



WELCOME TO THE

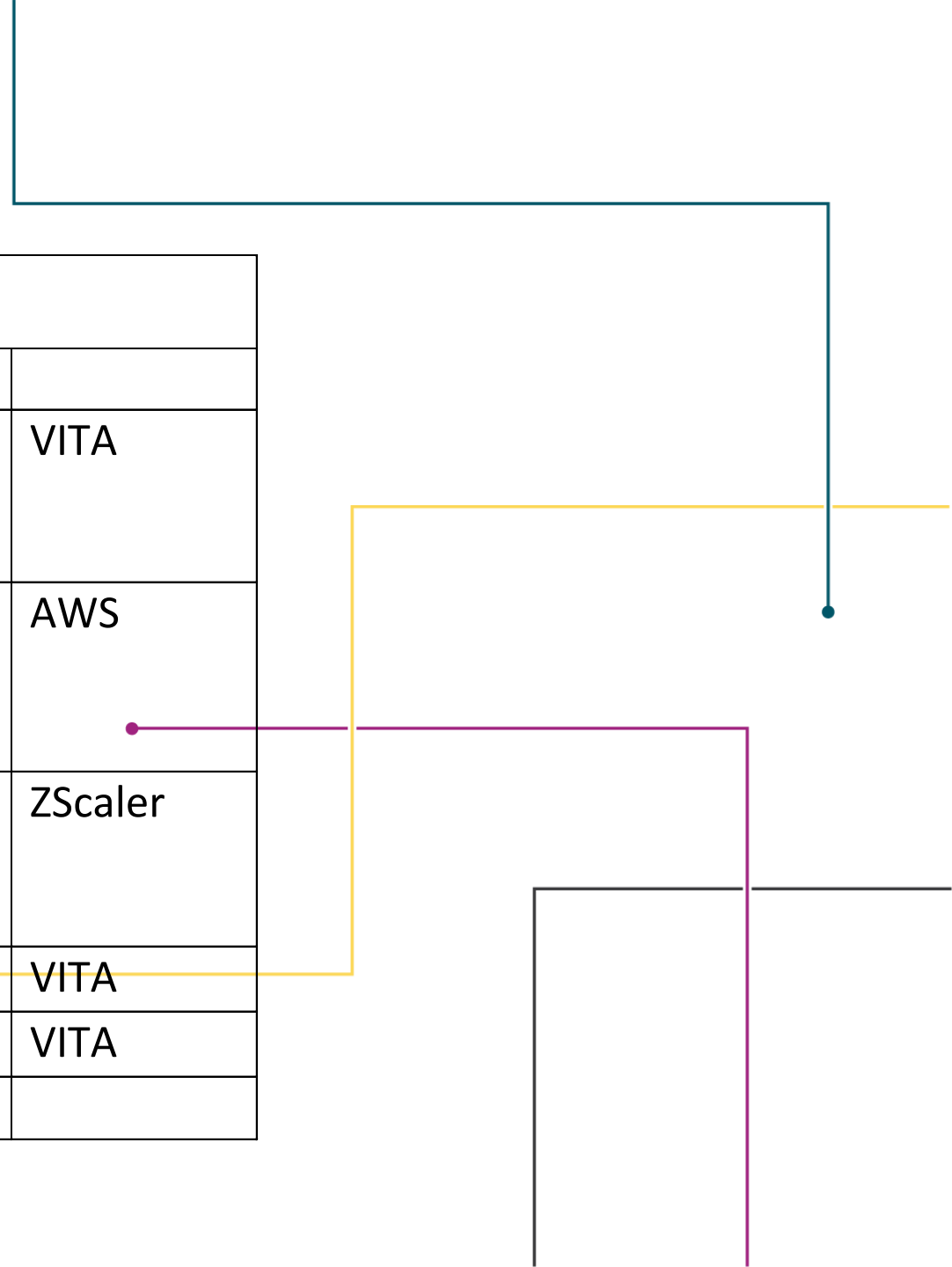
Aug. 3, 2022,

ISOAG MEETING



AGENDA

• Welcome		
• Status of Archive, eDiscovery and Records Management in Microsoft	Amy Judd Compliance Specialist	VITA
• Layering AWS Security Services to automated secure Landing Zones, DR and Incident Response	Milty Brizan Sr. Solutions Architect	AWS
• Proactive Defense Technology to Detect and Protect Environments from Cyber Threats and Ransomware Attacks	Jeff Spencer & Raazi Zain	ZScaler
• 2022 Cybersecurity Awareness Month	Tina Gaines	VITA
• Upcoming Events / Announcements	Ed Miller	VITA
• Adjourn		

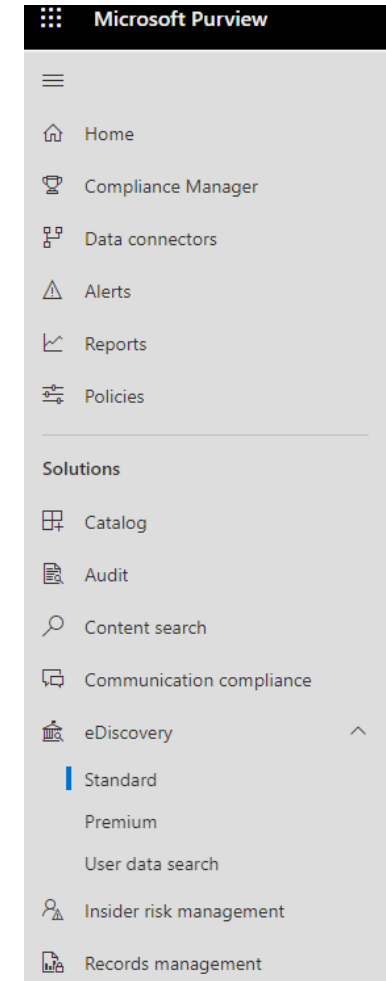


STATUS OF ARCHIVE, EDISCOVERY AND RECORDS MANAGEMENT IN MICROSOFT

- Presented by
- Amy Judd / VITA

PURVIEW

- Interim solution
- Microsoft equivalent of Google Vault
 - Includes Purview eDiscovery (Standard) for G3 licenses
 - Email: captures and maintains all sent/received
 - SharePoint, OneDrive, Teams
- VITA has active procurement for statewide eDiscovery contracts (expected 2022)
 - Five-member evaluation team
 - Reps from VITA, OAG, and three customer agencies
- Investigating potential longer-term Archives and Records Management services
 - Working with NTT and the Library of Virginia (LVA)
 - Vault and Purview do not meet RM best practices for government or LVA rules & guidelines





Layering AWS security services to automate secure Landing Zones, DR and incident response

Milty Brizan, Sr. Solutions Architect
August 2022, CoVA ISOAG





- Former Navy Submariner
 - USS Norfolk (SSN 714)
 - USS Memphis (SSN 691)
- Ex JPMC
- AWS for 7 years, all in SLG
- Application Modernization

Agenda

- The AWS Story
- The security needs of customers
- AWS layered security services portfolio
- Cloud Security best practices
 - Well-architected applications
- Automating Security and Governance
 - AWS Control Tower
 - AWS Security Hub
- Adding automated response & remediation
- Disaster Recovery

The AWS Story

What is AWS?

AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers millions of businesses in over 240 countries and territories around the world.

Benefits

- Low Cost
- Elasticity & Agility
- Open & Flexible
- Secure
- Global Reach

The image is a promotional graphic for AWS Global Infrastructure. It features a dark blue background with a stylized globe on the right side, showing a network of white lines representing global connectivity. In the top left corner, the AWS logo is displayed in white. Below the logo, the text reads: "The Most Extensive, Reliable and Secure Global Cloud Infrastructure Available". Underneath this text is a button with the text "SEE HOW WE DO IT >>". At the bottom left, there is a small paragraph of text: "The Amazon Web Services (AWS) Global Infrastructure delivers a cloud infrastructure companies can depend on—no matter their size, changing needs, or challenges. The AWS Global Infrastructure is designed and built to deliver the most flexible, reliable, scalable, and secure cloud computing environment with the highest quality global".








aws

The Most Extensive, Reliable and Secure Global Cloud Infrastructure Available

[SEE HOW WE DO IT >>](#)

The Amazon Web Services (AWS) Global Infrastructure delivers a cloud infrastructure companies can depend on—no matter their size, changing needs, or challenges. The AWS Global Infrastructure is designed and built to deliver the most flexible, reliable, scalable, and secure cloud computing environment with the highest quality global

What sets AWS apart?

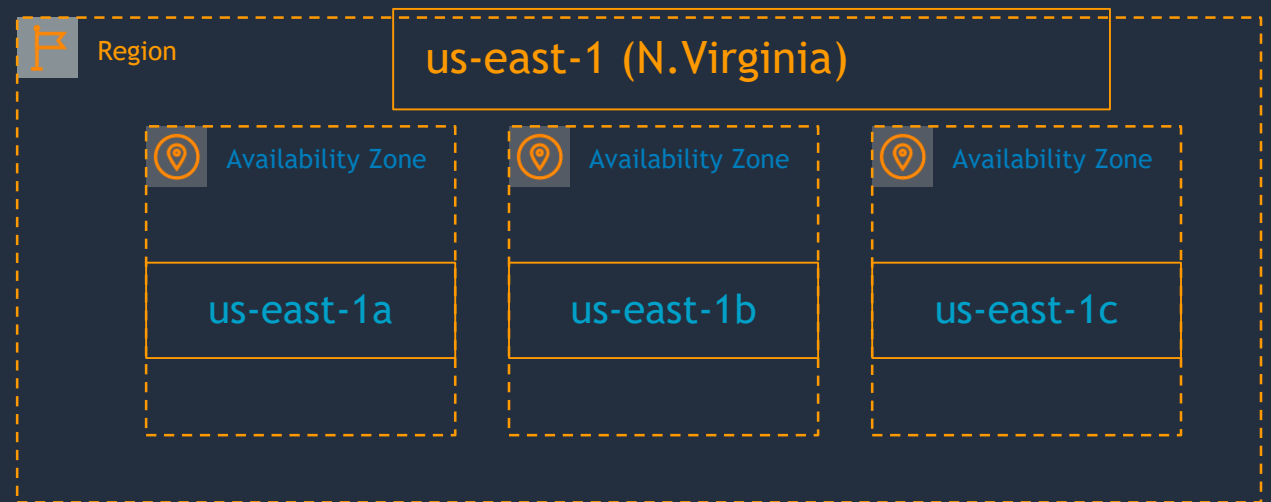
-  **Security**
Fine-grained identity and access control;
Build with the Highest Standards for Privacy and Data Security
-  **Service Breadth & Depth;
Pace of Innovation**
200+ fully featured services to support any cloud workload; AWS released 3,084 significant features and services in 2021
-  **Experience: 1M+ customers**
Building and managing cloud since 2006
-  **Global Footprint**
84 Availability Zones within 26 geographic Regions, 17 Local Zones, 410+ Points of Presence (400+ Edge Locations and 13 Regional Edge Caches) in 90+ cities across 47 countries.
-  **Machine Learning**
More machine learning happens on AWS than anywhere else.
Machine learning in the hands of every developer and data scientist.
-  **Ecosystem**
100,000+ APN partners from over 150 countries. The AWS Marketplace offers 50 categories, and 10,000+ Products
-  **Enterprise leader**
AWS positioned as a Leader in the Gartner Magic Quadrant for Cloud Infrastructure and Platform Services

26 Regions



Availability Zones

- Each AWS Region consists of multiple, isolated, and physically separate AZs within a geographic area
- An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region
- High throughput, low latency (<10mS) network between Availability Zones
- All traffic between AZ's is encrypted
- Physical separation with 100 km (60 miles)



Customer obsessed



90%

of roadmap originates with customer requests and are designed to meet specific needs



"Performance, reliability, and responsiveness are fundamental to our customer experience, and T3 instances help us to deliver on that customer promise while also controlling our costs."

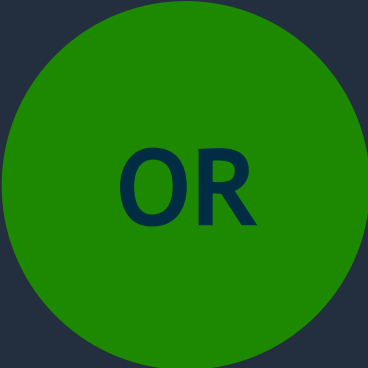
—Heroku



The security needs of customers

Before...

Move fast



Stay secure

Now...

Move fast **AND** Stay secure

Balancing the needs of builders and central cloud IT

Builders:
Stay agile



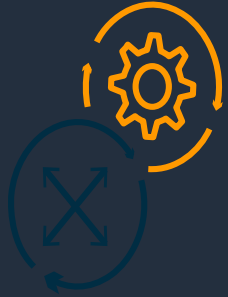
Innovate with the speed and
agility of AWS

Cloud IT:
Establish governance



Govern at scale with
central controls

More innovation, greater agility, with control



Agility

Experiment

Be productive
Empower distributed
teams
Self-service access
Respond quickly
to change

Don't choose between
Agility or Control
*You need and want
both*



Governance

Enable
Provision
Operate

Secure & Compliant
Operations & Spend
Management

The most-sensitive workloads run on AWS



“We prioritize data privacy and security in our platforms as well as ensuring we observe customer preferences. AWS was chosen because it's great in rich web application services.”

—Christopher Bird, global platform CTO of messaging, HSBC’s Wealth & Personal Banking



“The maturity of AWS infrastructure and the level of security audits that AWS performs on its data centers and services gave us peace of mind. We knew that the privacy and security of patient and customer data would be the top priority.”

—Mark Maalouf, Vice President, Global Digital Health, Teva



“Migrating to AWS was an important step in creating better delivery velocity for our security applications.”

—Jon Barcellona, Cybersecurity Engineering Director, Southwest Airlines

Customers need....

Infrastructure & services to elevate security



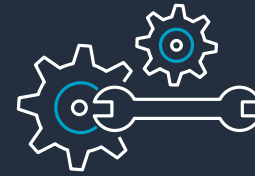
Inherit global security and compliance controls



Scale with superior visibility and control



Highest standards for privacy and data security



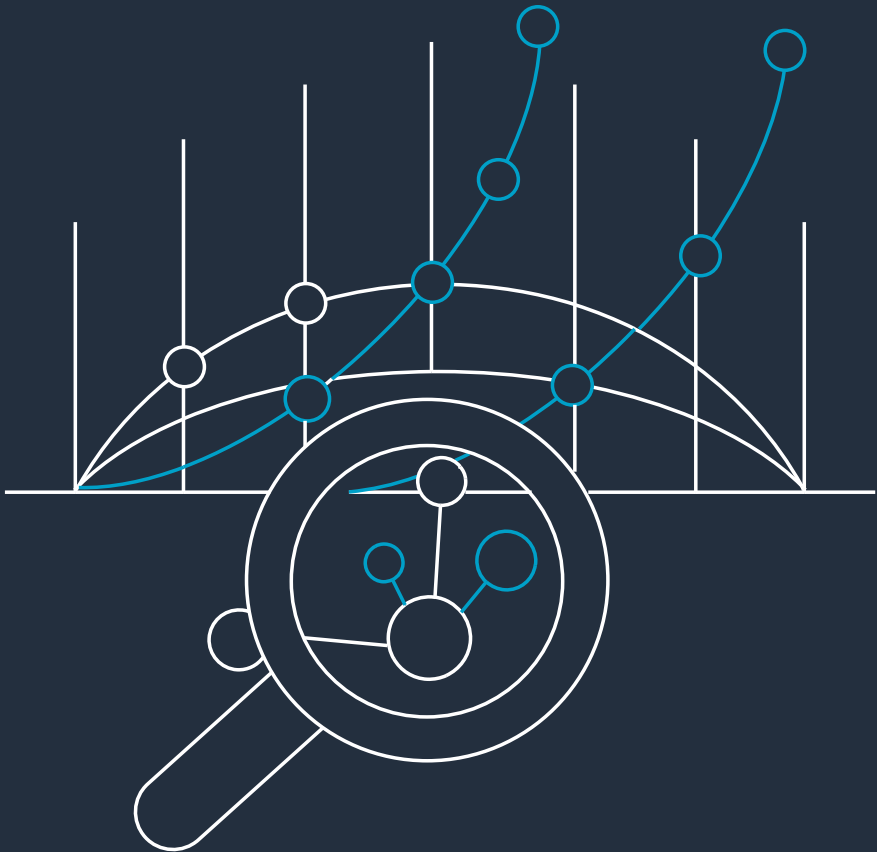
Automate & reduce risk with deeply integrated services



Largest ecosystem of security partners and solutions

Customers need....

Scale with superior visibility and control



Control where your data is stored and who can access it

Fine-grain identity and access controls so users and groups have the right access to resources

Reduce risk via security automation and continuous monitoring

Integrate AWS services with your solutions to support existing workflows, streamline ops, and simplify compliance reporting

Customers need....

Highest standards for privacy and data security



Meet data residency requirements

Choose an AWS Region, and AWS will not replicate it elsewhere unless you choose to do so



Encryption at scale with keys managed by AWS Key Management Service or managing your own encryption keys with AWS CloudHSM using FIPS 140-2 Level 3 validated HSMs



Comply with local data privacy laws by controlling who can access content, its lifecycle, and its disposal




Access services and tools that enable you to **build compliant infrastructure** on top of AWS

Customers need....

To automate and reduce risk with integrated services

Comprehensive set of APIs
and security tools




Continuous monitoring
and protection 



 Threat remediation
and response

Operational efficiencies to
focus on critical issues 

 Securely deploy business
critical applications

Gain access to a world-class security team

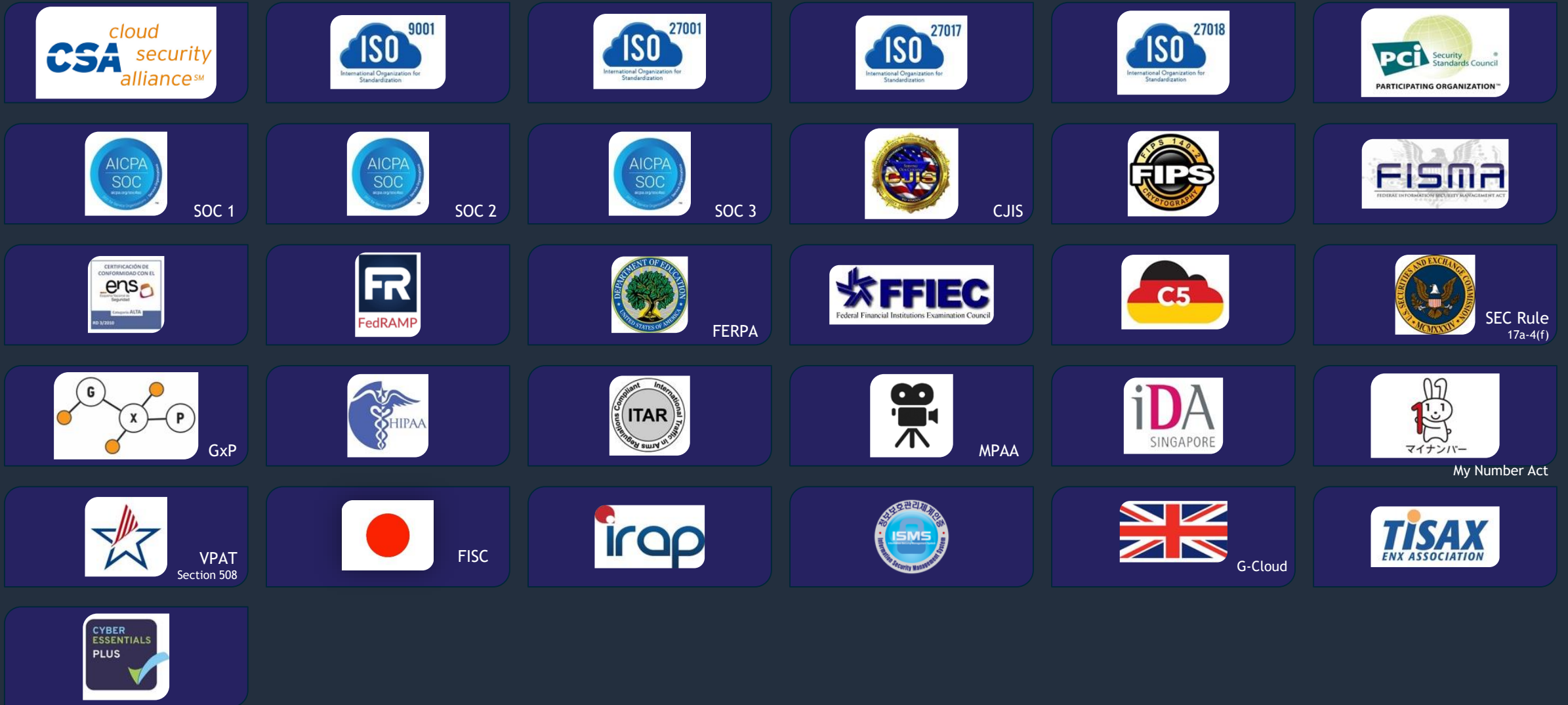
Where would some of the world's top security people like to work? At scale on huge challenges with huge rewards

So AWS has **world-class security and compliance** teams watching your back!

