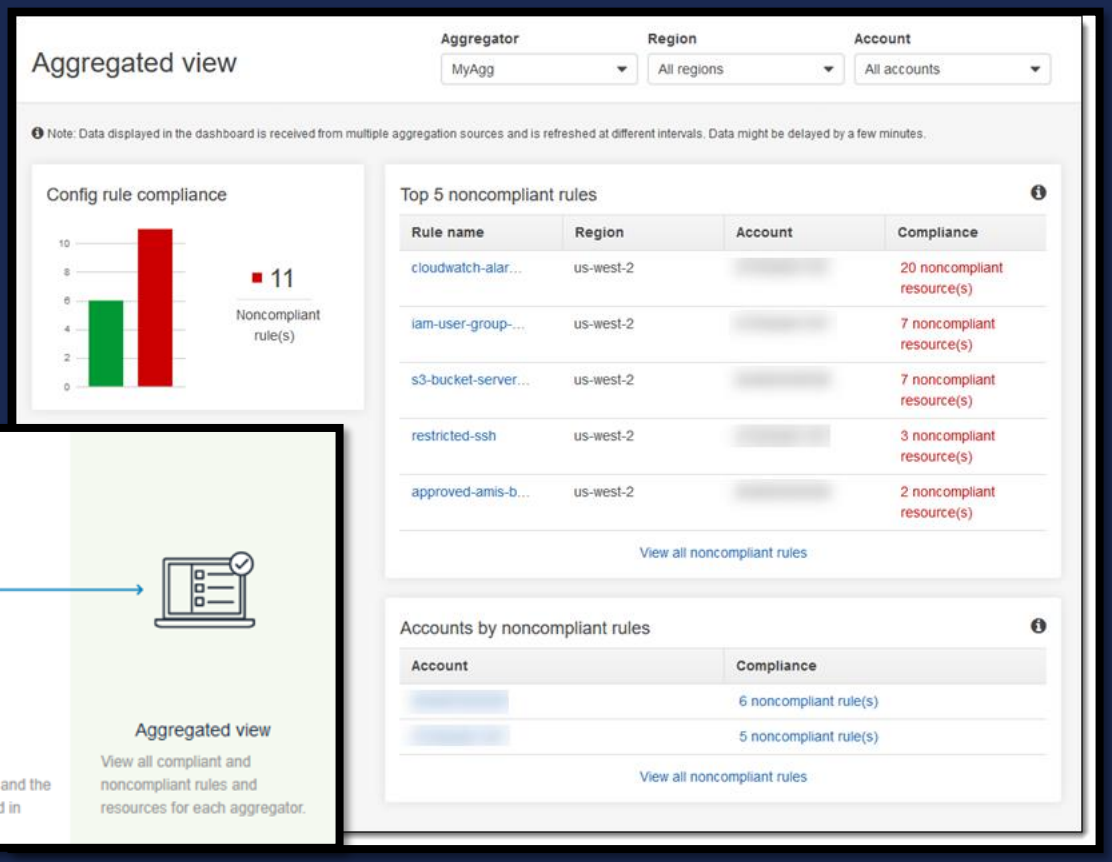
Select which secret will be used to perform the rotation Info

- ◉ 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.