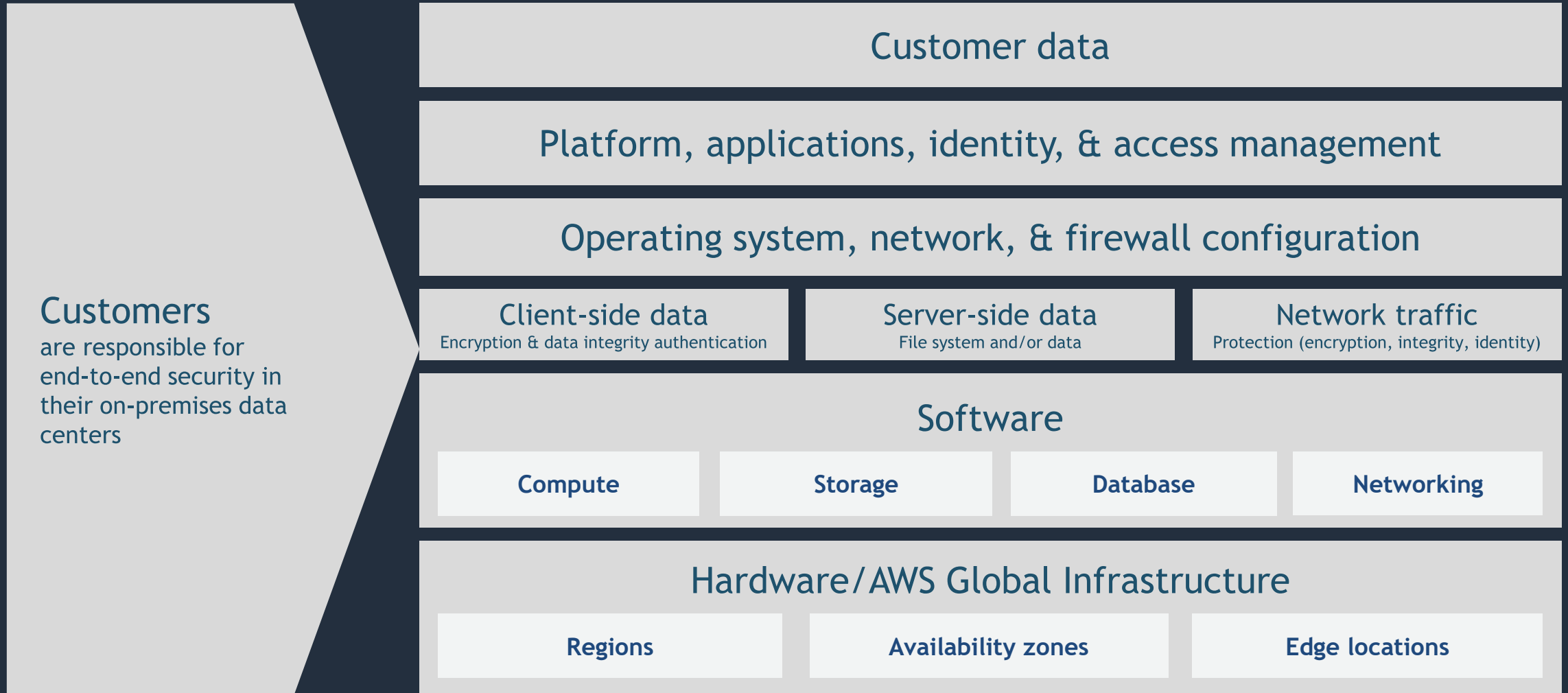
Every customer benefits from the tough scrutiny of other AWS customers



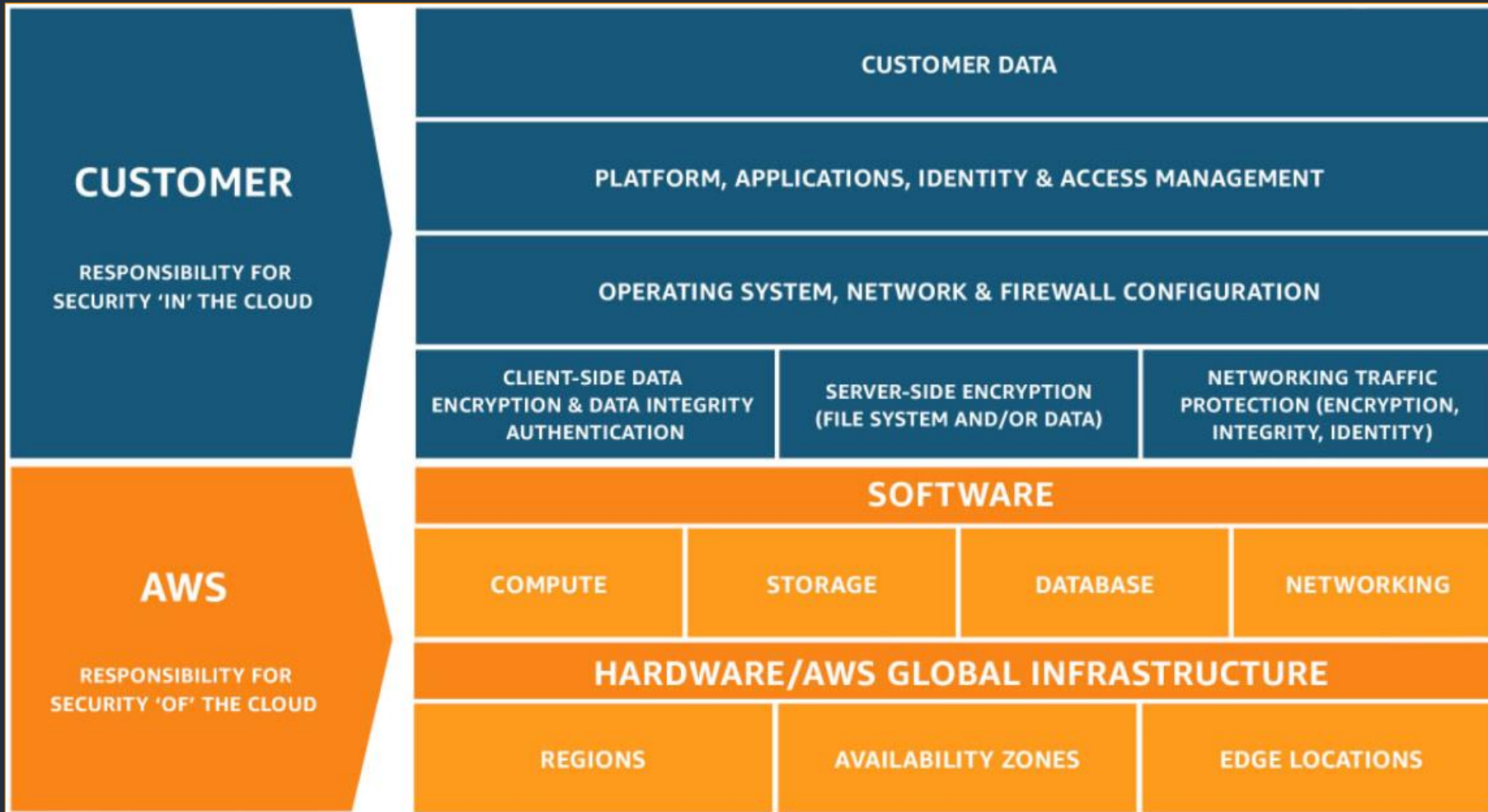
Inherit global security and compliance controls



Traditional on-premises security model



Security & Compliance is a **Shared Responsibility**



FSI Auditors



Third-party Independent Auditors

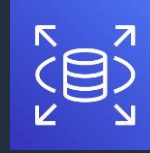
<https://aws.amazon.com/compliance/shared-responsibility-model/>



The Line **Varies** ...



Amazon EC2



Amazon RDS



AWS S3

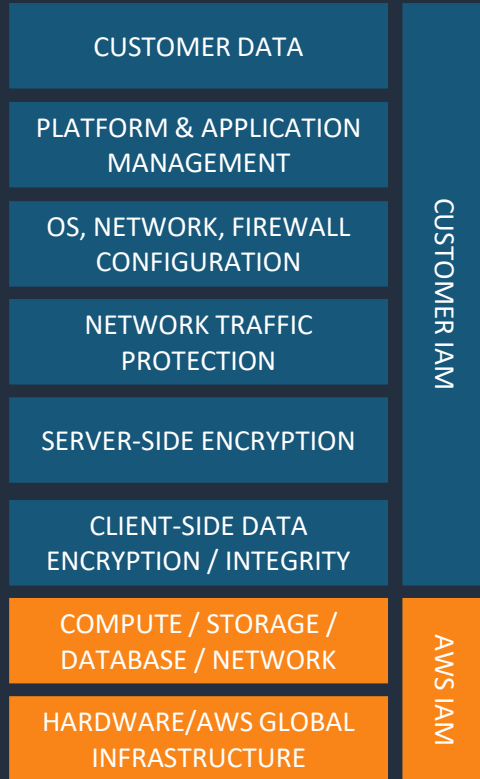


AWS KMS

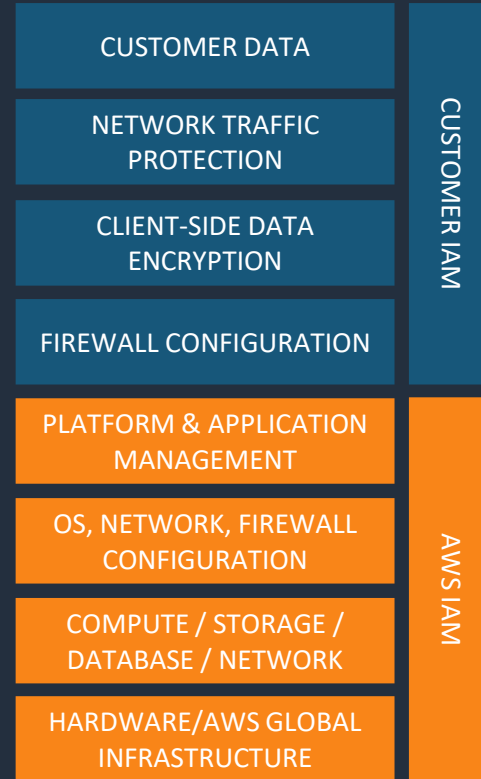


DynamoDB

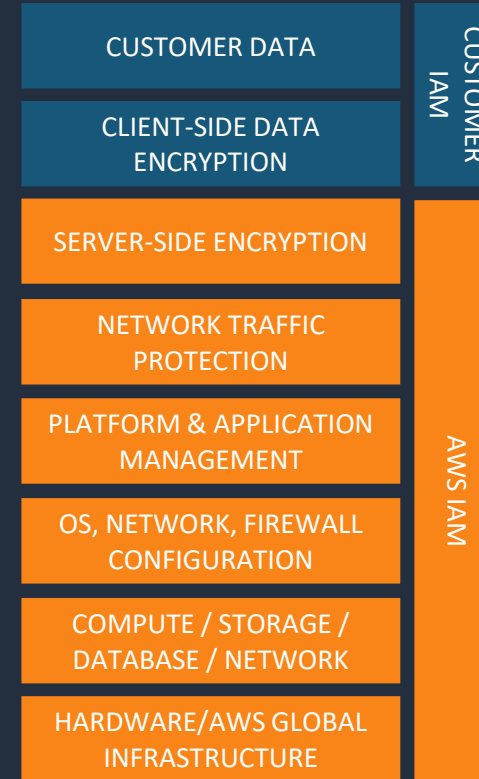
More Customizable
+
More Customer Responsibility



Infrastructure Services



Container Services



Abstracted Services

Less Customizable
+
Less Customer Responsibility
+
More Best Practices built-in

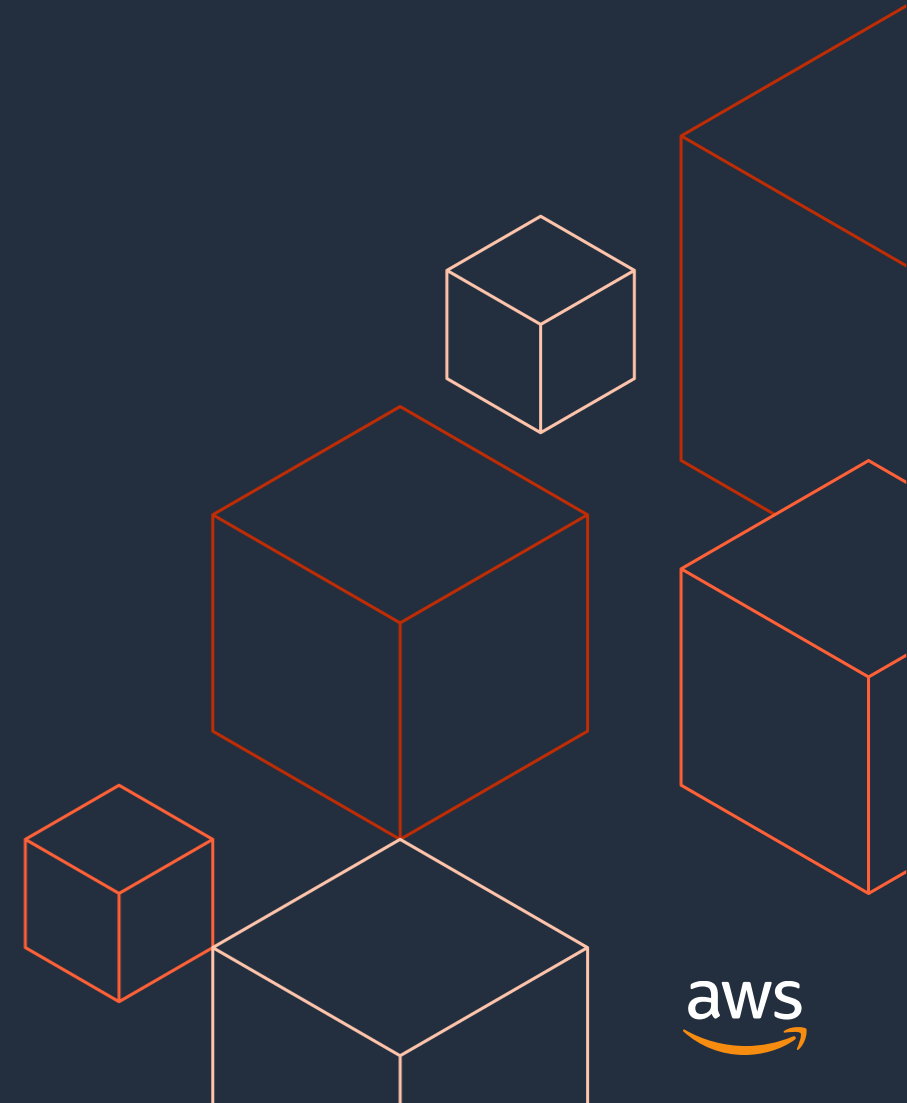
The layered security approach



AWS foundational and layered security services



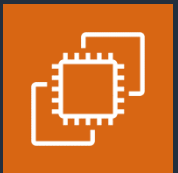
How do I enable threat detection at scale?



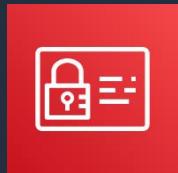
Threat detection, monitoring, and response



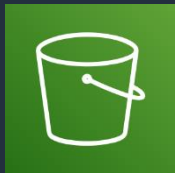
Security Monitoring and Threat Detection



Amazon EC2



AWS Identity and Access Management (IAM)



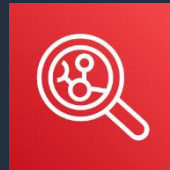
Amazon Simple Storage Service (S3)



Amazon GuardDuty



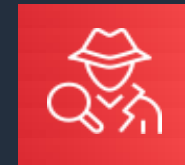
Amazon Macie



Amazon Inspector



AWS Security Hub



Amazon Detective

“Take Action”

Scalable and centralized management

Built-in integration with AWS Organizations

Administrator / member setup



- Designate a centralized delegated administrator



- Add all member accounts



- Auto-enable services on all member accounts

Amazon GuardDuty

Foundational threat detection & monitoring layer

Protect your AWS accounts, workloads, and data with intelligent threat detection and continuous monitoring



One-click activation with no performance impact



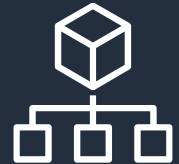
Continuous monitoring of AWS accounts and resources



Global coverage with regional results

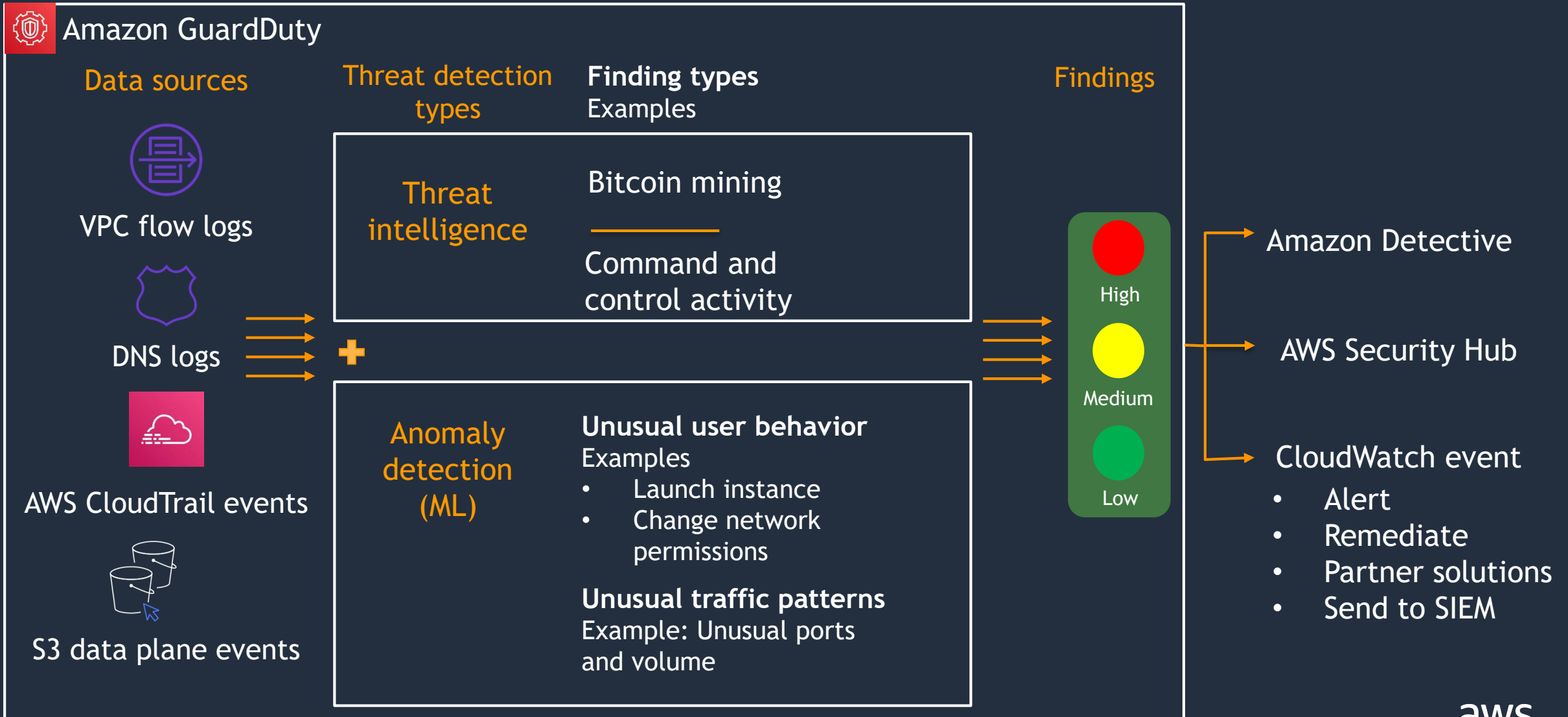


Detect known & unknown threats



Enterprise-wide consolidation & management

Amazon GuardDuty: How it works



Amazon GuardDuty built-in data sources



Amazon VPC flow logs

VPC flow logs capture information about the IP traffic going to and from network interfaces in your VPC

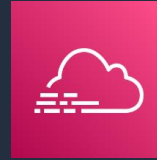
VPC flow logs **do not** need to be turned on to generate findings; data is consumed through an independent stream



DNS logs

DNS logs are based on queries made from Amazon EC2 instances to known and unknown questionable domains

DNS logs are in addition to Amazon Route 53 query logs; Route 53 is not required for GuardDuty to generate DNS-based findings



CloudTrail events

AWS CloudTrail provides a history of API calls used to access AWS Management Console, SDKs, AWS CLI

Identification of user and account activity, including source IP address used to make the calls; CloudTrail event logs **do not** need to be turned on to generate findings



CloudTrail S3 data events

Data events, also known as data plane operations, provide insight into the resource operations performed on or within a resource

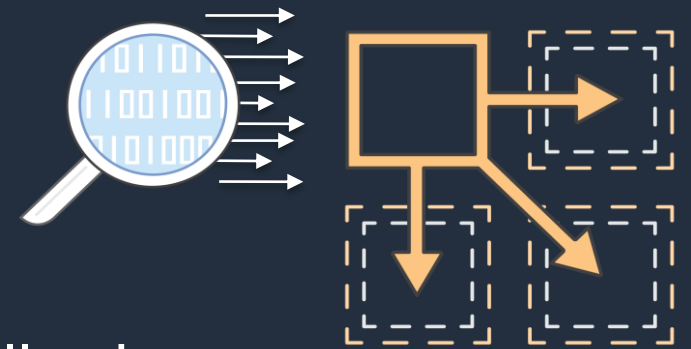
GetObject, ListObjects, DeleteObject, and PutObject API operations

What can GuardDuty detect?

Detecting known threats using threat intelligence

GuardDuty leverages threat intelligence from various sources

- AWS security intel
- AWS partners CrowdStrike and Proofpoint
- Customer-provided threat intel



Threat intelligence enables GuardDuty to identify the following

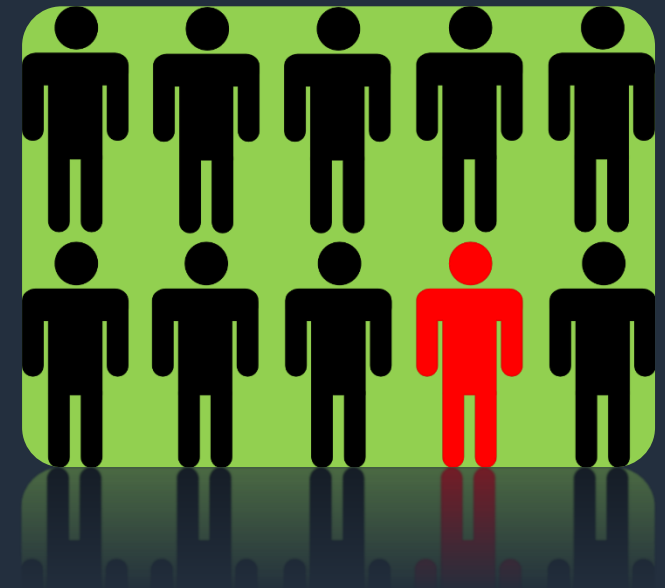
- Known malware-infected hosts
- Anonymizing proxies
- Sites hosting malware and hacker tools
- Cryptocurrency mining pools and wallets

What can GuardDuty detect?

Unknown threats using machine learning

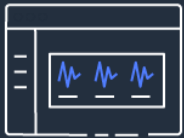
Algorithms to detect unusual behavior

- Inspecting signal patterns for heuristics
- Profiling the normal and looking at deviations
- Machine learning classifiers



Amazon Inspector

Automated and Continuous Vulnerability Management at Scale



Gain centralized visibility

- Environment coverage
- High impact findings
- Resources by finding severity



One-click continuous monitoring

- Automatic discovery of resources
- Monitors throughout the resource life-cycle



Prioritize with contextualized scoring

- Inspector Risk score
- Security metrics
- Customized views



Centrally manage at scale

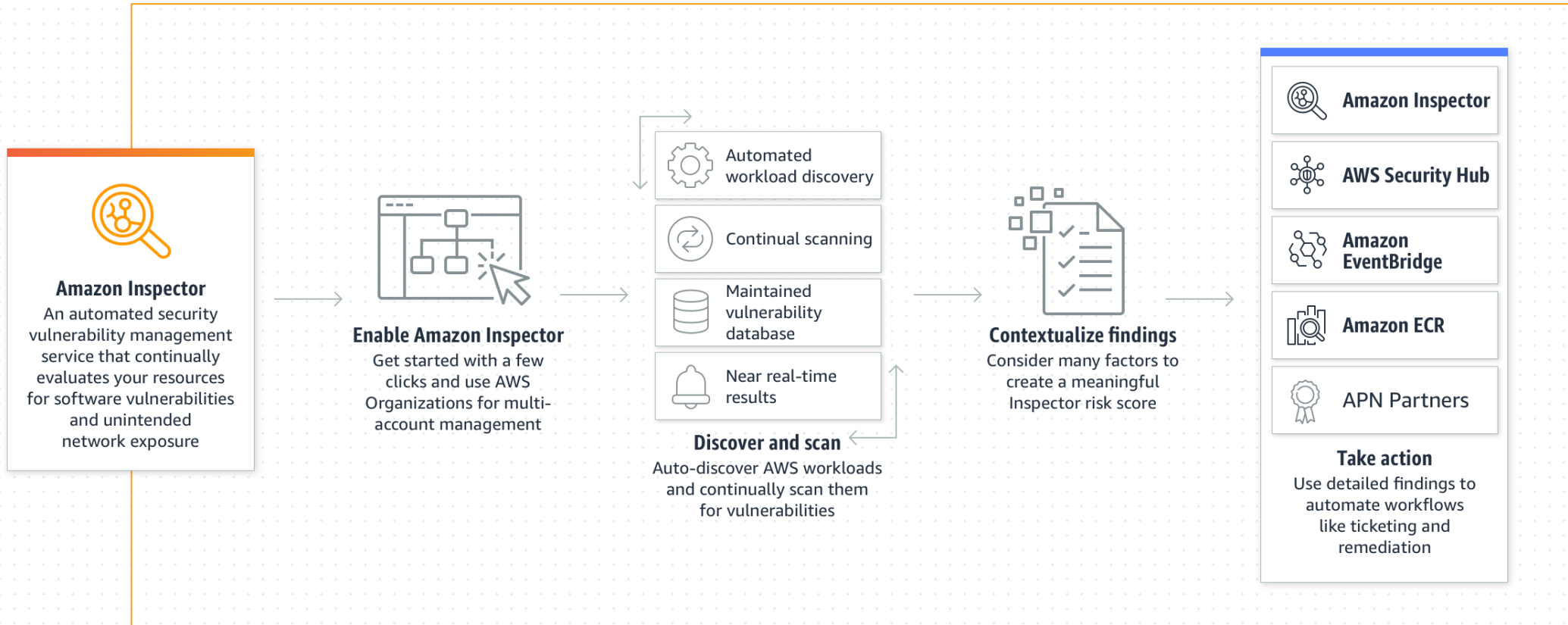
- AWS Organizations
- Package vulnerability, Network reachability
- Environment coverage



Automate and take actions

- Management APIs
- Detailed findings in Eventbridge
- Security Hub integration

Amazon Inspector - How it works



Continuous discovery and scanning

Automatically discover workloads and continually scan them for vulnerabilities across your organization



- **Automatic Discovery** - Amazon Inspector automatically discovers all eligible resources and begins continuous scans of those resources for software vulnerabilities and unintended network exposure.
- **Continuous scanning** - Amazon Inspector employs its own, purpose-built scanning engine to monitor your resources for software vulnerabilities or open network paths that can result in compromised workloads, malicious use or resources, or unauthorized access to your data.

Amazon Inspector monitors your environment throughout the life-cycle of your resources by running scans in response to events such as after the installation of a new application or patch.

Amazon Inspector utilizes the SSM (SSM) service to collect software application inventory needed to scan Amazon EC2 instances for software vulnerabilities. Amazon Inspector can only scan for software vulnerabilities in operating systems supported by SSM.

Prioritized and contextualized scoring

Drive efficiency and accuracy with the Amazon Inspector risk score for prioritized, contextualized, and actionable results.



- **Amazon Inspector score** - The Inspector risk score is a highly contextualized score that is generated for each finding by correlating common vulnerabilities and exposures (CVE) information with network reachability results, and exploitability data.
- **Vendor score**
 - **Software package vulnerability scoring** - Amazon Inspector uses the NVD/CVSS score as the basis of severity scoring for software package vulnerabilities.
 - **Network Reachability scoring** - Amazon Inspector uses the NVD/CVSS score as the basis of severity scoring for software package vulnerabilities. The NVD/CVSS score is the vulnerability severity score published by the NVD and is defined by the CVSS.

Amazon Inspector examines the security metrics that compose the National Vulnerability Database (NVD) base score for the vulnerability and adjusts them according your compute environment.

Amazon Detective

Investigative layer

Quickly analyze, investigate, and identify root cause of security issues



Built-in data
collection

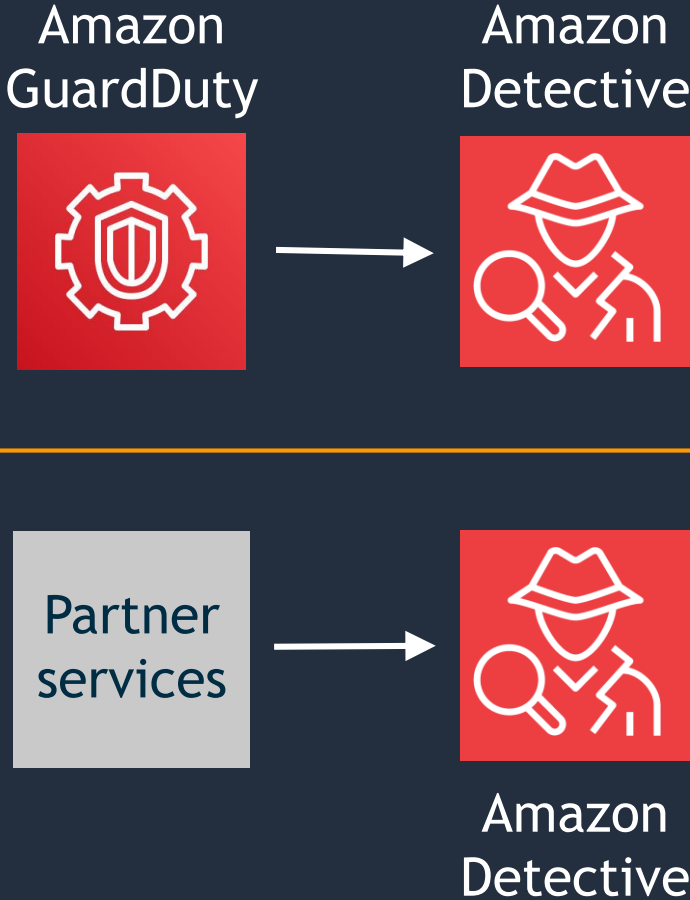
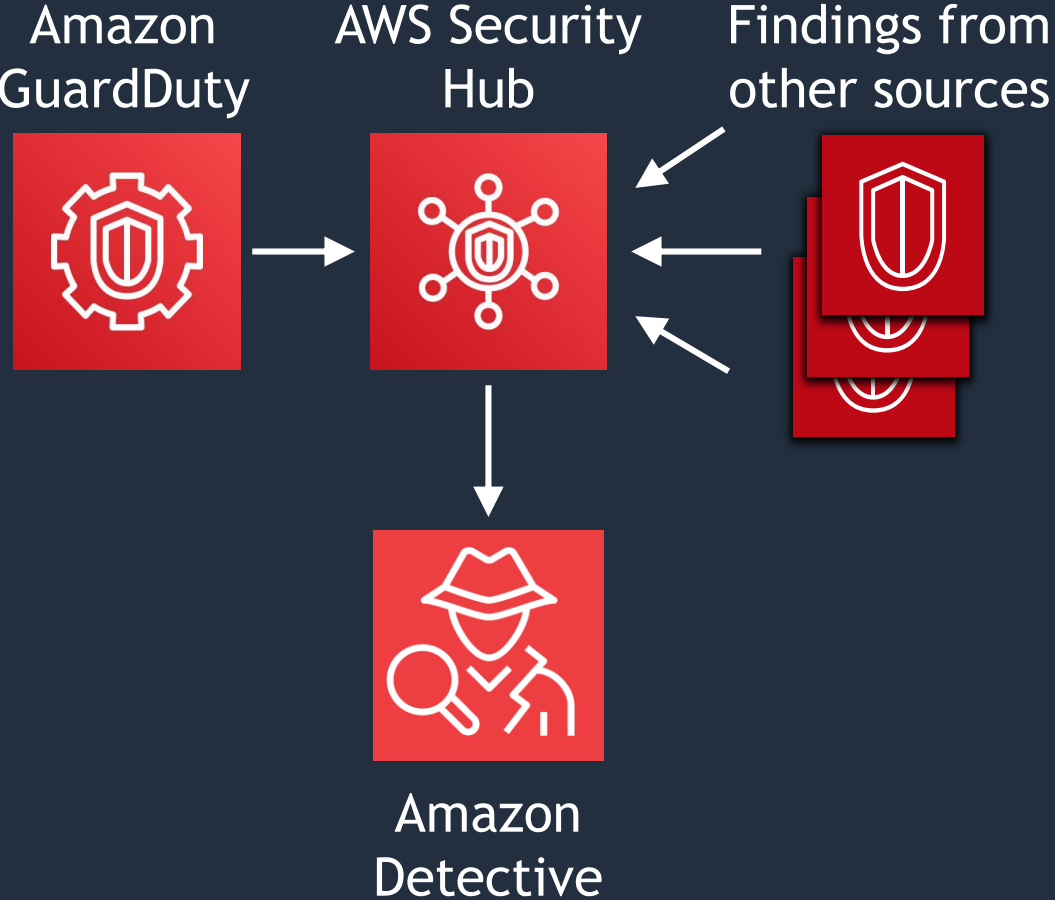


Automated analysis



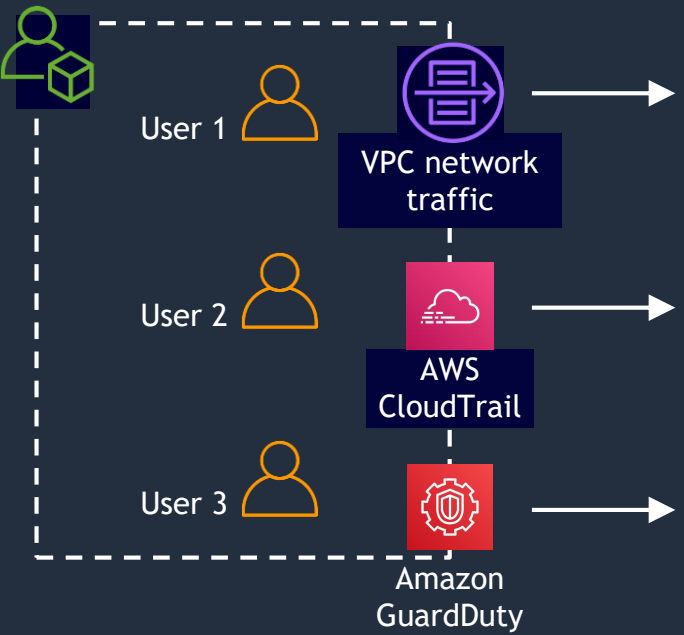
Visual insights

Amazon Detective usage flow

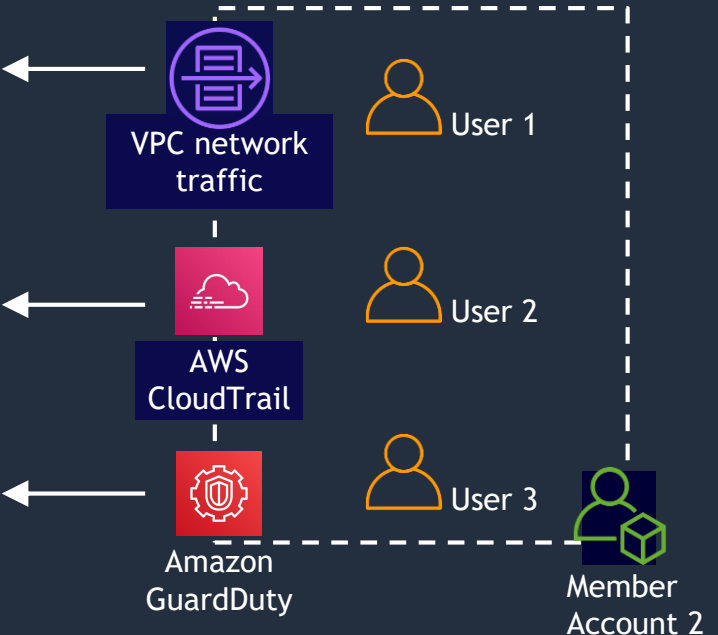
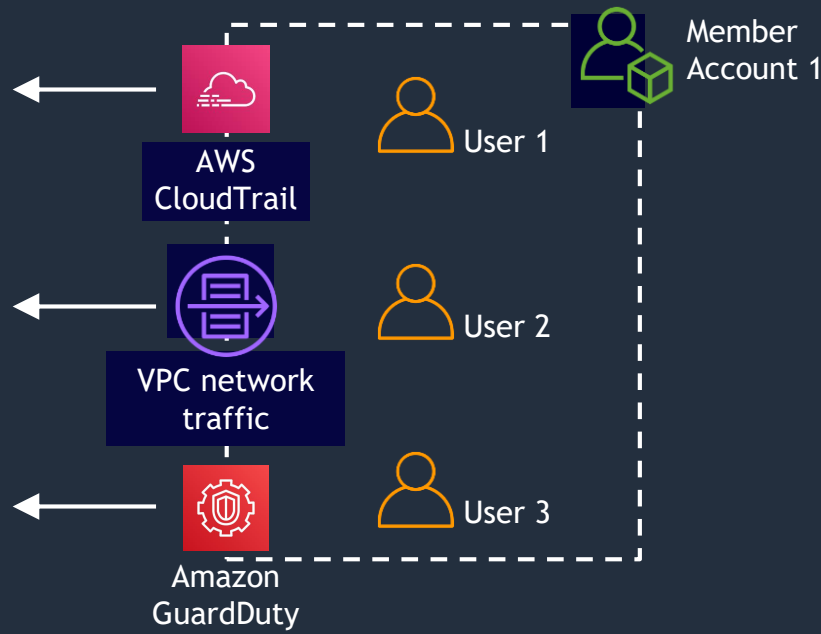
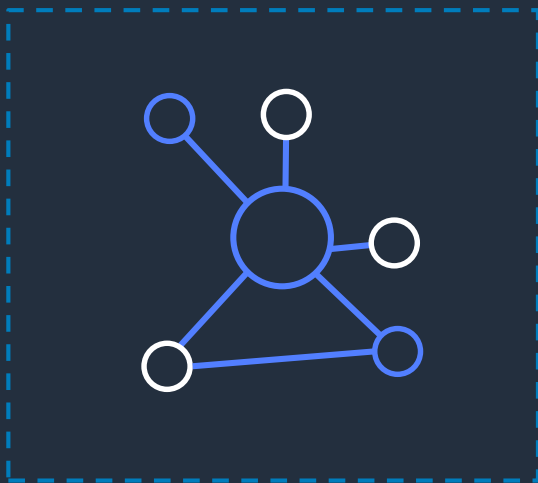


Multi-account telemetry collection

Administrator account



Administrator accounts
Amazon Detective
security behavior graph



How do I monitor & respond to threats at scale?



AWS Security Hub

Continuous security assessment & automated response layer

Centrally view & manage security alerts & automate security checks



Save time with aggregated findings



Improve security posture with automated checks



Curated security best practices



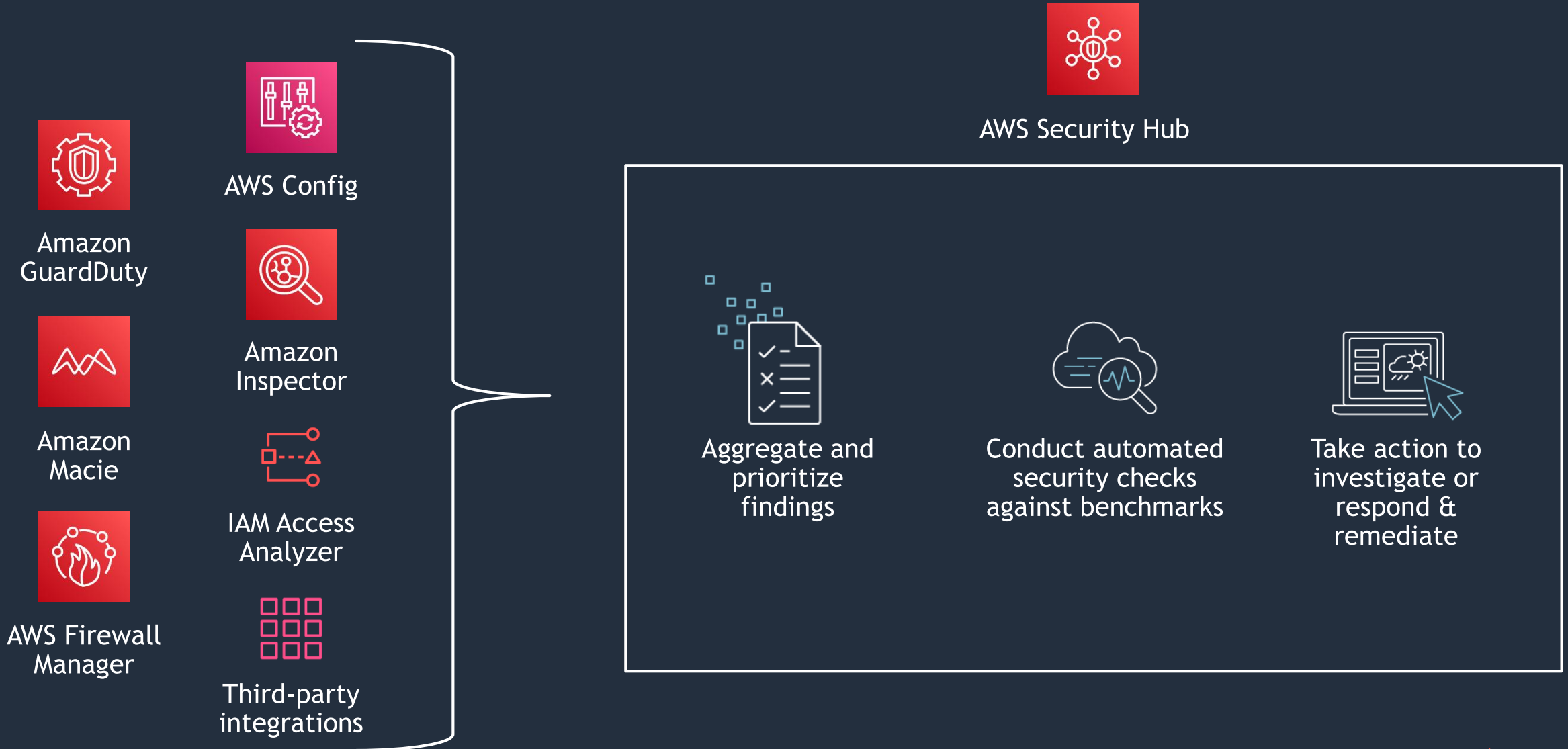
Seamless integration w/ standardized findings format

Account 1
Account 2
Account 3



Multi-account support

How AWS Security Hub works




Automated security & compliance checks

Security Hub > Security standards

Security standards

New **AWS Foundational Security Best Practices v1.0.0** by AWS


Description
The AWS Foundational Security Best Practices standard is a set of automated security checks that detect when AWS accounts and deployed resources do not align with security best practices. The standard is defined by AWS security experts. This curated set of controls helps improve your security posture in AWS, and covers AWS's most popular and foundational services.