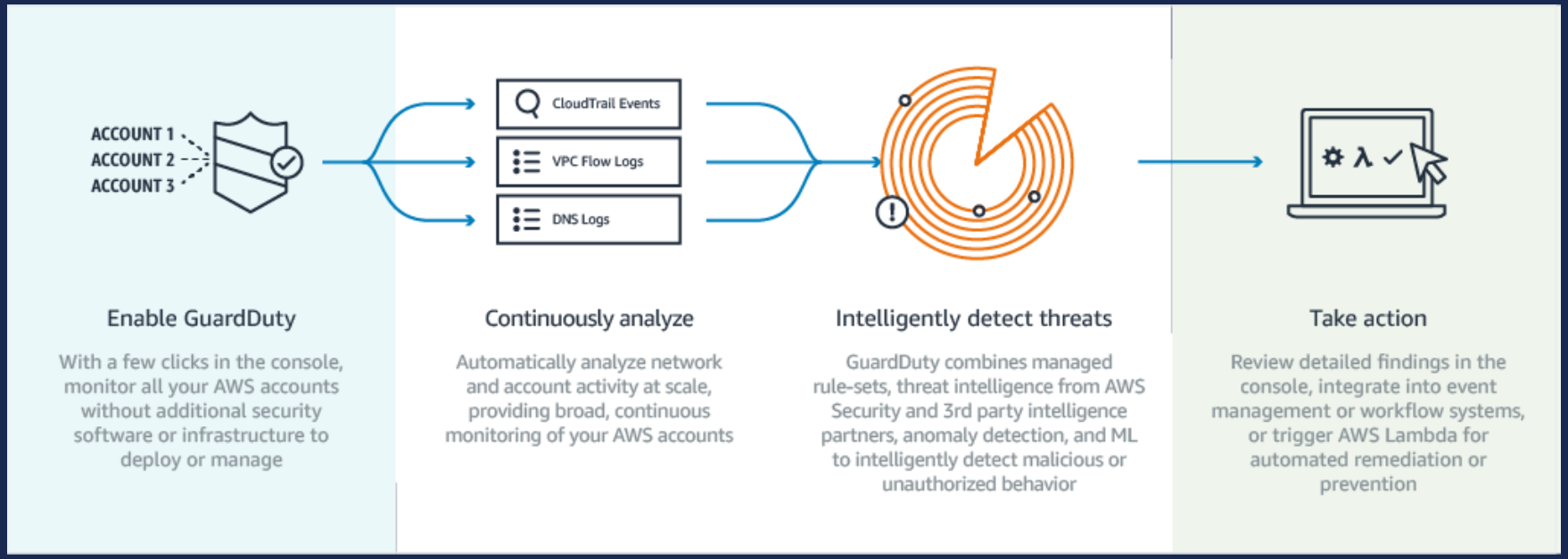
Cancel | Previous | Next

AWS Config Rules aggregation





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

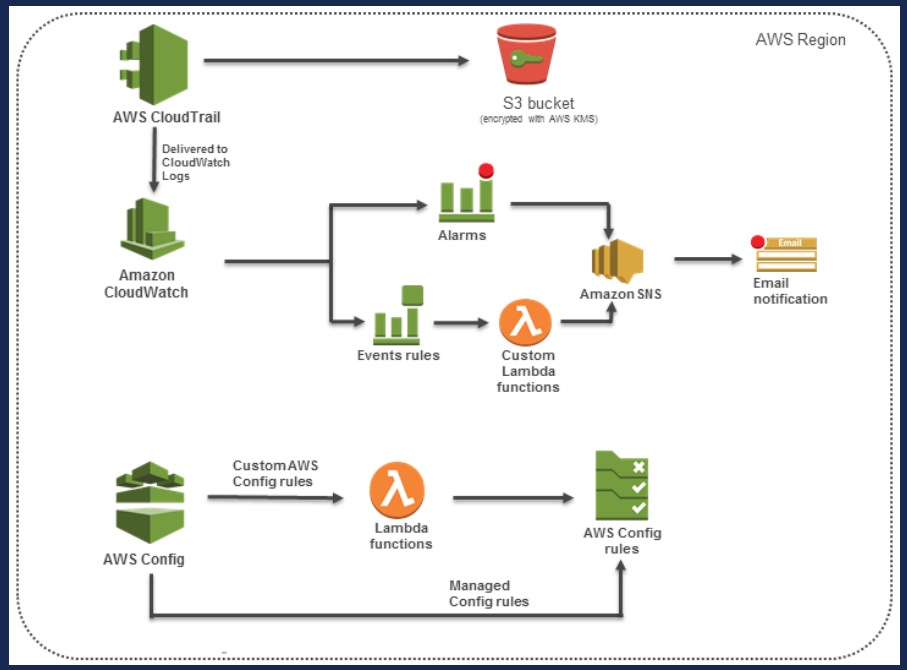
Symantec Protection Engine
Content scanning, malware and threat detection
Learn more | View guide