Security score
 58%

[Disable](#) [View results](#)

CIS AWS Foundations Benchmark v1.2.0 by AWS


Description
The Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.

Security score
 19%

[Disable](#) [View results](#)

PCI DSS v3.2.1 by AWS

Description
The Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 is an information security standard for entities that store, process, and/or transmit cardholder data. This Security Hub standard automatically checks for your compliance readiness against a subset of PCI DSS requirements.

Security score
 41%

[Disable](#) [View results](#)

- 150+ fully automated, nearly continuous checks evaluated against pre-configured rules
- Findings are displayed on main dashboard for quick access.
- Best practices information is provided to help mitigate gaps to be in compliance.

Security Hub as a central dashboard



Centralize across accounts and prioritize findings without needing to normalize



View security and compliance posture against key standards

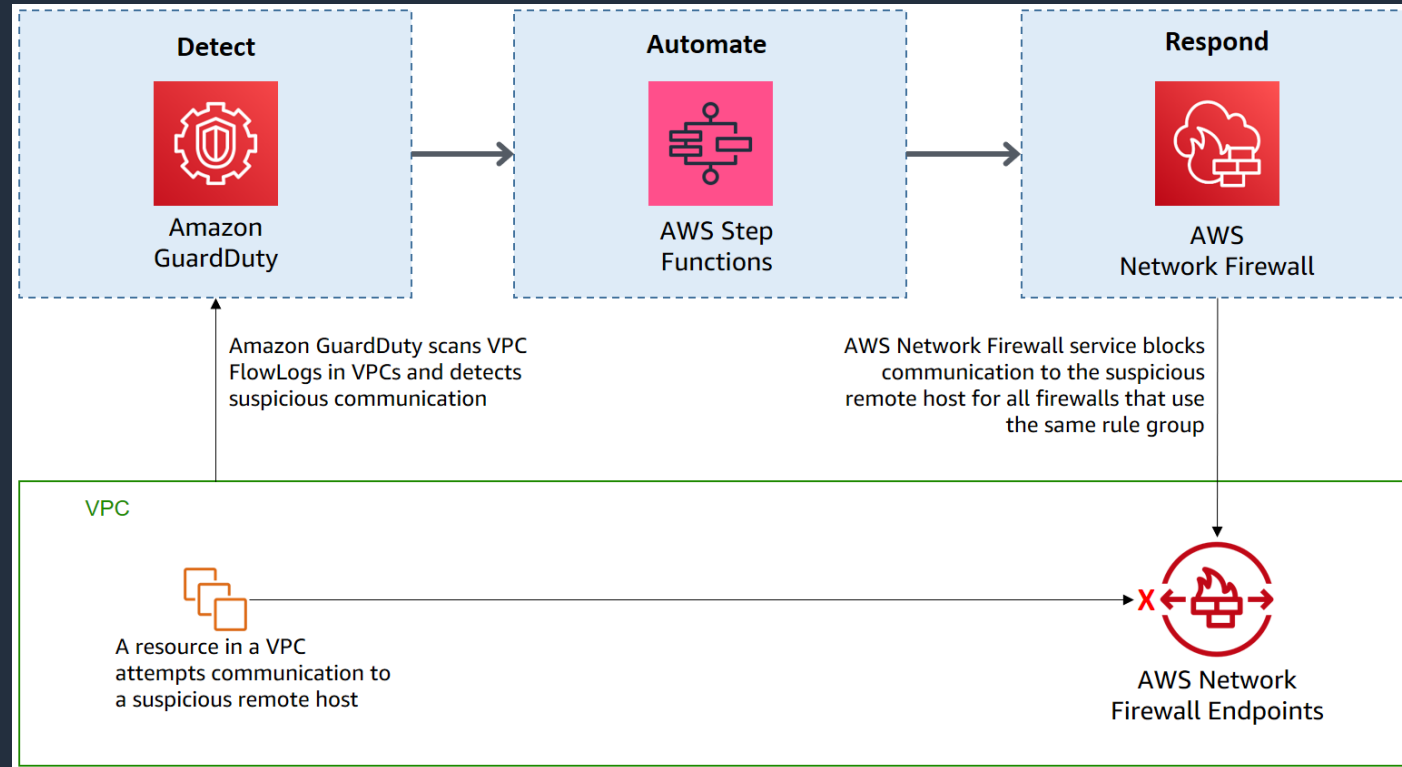


Take automated action on findings through CloudWatch Events

How do I automate response & remediation?



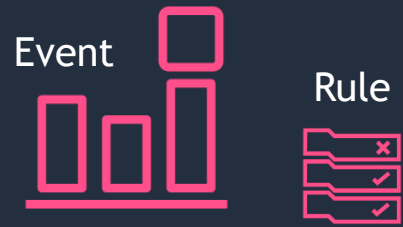
Automated detection & response



- Blocking traffic to and from suspicious remote hosts, for example to IP addresses associated with known command and control servers for botnets.
- GuardDuty detection of unintended communication with remote hosts triggers a series of steps, including blocking of network traffic to those hosts by using Network Firewall, and notification of security operators.

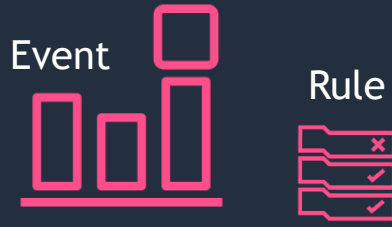
Use Security Hub Custom Actions to trigger automation

Security Hub Custom Action



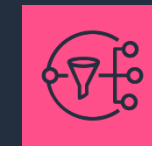
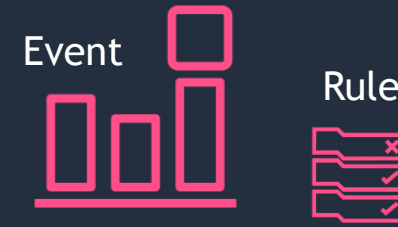
Lambda Function

Security Hub Custom Action



Amazon Kinesis Data Streams

Security Hub Custom Action

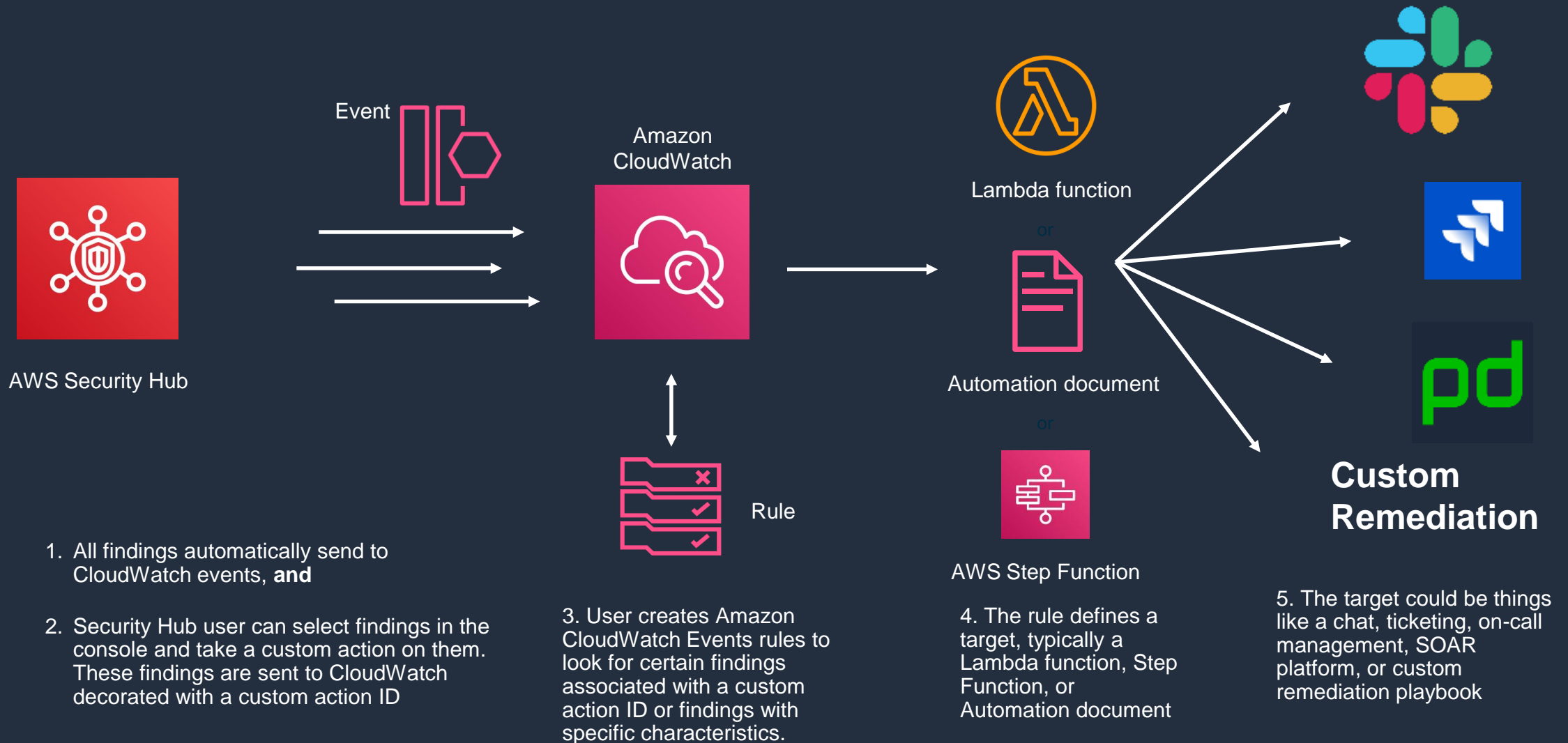


Amazon Simple Notification Service

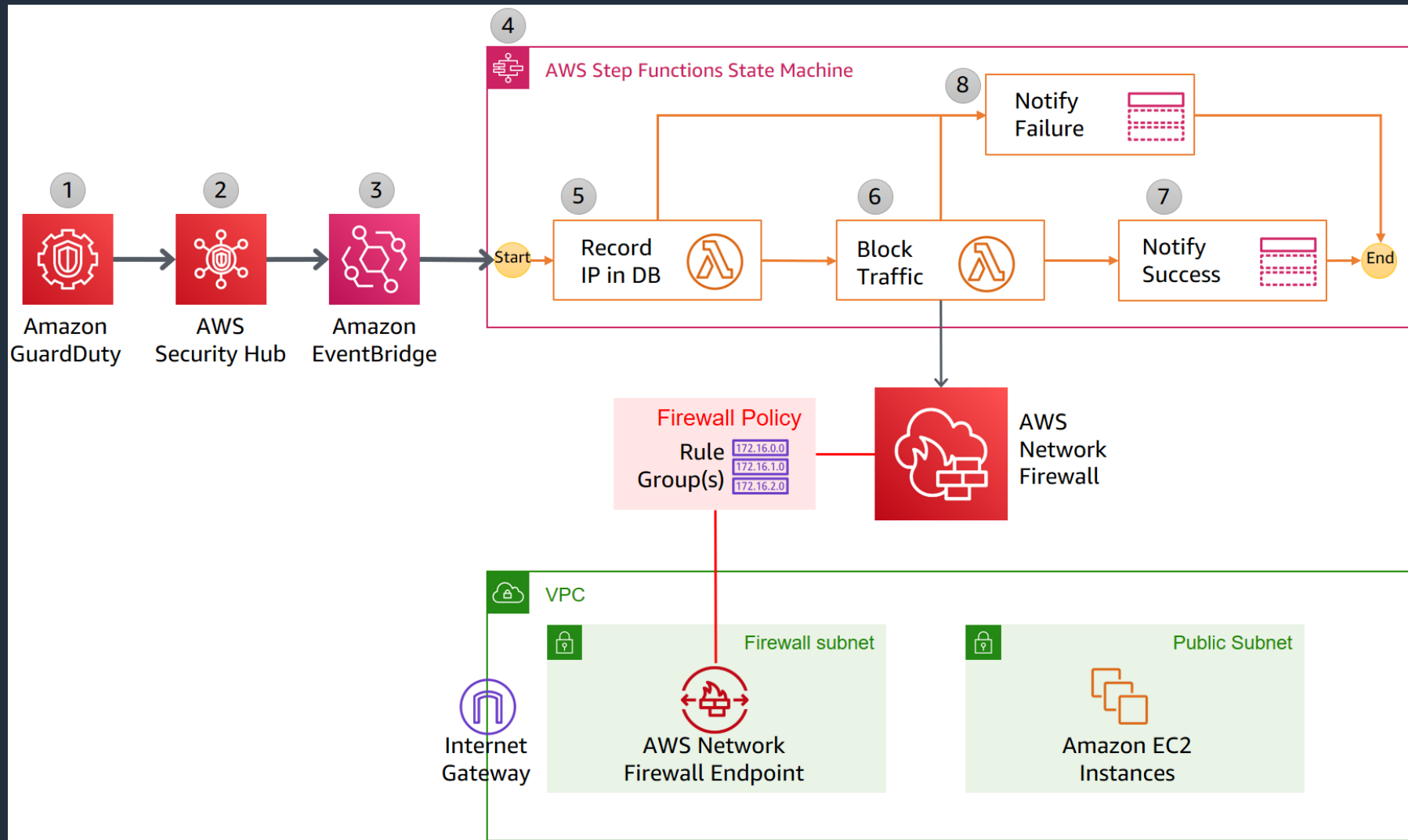


Run command

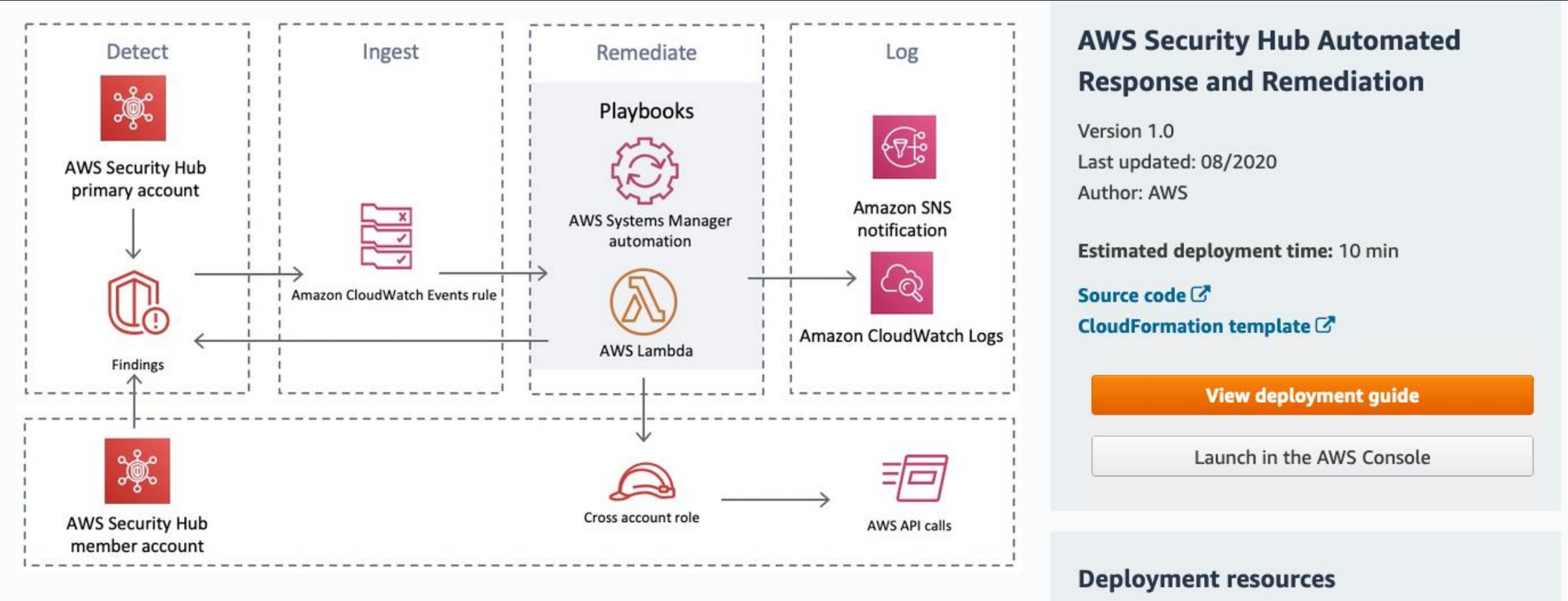
Customizable response and remediation actions



Customizable response and remediation actions



AWS Security Hub Automated Response and Remediation solution architecture



<https://aws.amazon.com/solutions/implementations/aws-security-hub-automated-response-and-remediation/>



Layer Threat Detection and Response Services

Advanced threat detection and response on AWS



Security tools natively available in AWS and from third parties



Reduce the burden for the security team



Centralized & scalable deployment with a click of a button

Sources of Best Practices

AWS Cloud Adoption Framework (CAF)



How to move to the cloud securely including the “Core Five Epics”:

- Identity and Access Management
- Logging and Monitoring
- Infrastructure Security
- Data Protection
- Incident Response

AWS Architecture Center



Architecture Center contains workshops, whitepapers, trainings and technical guides focusing on Security, including the Well Architect Framework (specially the Security pillar), and the AWS Security Reference Architecture.

CIS Benchmarks



148 detailed recommendations for configuration and auditing covering:

- “AWS Foundations” with 52 checks aligned to AWS Best Practices
- “AWS Three-Tier Web Architecture” with 96 checks for web applications

CIS Benchmarks: What, Why, Check, Fix

2.1 Ensure CloudTrail is enabled in all regions (Scored)

Profile Applicability:

- Level 1

Description:

AWS CloudTrail is a web log files to you. The records the API call, the source IP, response elements returned for an account, including line tools, and higher-level

Rationale:

The AWS API call history change tracking, and compliance exists will ensure that unauthorized

Audit:

Perform the following to determine

Via the management Console

1. Sign in to the AWS Management Console at <https://console.aws.amazon.com>
2. Click on Trails on the left navigation pane
 1. You will be presented with a list of trails
3. Ensure at least one Trail is enabled
4. Click on a trail via the link
5. Ensure Logging is set to On
6. Ensure Apply trail to all regions is checked

Via CLI

```
aws cloudtrail describe-trails
```

Remediation:

Perform the following to enable global CloudTrail logging:

Via the management Console

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/cloudtrail>
2. Click on Trails on the left navigation pane
3. Click Get Started Now, if presented
 - Click Add new trail
 - Enter a trail name in the Trail name box
 - Set the Apply trail to all regions option to Yes
 - Specify an S3 bucket name in the S3 bucket box
 - Click Create
4. If 1 or more trails already exist, select the target trail to enable for global logging
 1. Click the edit icon (pencil) next to Apply trail to all regions
 2. Click Yes
 3. Click Save

Via CLI

```
aws cloudtrail create-trail --name <trail_name> --bucket-name <s3_bucket_for_cloudtrail> --is-multi-region-trail
aws cloudtrail update-trail --name <trail_name> --is-multi-region-trail
```


Best-of-the-Best Practices: Identity and Access Management

1) Use **multiple AWS accounts** to reduce scope of impact

Production



Staging



AWS accounts provide administrative isolation between workloads across different lines of business, regions, stages of production and classes of data.

5

CIS Foundation Benchmark

0

CIS Web-Tier Benchmark

2) Use **limited roles** and grant **temporary security credentials**



IAM



IAM Roles



Secrets Manager

IAM roles and temporary security credentials mean you don't always have to manage long-term credentials and IAM users for each entity that requires access to a resource.

13

CIS Foundation Benchmark

8

CIS Web-Tier Benchmark

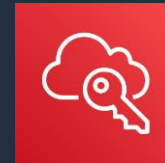
3) **Federate** to an existing identity service



IAM



MFA token



AWS SSO

Control access to AWS resources, and manage the authentication and authorization process without needing to recreate all your corporate users as IAM users.

0

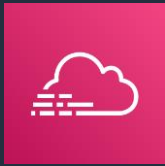
CIS Foundation Benchmark

0

CIS Web-Tier Benchmark

Best-of-the-Best Practices: Logging and Monitoring

4) Turn on logging in all accounts, for all services, in all regions



AWS
CloudTrail



Amazon
GuardDuty

The AWS API history in CloudTrail enables security analysis, resource change tracking, and compliance auditing. GuardDuty provides managed threat intelligence and findings.