Security and analytics with Palo Alto Networks and Splunk
Palo Alto Networks VM-Series firewall and Splunk Enterprise on AWS
Learn more | View guide

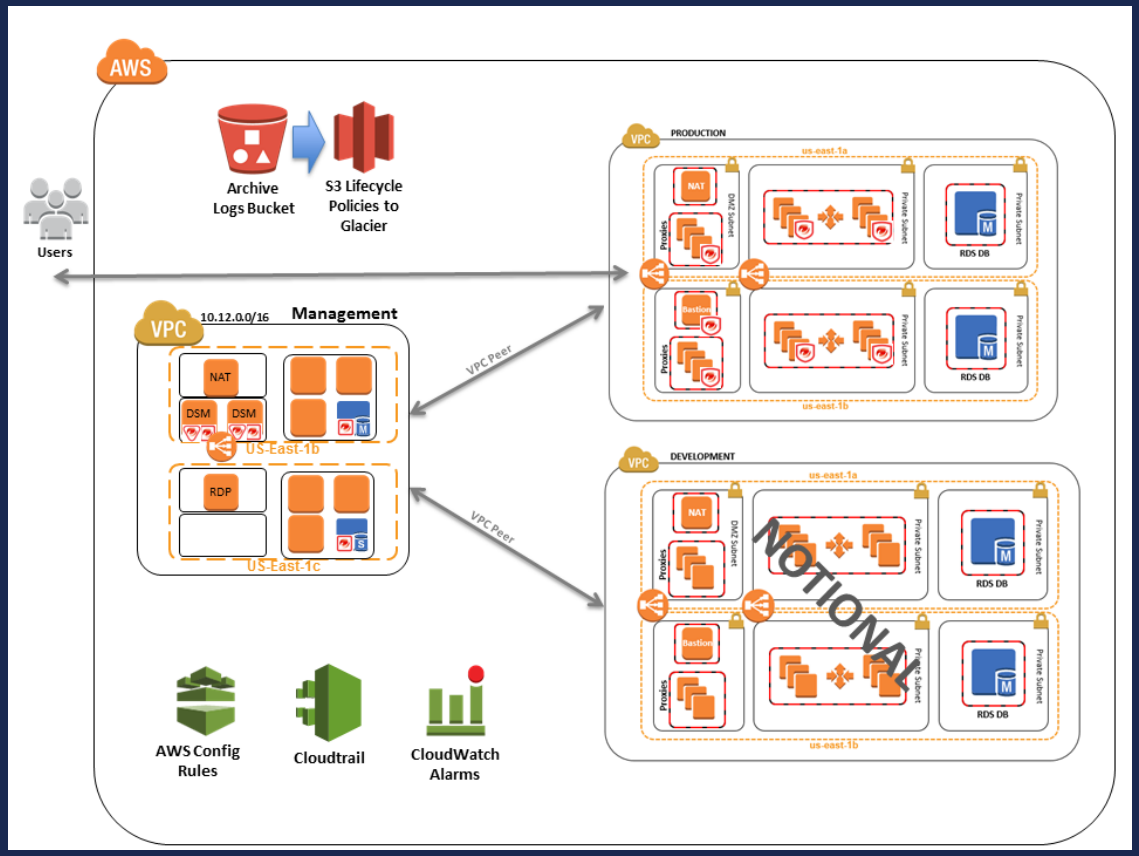
CIS Benchmark on AWS

- 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

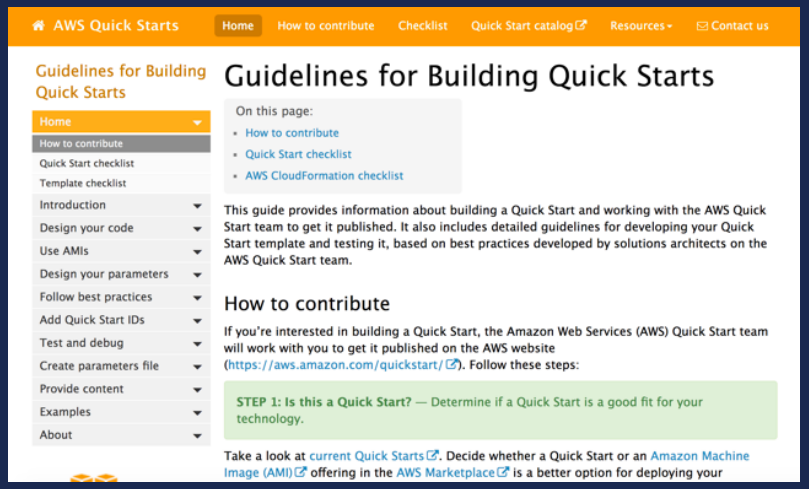


NIST High-Impact on AWS



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



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

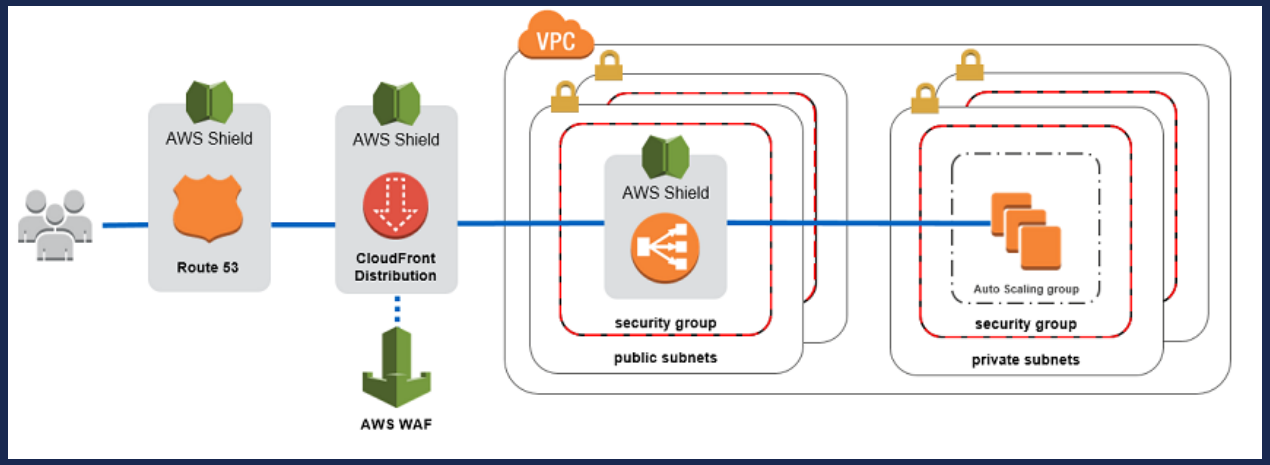
- **https://aws.amazon.com/answers/**

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?