CIS Foundation
Benchmark



CIS Web-Tier
Benchmark

5) Use the AWS platform's built-in monitoring and alerting features



AWS Security
Hub



AWS Config

Monitoring a broad range of sources will ensure that unexpected occurrences are detected. Establish alarms and notifications for anomalous or sensitive account activity.



CIS Foundation
Benchmark



CIS Web-Tier
Benchmark

6) Use a separate AWS account to fetch and store copies of all logs

Production



Security



Configuring a security account to copy logs to a separate bucket ensures access to information which can be useful in security incident response workflows.



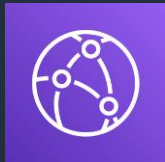
CIS Foundation
Benchmark



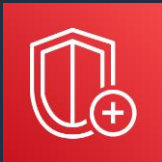
CIS Web-Tier
Benchmark

Best-of-the-Best Practices: Infrastructure Security

7) Create a **threat prevention layer** using AWS edge services



Amazon CloudFront



AWS Shield



AWS WAF

Use the hundreds of worldwide points of presence in the AWS edge network to provide scalability, protect from denial-of-service attacks, and protect from web application attacks.

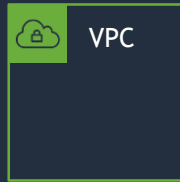


CIS Foundation Benchmark



CIS Web-Tier Benchmark

8) Create **network zones** with Virtual Private Clouds (VPCs) and security groups



Implement security controls at the boundaries of hosts and virtual networks within the cloud environment to enforce access policy.



CIS Foundation Benchmark



CIS Web-Tier Benchmark

9) Manage vulnerabilities through **patching and scanning**



Amazon Inspector

Test virtual machine images and snapshots for operating system and application vulnerabilities throughout the build pipeline, and into the operational environment.



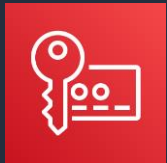
CIS Foundation Benchmark



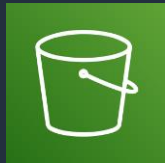
CIS Web-Tier Benchmark

Best-of-the-Best Practices: Data Protection

10) Encrypt **data at rest**
(with occasional exceptions)



AWS KMS



Amazon S3

Enabling encryption at rest helps ensure the confidentiality and integrity of data. Consider encrypting everything that is not public.



CIS Foundation Benchmark



CIS Web-Tier Benchmark

11) Use **server-side encryption** with provider managed keys



AWS KMS



Data Encryption Key

AWS Key Management Service (KMS) is seamlessly integrated with multiple AWS services. You can use a default master key or select a custom master key, both managed by AWS.

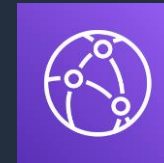


CIS Foundation Benchmark

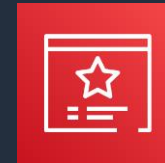


CIS Web-Tier Benchmark

12) Encrypt **data in transit**
(with no exceptions)



Amazon CloudFront



Certificate Manager



SSL / TLS / HTTPS

Encryption of data in transit provides protection from accidental disclosure, verifies the integrity of the data, and can be used to validate the remote connection.



CIS Foundation Benchmark



CIS Web-Tier Benchmark

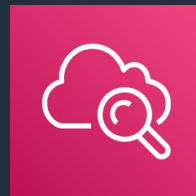
Tools and Automation

AWS Security Hub



An automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices.

Amazon CloudWatch Events



A monitoring service for AWS cloud resources and the applications you run on AWS. You can easily build workflows that automatically take actions you define, such as invoking an AWS Lambda function, when an event of interest occurs.

AWS Config Rules



A fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications. Config Rules enables you to create rules that automatically check the configuration of AWS resources recorded by AWS Config.

Resources

AWS Security Pillar Well Architected Framework

<http://bit.ly/WellArchSec>

CIS AWS Security Foundations Benchmark

<http://bit.ly/AWSCIS>

AWS Architecture Center - Security, Identity, & Compliance

<http://bit.ly/BstSec>

CIS AWS Three - Tier Web Architecture Benchmark

<http://bit.ly/AWSCIS3T>

AWS Security Reference Architecture

<https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/welcome.html>

Wouldn't it be great if there
was a service to orchestrate
everything?



AWS Control Tower: Easiest way to set up and govern AWS at scale



Enable



Provision



Operate

Business agility + governance control

Why use AWS Control Tower?



Set up a best-practices AWS environment in a few clicks

Standardize account provisioning

Centralize policy management

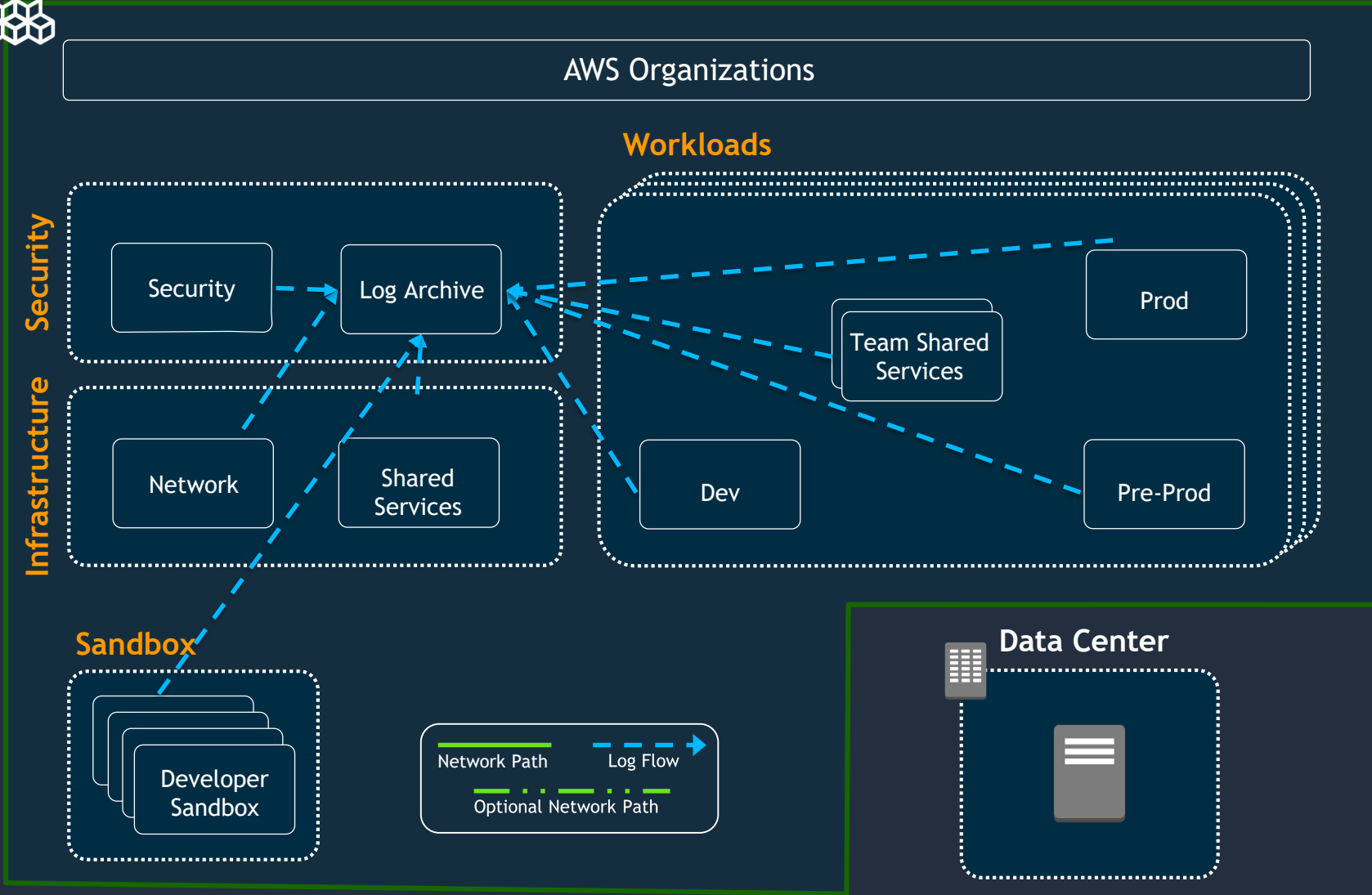
Enforce governance and compliance proactively

Enable end user self-service

Get continuous visibility into your AWS environment

Gain peace of mind

Multi-account approach // security log flow



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: AWS Direct Connect

Dev Sandbox: Experiments, Learning

Dev: Development

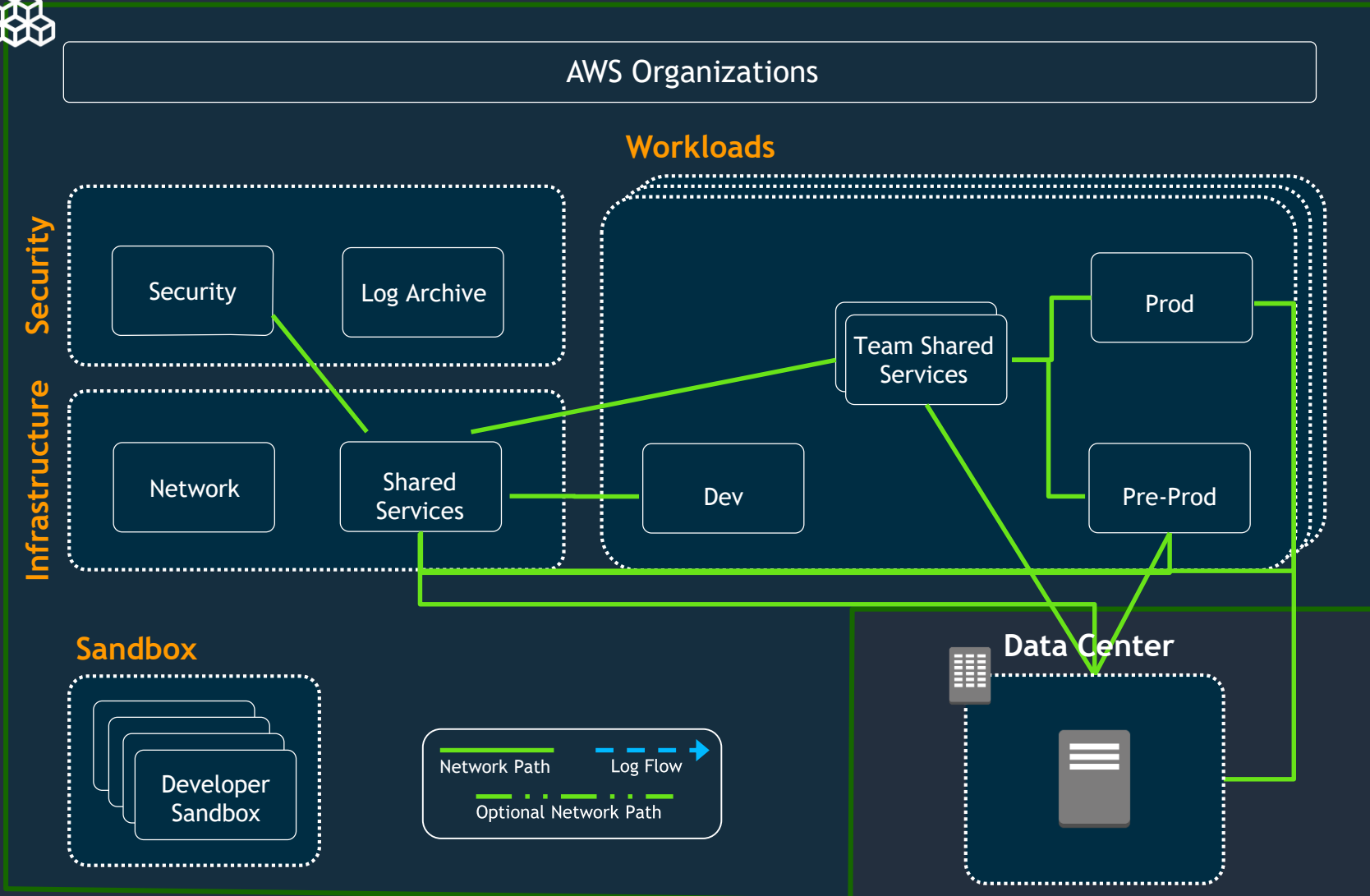
Pre-Prod: Staging

Prod: Production

Team SS: Team Shared Services, Data Lake



Multi-account approach // network connectivity



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: AWS Direct Connect

Dev Sandbox: Experiments, Learning

Dev: Development

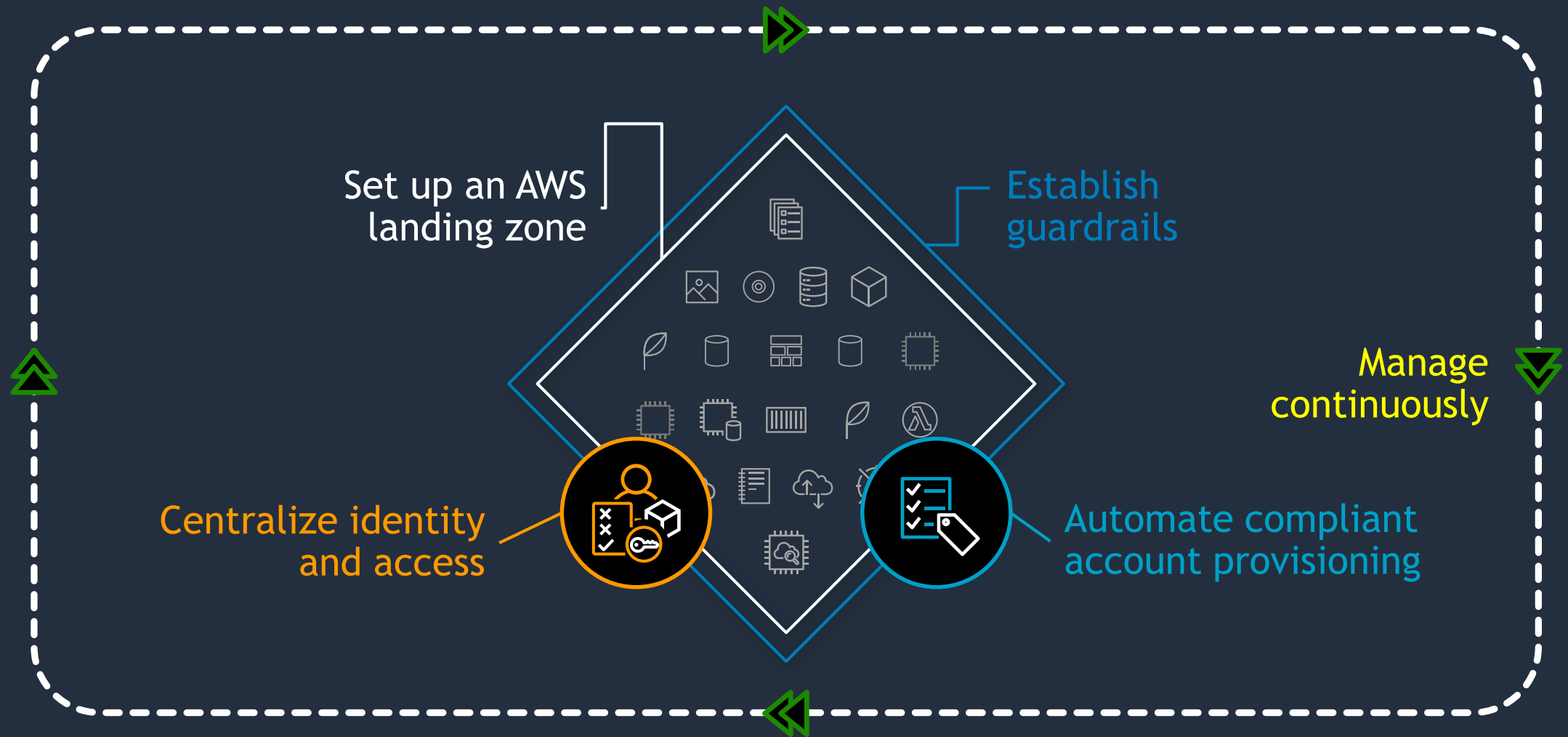
Pre-Prod: Staging

Prod: Production

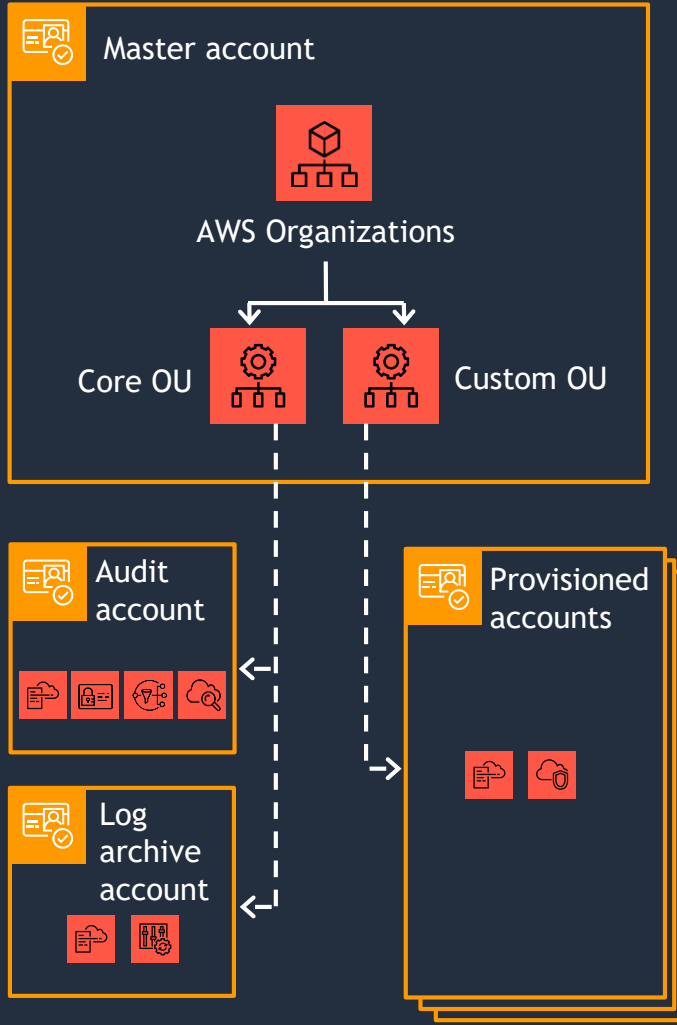
Team SS: Team Shared Services, Data Lake

Enable governance

Enable

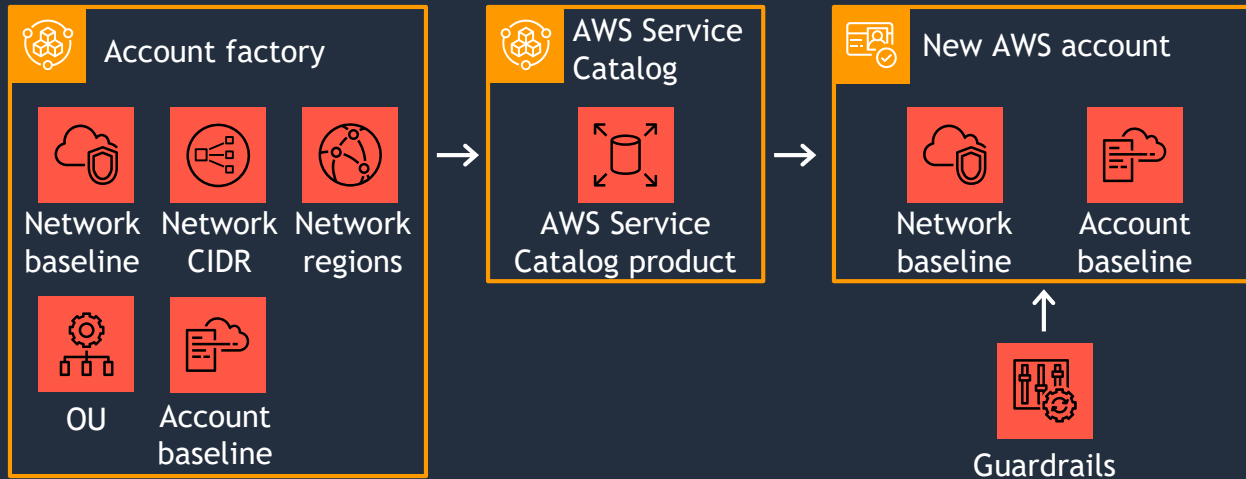


Multi-account architecture



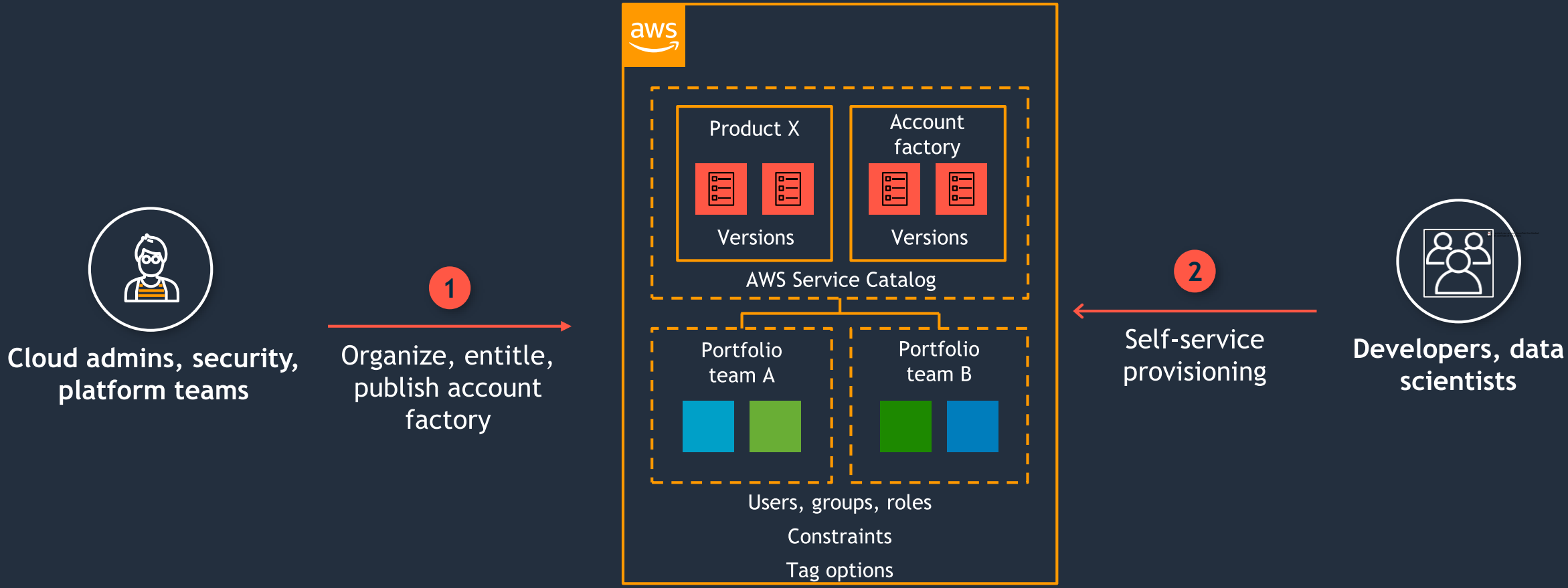
- Master account: designation of your existing account to create a new organization. Also your master payer account
- Organization consists of 2 OUs with pre-configured accounts -
 - Core OU: AWS Control Tower-created accounts, i.e., Audit account and Log archive account
 - Custom OU: Your provisioned accounts