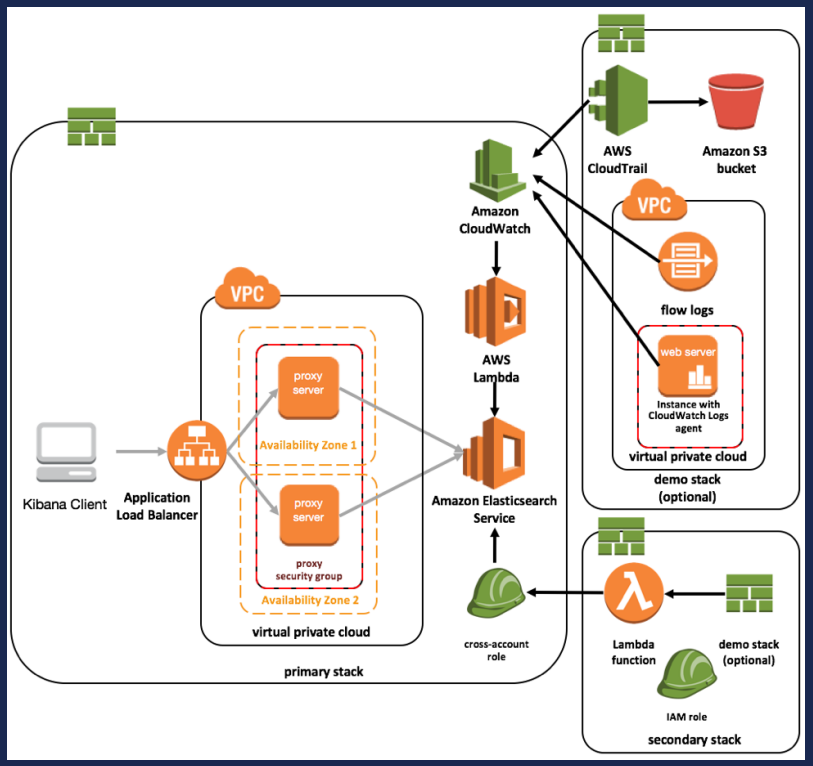
Protecting web applications from DDoS attacks

- 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



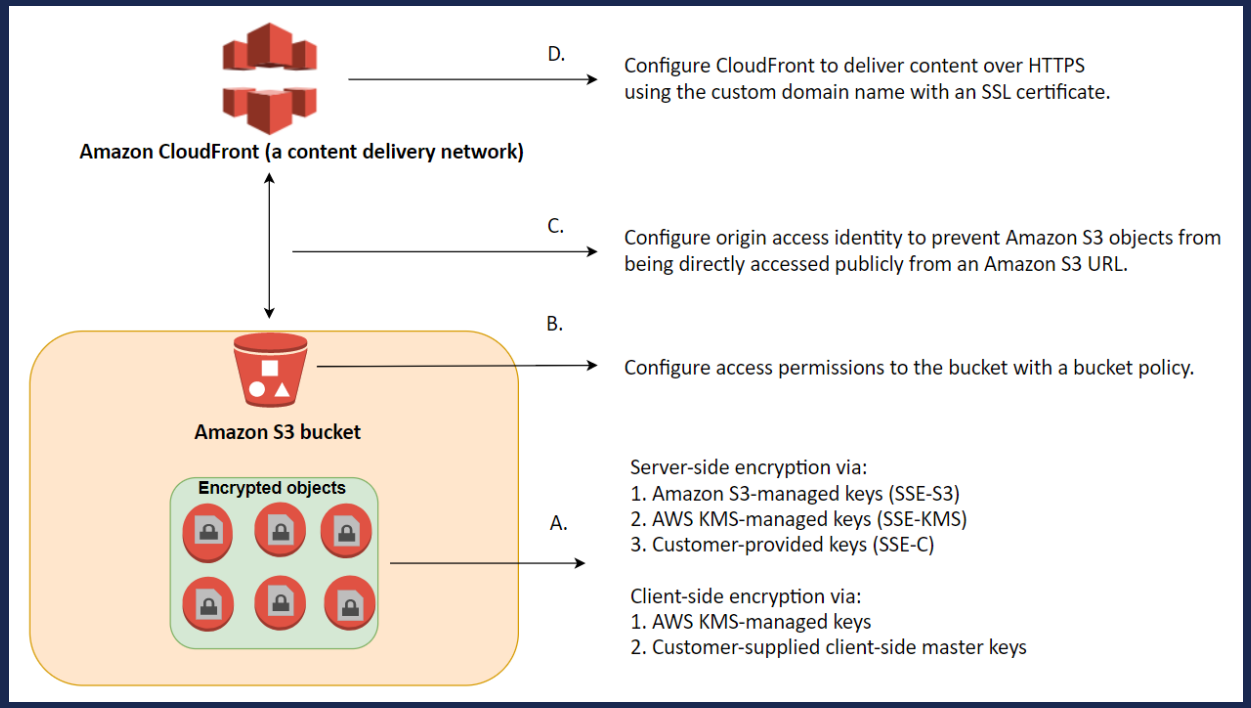
AWS Blogs

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



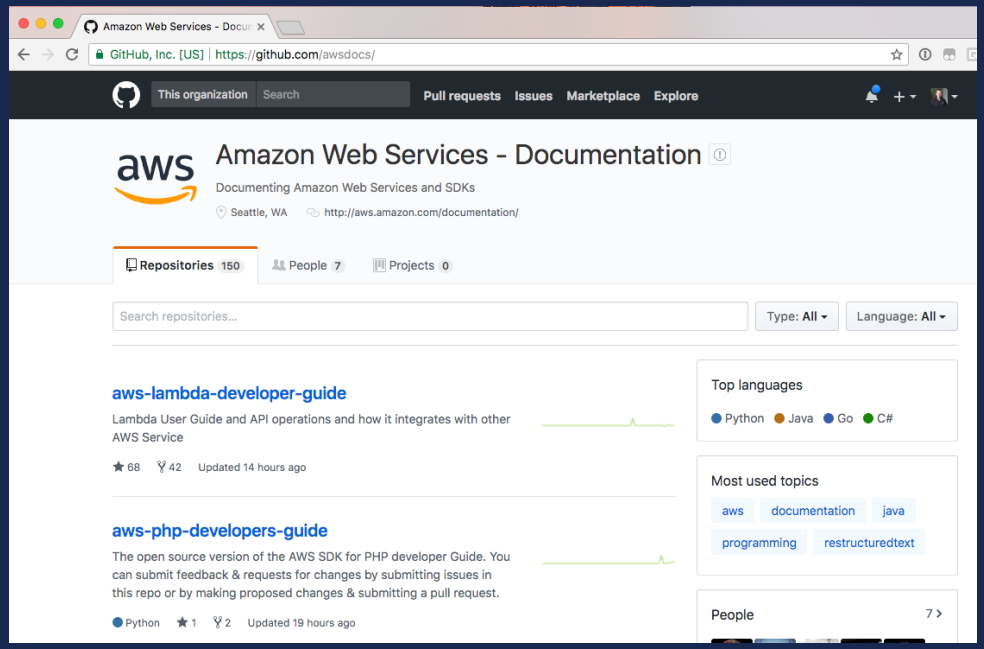
https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-your-amazon-s3-data/

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
cisco	ALERTLOGIC	okta	QUALYSGUARD	gemalto
f5	splunk>	CIPHERGRAPH networks	TREND MICRO	Vormetric
CITRIX	sumologic	Elastic SSO	tenable network security	HYTRUST
SOPHOS	CloudPassage	conjur	RAPID7	KeyNexus
Barracuda	loggly	onelogin	evident.io	Townsend SECURITY
FORTINET				druva
intel Security				
paloalto networks				
Check Point We Secure the Internet				
IMPERVA				

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/

aws PUBLIC SECTOR SUMMIT

Thank you!

Upcoming events

Virginia Information Technologies Agency

Cybersecurity Awareness Month: Oct. 2020

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

Virginia Information Technologies Agency

COVITS 2020

government technology

VIRTUAL

COVITS

September 9-10, 2020

Virginia Information Technologies Agency

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

Picture courtesy of www.v3.co.uk