Automate compliant account provisioning

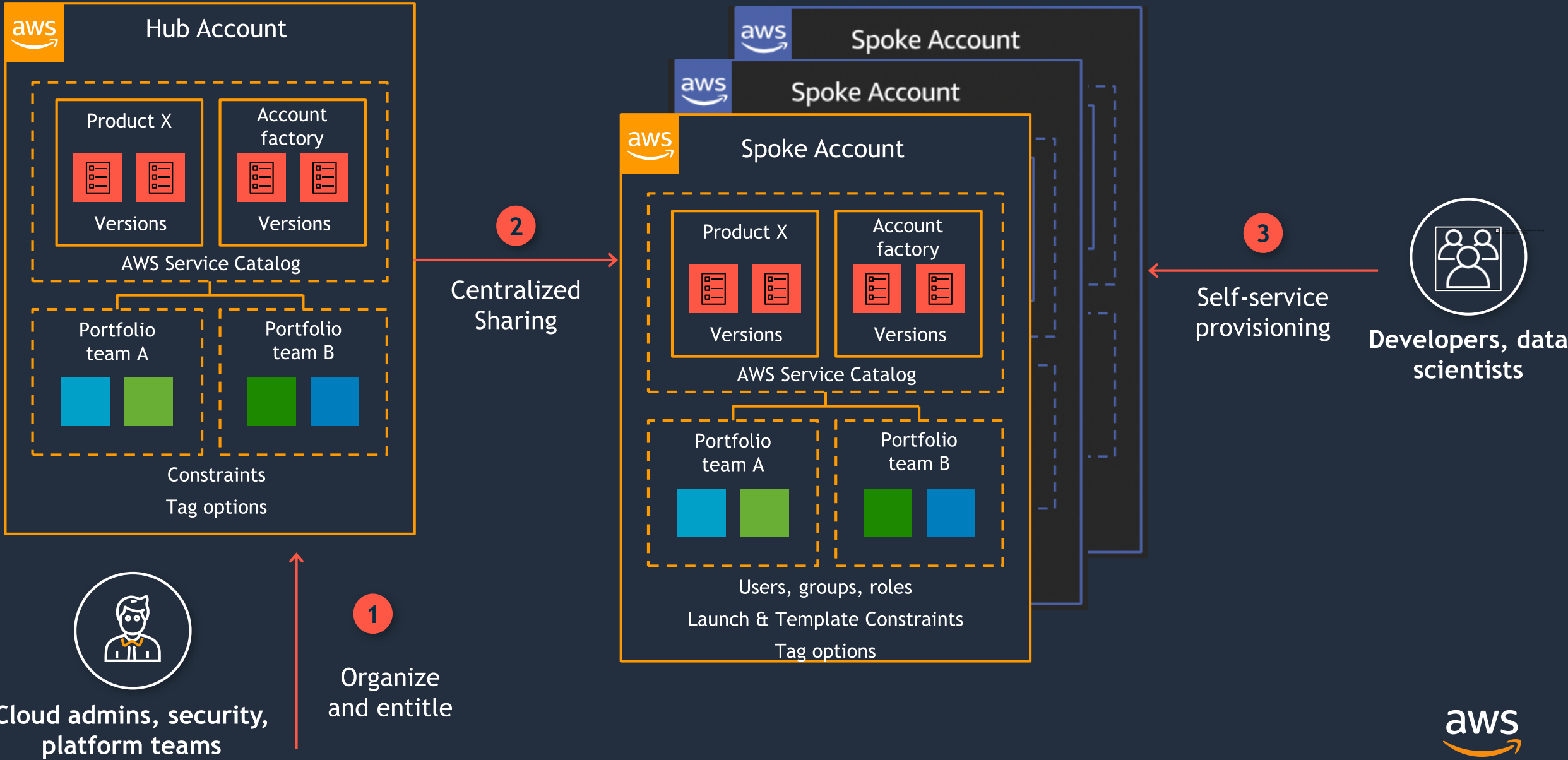


- Built-in account factory provides a template to standardize account provisioning
- Configurable network settings (e.g., subnets, IP addresses)
- Automatic enforcement of account baselines and guardrails
- Published to AWS Service Catalog

Enable self-service with AWS Service Catalog



Automate governance at scale



Operate with agility + control



Dashboard for oversight

The screenshot displays the AWS Control Tower dashboard. At the top, the AWS logo is on the left, and navigation links for Services, Resource Groups, and a search icon are in the center. On the right, there are links for Admin/0490293 @ 423..., Oregon, and Support. A left-hand navigation pane is titled 'AWS Control Tower' and includes sections for Dashboard (Accounts, Organizational units, Guardrails, Users and access), Account factory, and Shared accounts. The main content area is titled 'AWS Control Tower > Dashboard' and features a 'Recommended actions' section. Below this are two summary cards: 'Environment summary' showing 3 Organizational units and 34 Accounts, and 'Guardrail summary' showing 28 Preventive guardrails and 12 Detective guardrails. A 'Noncompliant resources' section contains a table with columns for Resource ID, Resource type, Service, Region, Account name, OU, and Guardrail. The table lists three resources: two EBS volumes and one Security Group. Below this is an 'Organizational units' section with a table showing Name, Parent OU, and Compliance status for Core, Project 1, and Custom OUs. The 'Accounts' section at the bottom has a table with columns for Account name, Account email, Organizational unit, Owner, and Compliance status, and includes a pagination control showing page 1 of 1.

Recommended actions

Environment summary

- 3 Organizational units
- 34 Accounts

Guardrail summary

- 28 Preventive guardrails
- 12 Detective guardrails

Noncompliant resources [Info](#)

Resource ID	Resource type	Service	Region	Account name	OU	Guardrail
vol-842jhdksj83821234	Volume	EC2	us-west-2	db-uswest-1-gamma	Custom	Enable encryption for EBS volumes at
vol-05flia830kd209897	Volume	EC2	us-east-1	testing-beta-1	Project 1	Enable encryption for EBS volumes at
sg-031234b83bac98765	Security Group	EC2	eu-west-1	ops-test-4	Project 1	Disallow internet connection through

Organizational units [Info](#)

Name	Parent OU	Compliance
Core	Root	Compliant
Project 1	Root	Noncompliant
Custom	Root	Noncompliant

Accounts

Account name	Account email	Organizational unit	Owner	Compliance status
--------------	---------------	---------------------	-------	-------------------

< 1 ... >

Disaster Recovery



Disaster recovery benefits of the cloud



Traditional disaster recovery

- Massive upfront & ongoing hardware cost
- Management and infrastructure overhead
- Data growth increases costs
- Separation of test and production environment
- Vulnerable to cyber threats/hacking



DR in the cloud

- Pay as you go for the rightsized compute/storage
- Lower IT overhead
- **More automation**
- **Easy and repeatable testing**
- **Systems up in minutes (not hours/days!)**

Common disaster recovery challenges

- High cost of idle duplicate resources
- Diverse infrastructure and OS types
- Server compatibility issues
- Inability to achieve recovery objectives (RPOs/RTOs)
- Tests and drills are expensive and don't allow us to verify our security posture
- Different DR tools or processes for different applications
- Scaling and securing DR site

AWS Elastic Disaster Recovery use cases



On-premises to AWS



Cloud to AWS



AWS Region to
AWS Region

AWS Elastic Disaster Recovery benefits

Flexible



Replicate from any source



Supports a wide range of OS, applications, and databases



Remove idle recovery site resources and pay only for what you need

Reliable



Robust, non-disruptive continuous replication



RPO: Seconds
RTO: Minutes



Recover from ransomware, corruptions, and human errors

Highly automated



Minimal skill set required to operate



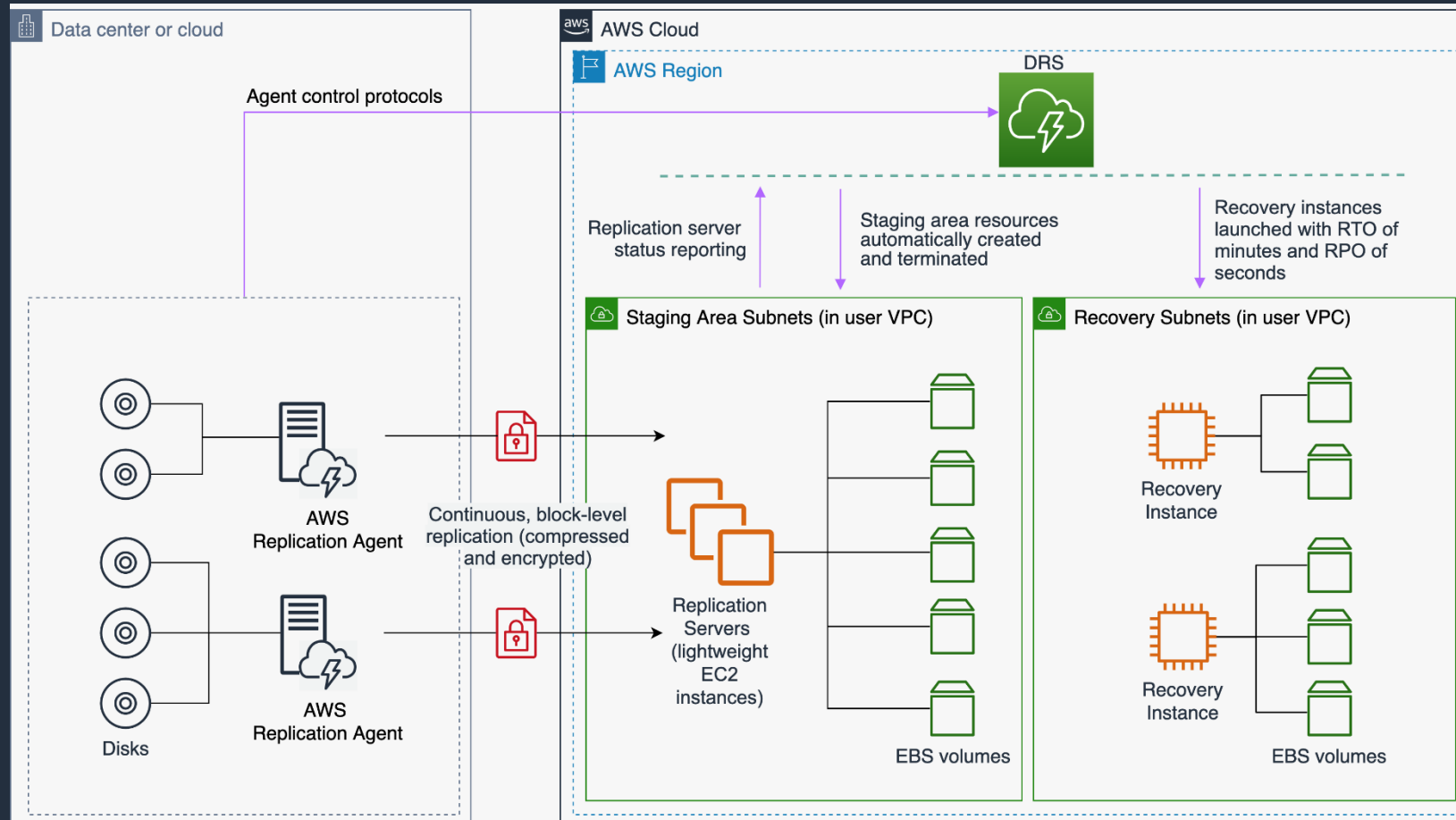
Easy, non-disruptive drills



Unified process to test, recover, and fail back

How AWS Elastic Disaster Recovery works

Continuous replication of on-premises and cloud servers with AWS as your elastic recovery site



Thank you!

brizanm@amazon.com





VITA ISOAG AND ZSCALER DECEPTION

Experience your network, Secured

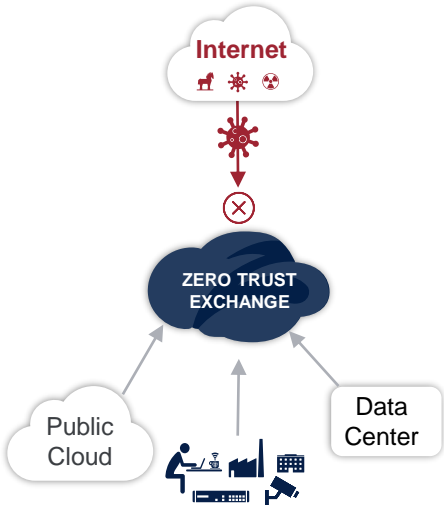
Jeff Spencer
Sales Engineer, Zscaler Deception

July 2022

Zero Trust Security: Cyber Threat Protection

Prevent Compromise

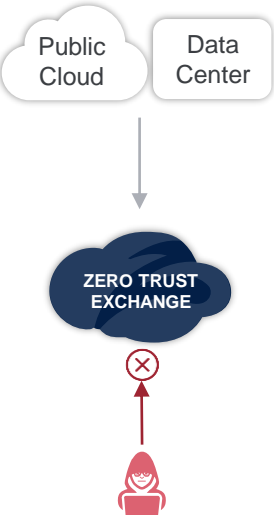
Block threats before they reach you



Protects users, servers, apps, IoT, OT systems

ZIA

Apps invisible to the internet

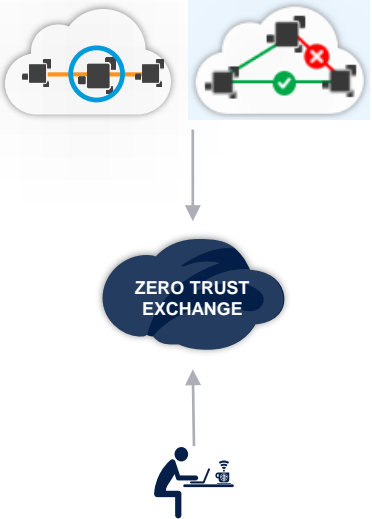


Can't attack what you can't see

ZPA

Prevent Lateral Movement

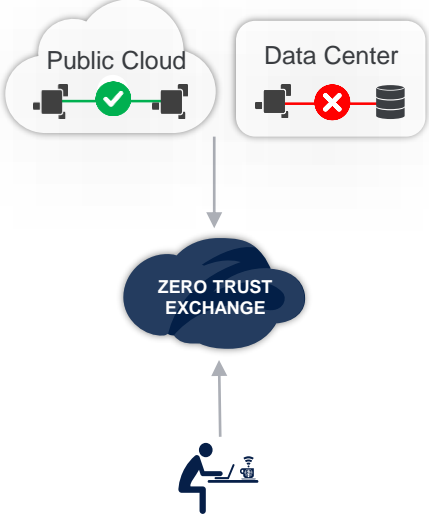
User & App Segmentation



Connects users to apps, not networks

ZPA + ZWS

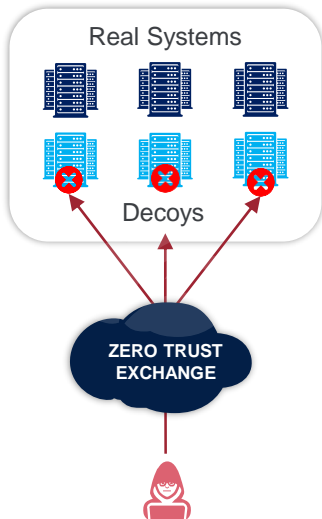
In-line Inspection & Web Isolation



Full In-line inspection of private App traffic, Remote Browser Isolation

ZPA

Decoys detect sophisticated threats



Attackers attempting to move laterally are detected & contained

Deception

What sets Zscaler Cyber Threat Protection apart?

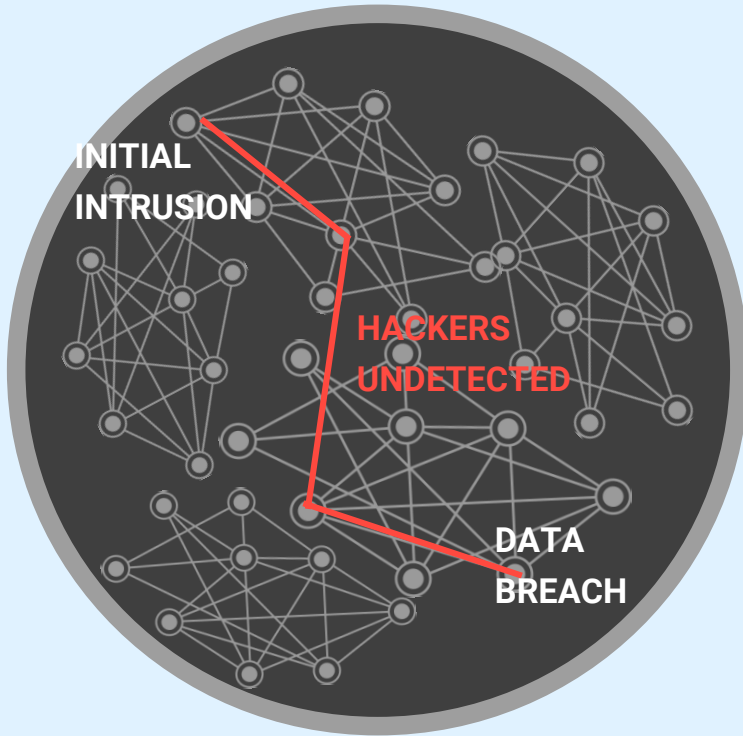
Zero Passthrough Connections

Zero Attack surface

Zero Lateral Movement

The Problem

Sophisticated attackers are stealthy



91% of attacks don't even generate a security alert.

[SOURCE: MANDIANT](#)

Advanced attacks are human-operated

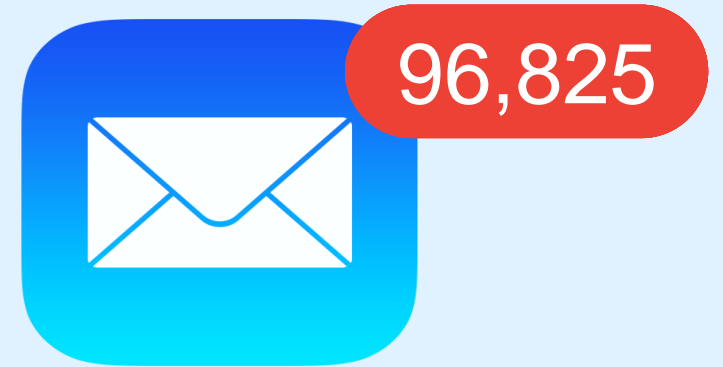


- Use active reconn / discovery
- Clone normal behavior
- Make real-time judgements

68% of attacks are not malware-based.

[SOURCE: CROWDSTRIKE](#)

Security analysts chase ghosts and burn out



Monitoring team faces

- Event fatigue
- Data paralysis
- Missed alerts

45% of alerts are false positives.

[SOURCE: ESG](#)

Current approach puts the burden on the defenders who are stretched thin

Use Cases

Where is Deception being used



What are experts saying

Gartner On Deception

“Prioritize alerts from the deception platforms as high-priority, high-fidelity alerts that need immediate attention.”

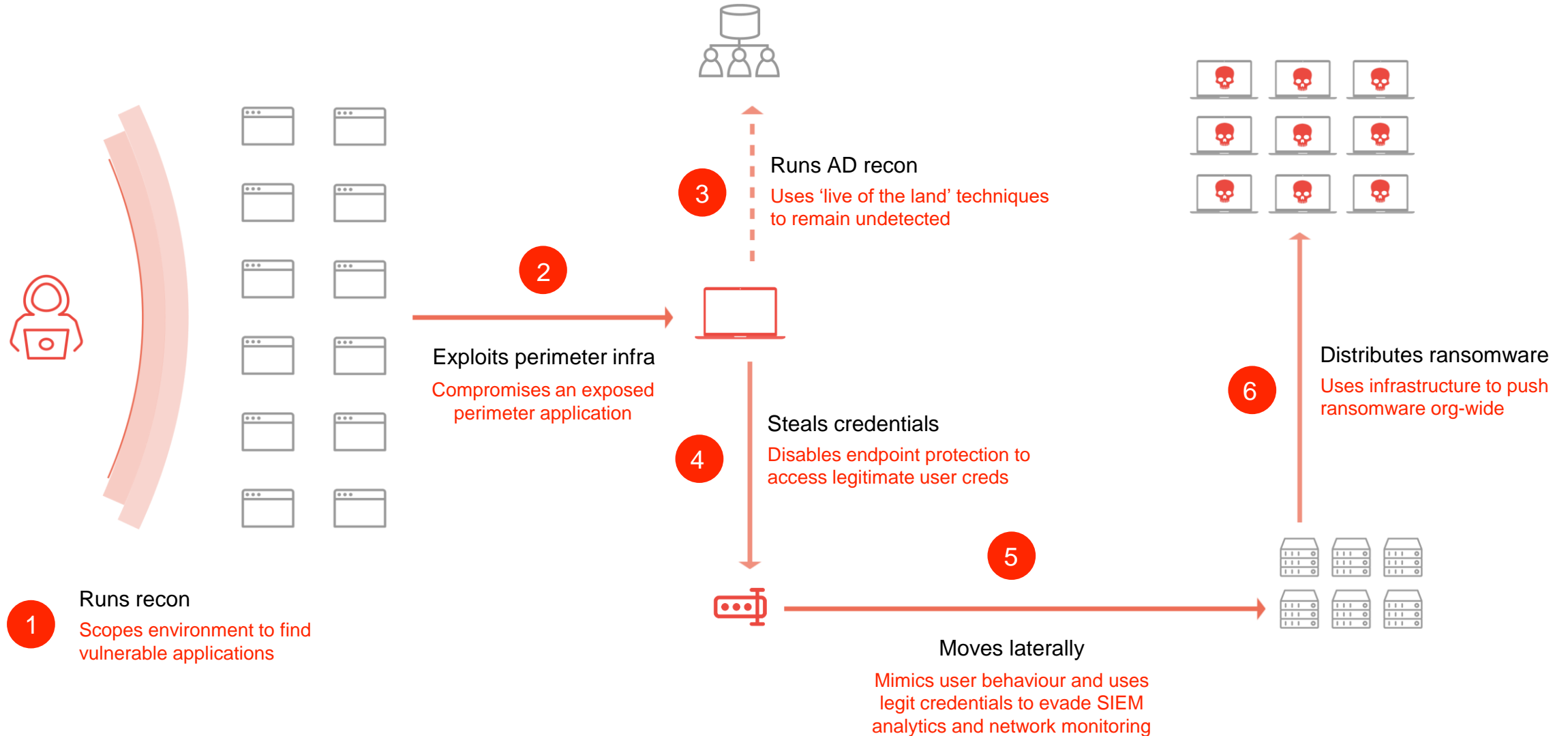
“Security leaders looking to build or expand their threat detection function should include deception tools in their stack.”

MITRE | Engage

Launched Framework for planning adversary engagement, deception and denial activities in order to help execute strategies and technologies

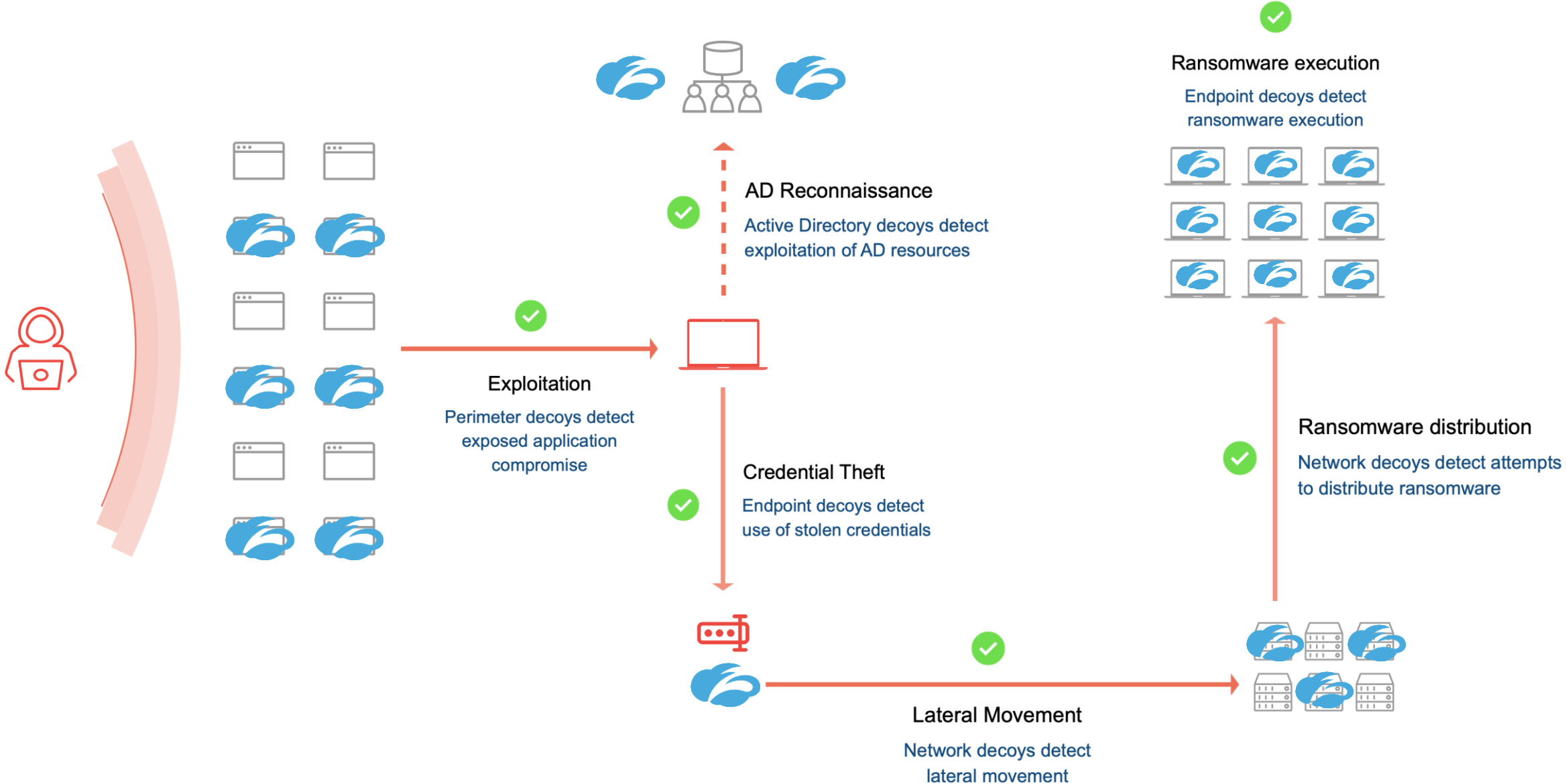
The anatomy of an advanced attack

How and why ransomware succeeds



The anatomy of an adversary engagement

Multiple opportunities to disrupt ransomware with deception technology



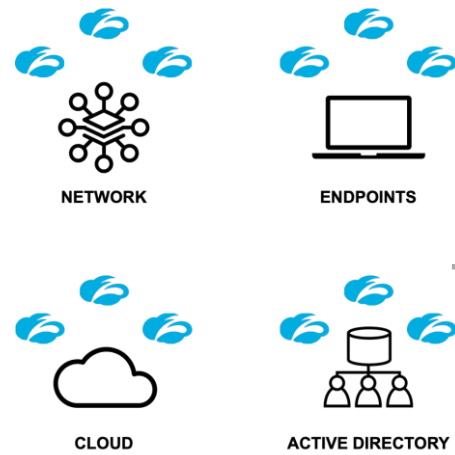
The solution

Zscaler Deception

Configure and Deploy



Detect threats



Investigate



Contain



Case Study : Stopping a targeted attack at a bank

INDUSTRY
Banking

NO. OF ASSETS
40,000+

DECEPTION COVERAGE
Perimeter, DC, DMZ, Active directory



01

Initial intrusion

Attacker gets in through an exposed Cisco router

03

Intelligence gathering

- Attacker spends 9.5 hours jumping from one decoy to the other.
- Zscaler captures attacker activity revealing their toolset and strategy

05

Active Defense

The location with the compromised endpoint is ring-fenced with decoys to shore up defenses

02

First Detection

The Cisco router is a Zscaler decoy and detects the attacker

04

Investigation

SOC correlates Zscaler intelligence with event logs and find that the attacker had compromised an endpoint in another part of the network.

06

Threat neutralized

Compromised endpoint is isolated and attacker is ejected from the network by cutting off CnC

Why Zscaler Deception

Benefits of integrated Deception and Adversary Engagement

+167%

Average increase in 'Opportunity to Detect' advanced attacks like ransomware

+50%

Average increase visibility for targeted threats not found in threat intel feeds

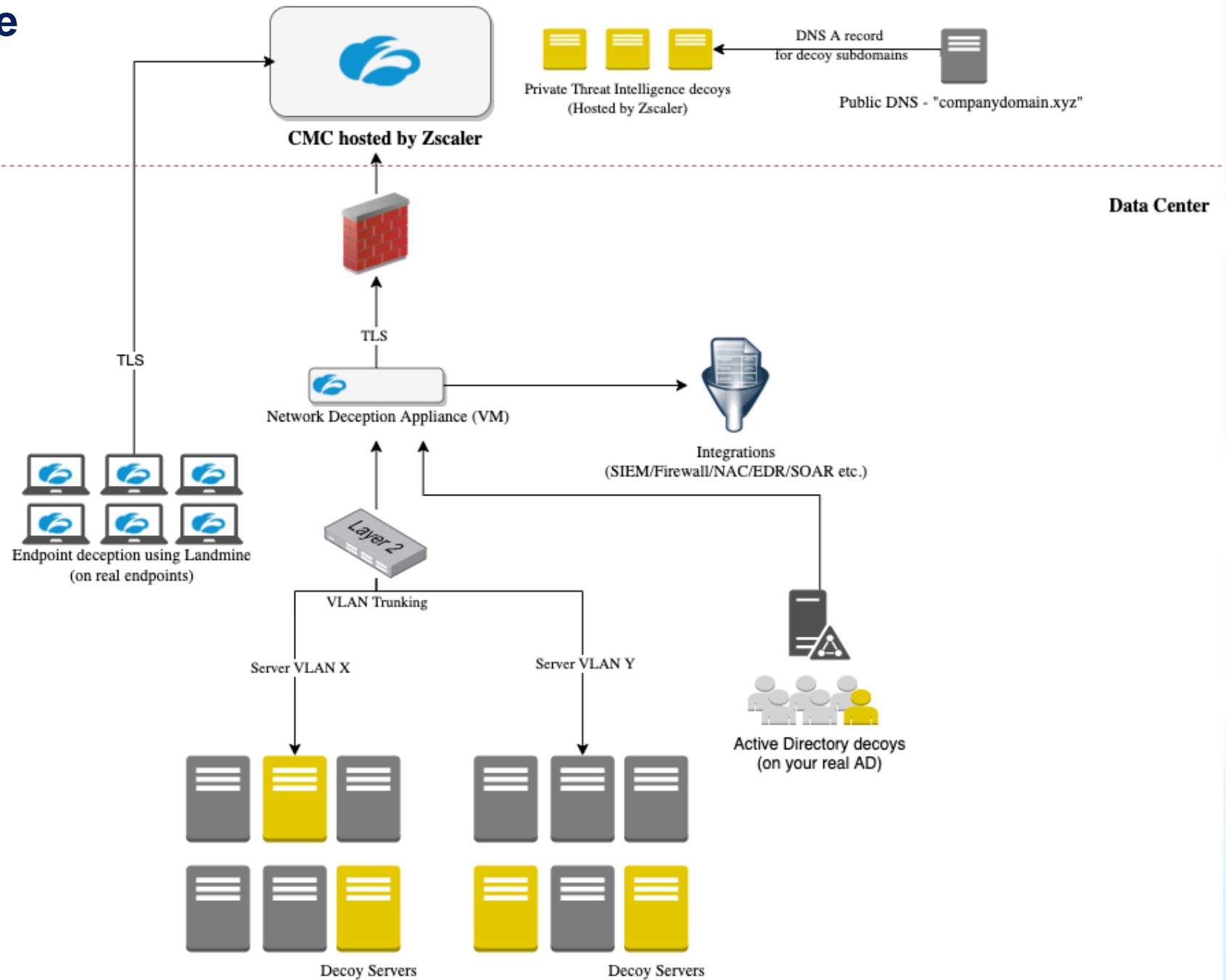
+90%

Average improvement in ability to detect an advanced threat in the early stages of an attack

98%

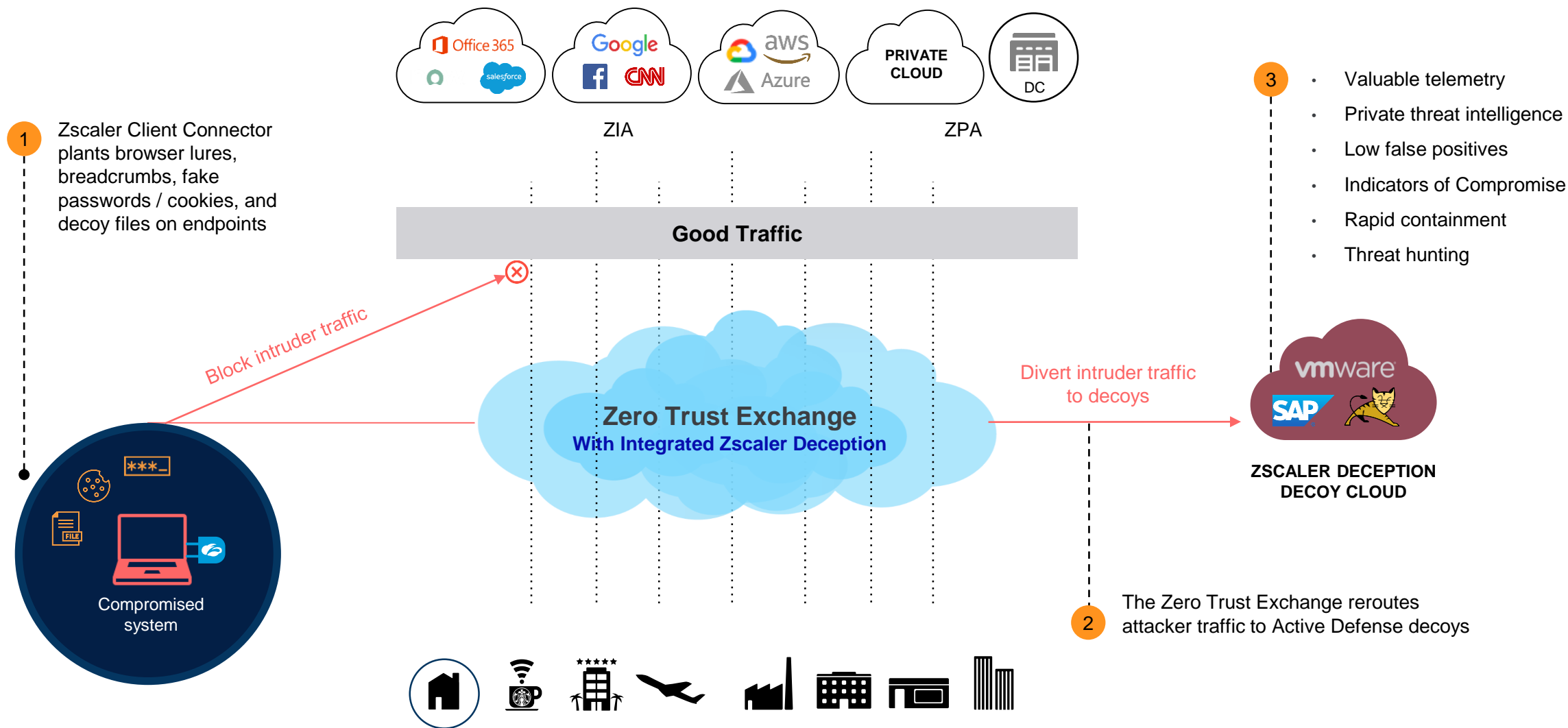
Average lesser alert volume than traditional detection controls

Detailed Architecture

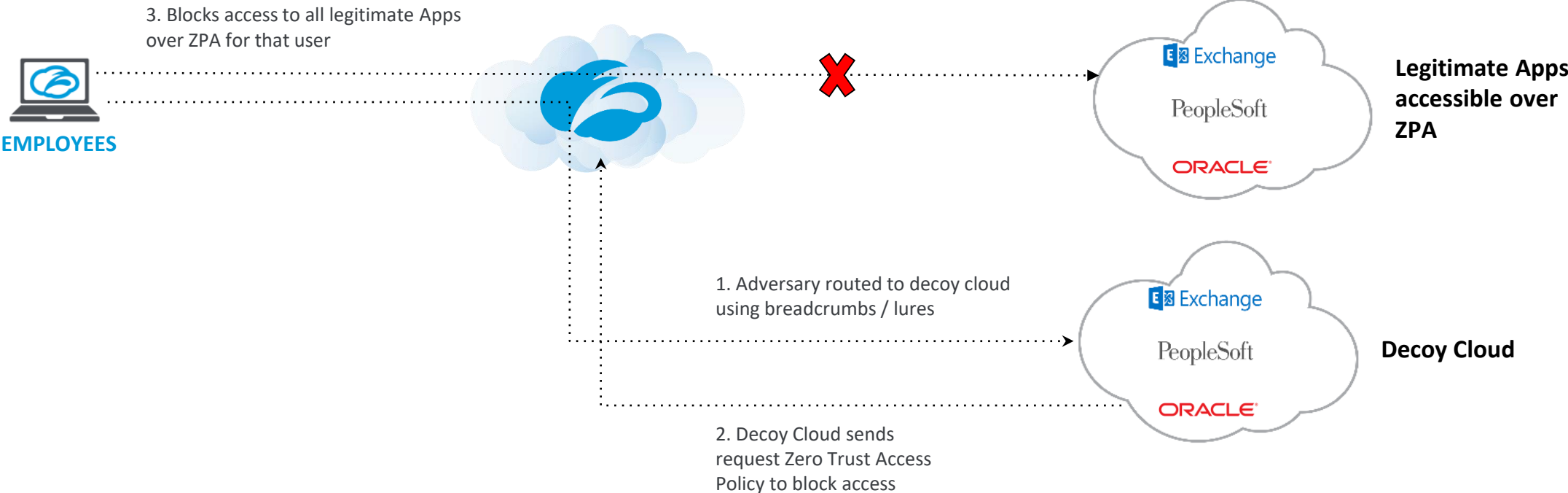


The future of targeted threat detection

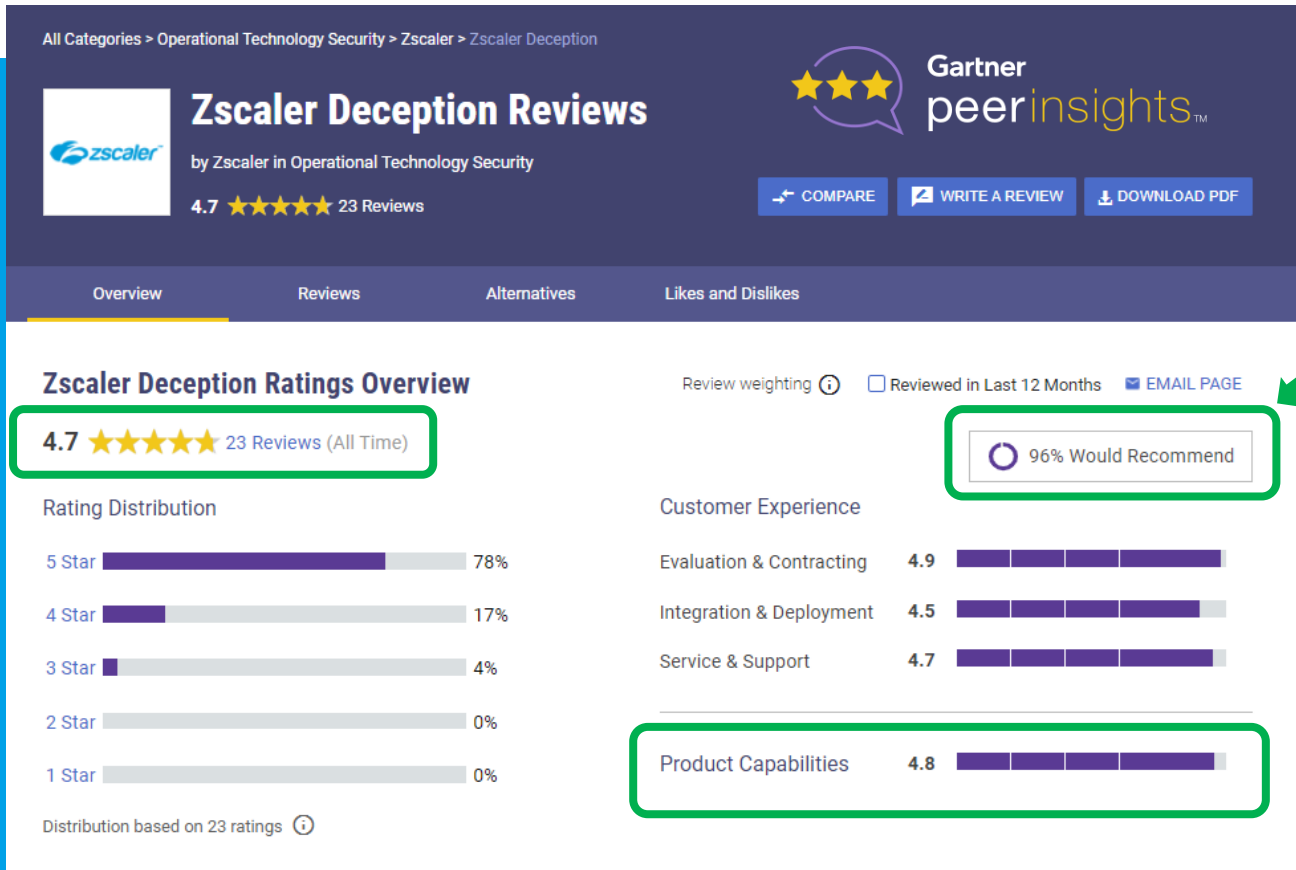
Zero Trust + Zscaler Deception



Use cases - Native containment



Gartner Peer Insights



“My team showed our findings, very impressive. Lets talk numbers” - CIO LoanDepot

“One of the best products that I have evaluated in recent memory” - CISO Waste Connections

“the last 7 days for my Incident responders have been transformative” - Mgr ITSec

“We caught the Red-Team in our audit, seems like this does work” - CISO of Bank

Operationalize your MITRE ENGAGE Framework

Zscaler Deception provides coverage for 99% capabilities for strategic deception and denial activities

PREPARE	EXPOSE		AFFECT			ELICIT		UNDERSTAND
Planning	Collection	Detection	Prevention	Direction	Disruption	Reassurance	Motivation	Analysis
Define Exit Criteria	API Monitoring	Decoy Artifacts and systems	Baseline	Decoy Artifacts and systems	Decoy Artifacts and systems	Application Diversity	Application Diversity	Distill Intelligence
Develop Threat Model	Network Monitoring	Detonate Malware	Hardware Manipulation	Detonate Malware	Isolation	Artifact Diversity	Artifact Diversity	Hotwash
Persona Creation	Software Manipulation	Network Analysis	Isolation	Email Manipulation	Network Manipulation	Burn-In	Detonate Malware	Inform Threat Model
Strategic Goal	System Activity Monitoring		Network Manipulation	Migrate Attack Vector	Software Manipulation	Email Manipulation	Information Manipulation	Redefine Operation Activities
Storyboarding			Security Controls	Network Manipulation		Information Manipulation	Personas	
				Peripheral Management		Network Diversity	Network Diversity	
				Security Controls		Peripheral Management		
				Software Manipulation		Pocket Litter		

 Coverage VIA On-boarding Training and services
 Out-of-the-box Solution Capabilities
 Use case not covered

Extensive built-in Decoys

APPLICATION DECOYS

LATERAL MOVEMENT

Detect lateral movement with decoys for SSH sessions, database client connections, and saved shares / mapped network drives.

ACTIVE DIRECTORY DECOYS

PRIVILEGE ESCALATION

Create deception in the Active Directory (AD). Smokescreen does this by using the real AD instead of a dummy AD / trust relationship.

PERIMETER THREAT INTELLIGENCE DECOYS

RECONNAISSANCE

Detects pre-attack reconnaissance activity against internet facing architecture to give provide intelligence about external attacks.

- ✓ **FULL KILL-CHAIN COVERAGE**
- ✓ **CUSTOMIZE DECOYS W/ VM IMAGES, DOCKER CONTAINERS**
- ✓ **ATTAIN REALISM USING KEYWORDS, NAMING CONVENTIONS ETC**

EMAIL DECOYS

EXPLOITATION

Email decoys that engage with attackers attempting to mount social-engineering / spear-phishing attacks on high-value personnel.

CLOUD DECOYS

LATERAL MOVEMENT

Decoy IAM credentials and S3 buckets that detect lateral movement in your Cloud environment.

FILE DECOYS

DATA THEFT

Auto generated file decoys with custom content, file names, and format that trigger when a file is opened, accessed, copied, or deleted.

CREDENTIAL DECOYS

PRIVILEGE ESCALATION

Inject fake credentials in credential managers, RDPs, and browsers that act as breadcrumbs to lure attackers.

MAN IN THE MIDDLE DETECTION

EXPLOITATION

Detect Man-in-the-Middle attacks for protocols like LLMNR, mDNS, and NBT-NS by identifying the spoofer.

PROCESS DECOYS

PRIVILEGE ESCALATION

Fake anti-malware / DLP processes that detect attackers when they try to disable them.

Thank you!



**NATIONAL
CYBERSECURITY
ALLIANCE**

How to Get Involved in Cybersecurity Awareness Month 2022

22 June 2022



What is Cybersecurity Awareness Month?

- Month of October
- Launched in 2004
- Co-lead by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Security Alliance
- Raises awareness about digital security and empower everyone to protect their personal data from digital forms of crime.

Overall Campaign



2022 Themes:

It's Easy to Stay Safe Online

Messaging

- Five Broad Campaign Topics –
 1. Cybersecurity Starts with You
 - Top priorities for collective responsibility
 2. Update Your Software
 - Prevent Malware Attacks
 3. Enable Multi-Factor Authentication
 - Create extra barriers against Threat Actors
 4. Use Trusted Password Management and Strong Passwords
 - Protect your Personally Identifiable Information
 5. Recognize and Report Phishing Attacks
 - Don't become a victim to cyber crimes





Overall Campaign

This year's focus are on four key behaviors instead of weekly themes

Topics covered:

- Enabling multi-factor authentication
- Using strong passwords and a password manager
- Updating software
- Recognizing and reporting phishing

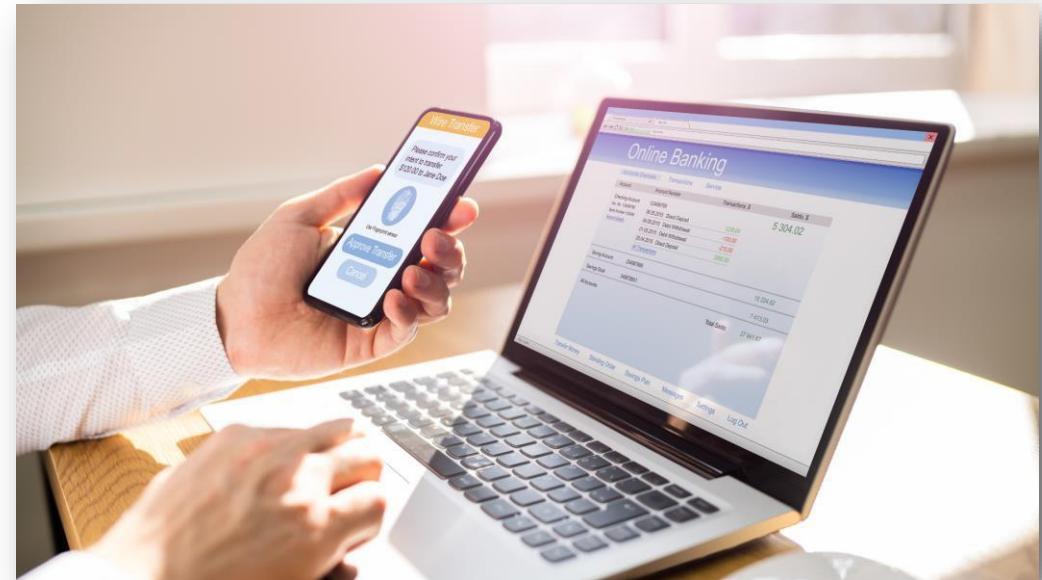


Overall Campaign

Enabling Multi-Factor Authentication

Topics covered:

- What is MFA
- Why is it important
- How does it work
- What does it look like
- What type of accounts offer MFA





Overall Campaign

Using Strong Passwords and Password Managers

Topics covered:

- What makes a strong password
- What is a password manager
- Why use a password manager
- Dispelling the myths that password managers are unsafe
- How to choose a password manager





Overall Campaign

Updating your Software

Topics covered:

- Why it's important
- When to update
- Setting automatic updates
- Avoiding fakes





Overall Campaign

Recognizing and Reporting Phishing

Topics covered:

- How to spot a phish on emails, texts or over the phone
- What to do if you spot a phish
- How to report a phish



Resources





Become a Champion

- **Show your support for Cybersecurity Awareness Month**
- **Champions represent those dedicated to promoting a safer, more secure and more trusted internet**
- **Becoming a Champion is easy and free**

<https://staysafeonline.org/programs/cybersecurity-champion/>



Become a Champion

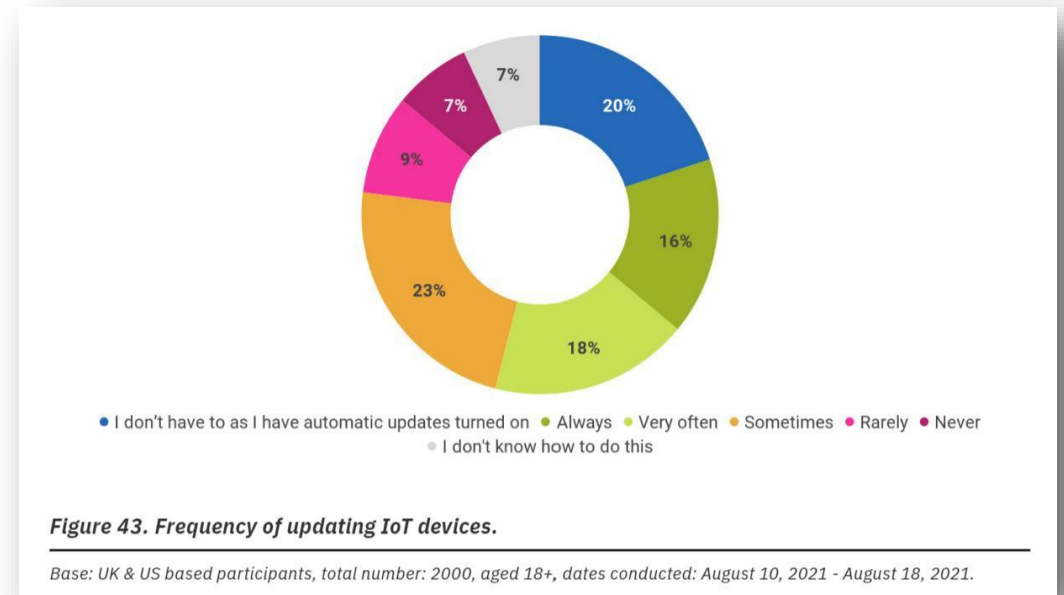
- Receive a **toolkit of materials exclusively for registered Champions**
- Organizations: Get your company name listed on staysafeonline.org
- Be among the **first to receive updates** on Cybersecurity Awareness Month news, events and materials



Resources

Snapshot of 2021's Findings:

- **Nearly half** of people surveyed say they have never heard of MFA.
- **47% of people** never or rarely use different passwords for their accounts
- **31% of people** keep track of their passwords by writing them down in a notebook
- **31%** say they either “sometimes,” “rarely,” or “never” install software updates.



Ways to Get Involved

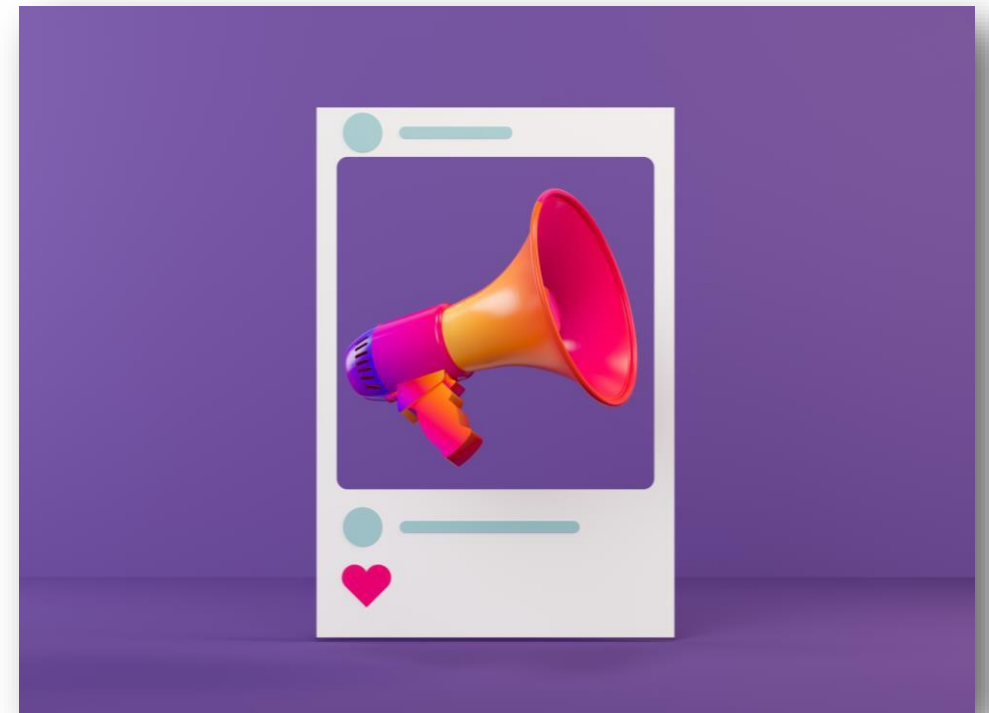




Ways to Get Involved

Online

- Join the conversation on social media using **#BeCyberSmart** and **#CybersecurityAwarenessMonth**
- Share the sample social media posts and graphics
- Add the logo to your website for the duration of October
- Blog about cybersecurity





Ways to Get Involved

At Work

- Send emails to employees/customers with educational materials or highlight your organization's activities
- Issue a company promotion related to the month such as a product discount or giveaway
- Mention Cybersecurity Awareness Month in your resources and materials
- Hold a contest for employees/students



Step 1: Train Your Staff

- Create a presentation for all staff; involve your IT staff if available, and include:
 - What's In It For Me (WIIFM)? Why cybersecurity is important for everyone
 - Teach cybersecurity basics; be proactive with materials and messaging
 - Share consistent information to promote action
- Follow up with employees regularly to confirm behavior integration and measure comprehension of training materials
- Explore training opportunities workforce development opportunities via National Initiative for Cybersecurity Careers and Studies
 - Interactive [Training and Education Catalog](#)
 - [Cybersecurity Career Pathways Tool](#)



Events





Hosting an Event or Training

- Identify your audience and the behavior you want to change/influence
- Keep the learning experience lighthearted, fun, relatable and interactive
- Include games/ giveaways
- Show buy-in from the C-suite
- Invite an outside speaker



Request a CISA Cybersecurity Speaker

**Interested in inviting an outside speaker for your
Cybersecurity Awareness Month events?**

Request a CISA speaker to discuss cybersecurity at your cybersecurity awareness month campaign event, by sending an email to CISA.speakers@cisa.dhs.gov or downloading the CISA Speaker Request Form at www.cisa.gov/request-cisa-speaker

Deadline: August 26, 2022.





Events

Request an NCA Speaker

<https://staysafeonline.org/contact-us/>

CONTACT US

Our goal is to make sure you have everything you need to feel safer and more secure online.

So let us know how we can help you. Or let us know if you're interested in helping us in our mission.

Fill out the form and someone will reach out to you.

We know how important cybersecurity is, so we will do our best to contact you as soon as we can.

Email*

First Name*

Last Name*

Anything else you'd like to add**

Submit



Events

Save the dates

- October 6: Cybersecurity America: A United Mission
- October 12: #BeCyberSmart Twitter Chat
- November 2: Afterglow Party

Share your event!

info@staysafeonline.org

NATIONAL CYBERSECURITY ALLIANCE

The screenshot displays the 'UPCOMING EVENTS' section of the National Cybersecurity Alliance website. It features a dark background with white and blue text. The main event highlighted is 'How To Get Involved In Cybersecurity Awareness Month 2022', which is a virtual webinar on Wednesday, June 22, 2022, at 2 PM ET / 11 AM PT. Below this, there are three partner events: 'RSA Conference' (June 6-9, 2022, San Francisco), 'SANS Security Awareness Summit & Training 2022' (August 3, 2022, Austin, TX), and 'InfoSec World' (September 26, 2022, Lake Buena Vista, Florida). Each event card includes a small image, a title, a brief description, the date and location, and a 'Learn more' button. A 'View all events' button is also present at the bottom left of the main event card.

UPCOMING EVENTS

OUR EVENTS

How To Get Involved In
Cybersecurity Awareness Month 2022

Join The Webinar
Wednesday, June 22
2PM ET/ 11AM PT

How to Get Involved in Cybersecurity Awareness Month 2022

Want to learn more about how you or your organization can get involved in Cybersecurity Awareness Month 2022? Take an in-depth dive into the campaign during this special webinar presented by the National Cybersecurity Alliance. We'll provide an overview of the new theme, review materials in this year's toolkit and share tips and advice for launching your own initiatives!

June 22, 2022 • Virtual

View all events

Learn more

PARTNER EVENTS

RSA Conference

Join your peers at RSAC 2022 in San Francisco, June 6-9, or digitally. Attend expert-led sessions, inspiring Keynotes, innovation programs, and much more.

June 6-9, 2022 • San Francisco

Learn more

SANS Security Awareness Summit & Training 2022

Summit: August 3-4
Training: August 1-2 & August 8-13
Austin, TX & Live Online

Managing Human Risk

Join us for the 9th annual SANS Security Awareness Summit to learn, connect, and share with thousands of fellow security awareness and culture professionals from around the world.

August 3, 2022 • Austin, TX

Learn more

InfoSec World

This leading cybersecurity conference for security practitioners and executives features expert insights, enlightening keynotes, and interactive breakout sessions that inform, engage, and connect the infosec community.

September 26, 2022 • Lake Buena Vista, Florida

Register now

VIEW ALL EVENTS →

Cybersecurity Awareness Month



Additional Resources

Cybersecurity Awareness Month

<https://staysafeonline.org/programs/cybersecurity-awareness-month/>

StaySafeOnline.org

<https://staysafeonline.org/>

Education Videos and Webinars:

<https://www.youtube.com/user/StaySafeOnline1>



For more information:

cisa.gov

**Cisa.gov/cybersecurity-awareness-
month**

cyberawareness@cisa.dhs.gov

Stay safe online.



**NATIONAL
CYBERSECURITY
ALLIANCE**

Website
StaySafeOnline.org

Twitter
[@staysafeonline](https://twitter.com/staysafeonline)

Facebook
[/staysafeonline](https://www.facebook.com/staysafeonline)

LinkedIn
[/national-cyber-security-alliance](https://www.linkedin.com/company/national-cyber-security-alliance)

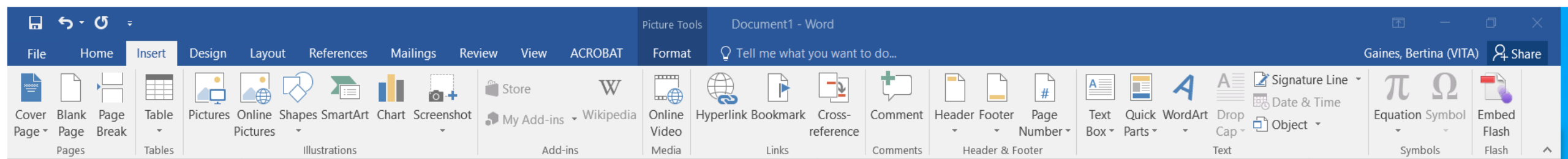
Email
info@staysafeonline.org



- Governor's Proclamation
- 2023 Kids Safe Online Poster Contest
- If you are scheduling any events, please let VITA know so we can post them to our website as well as our social media platform



- 2022 agency training should have started. 2022 training must be completed by Dec. 31, 2022. 2022 compliance forms are due to VITA Jan. 31, 2023.
- Minor definition changes have been made so SEC527. More information will be forthcoming. If you have any suggestions/comments to SEC527, let us know.
- Agency Compliance Form has been updated and will be updated in Archer and in SEC527.
- Please submit your 2022 training solution form to VITA by 9/30/2022. This can be entered in Archer or a paper copy may be submitted.



Commonwealth Security and Risk | <https://itgrcs.vita.virginia.gov/apps/ArcherApp/Home.aspx>

VIRGINIA IT AGENCY ENTERPRISE GOVERNANCE RISK and COMPLIANCE

Search [] Tina

Executive Workspace | Risk Management | Enterprise Management | Task Management | Threat Management | CSRM Analyst Workspace | Reports

Agency : Virginia Information Technologies Agency

EDIT VIEW

First Published: 8/6/2013 8:43 AM Last Updated: 7/28/2022 12:40 PM

ABOUT

NATIONWIDE CYBER SECURITY REVIEW 2020

Questionnaire ID: [583857](#)

SECURITY AWARENESS TRAINING QUESTIONNAIRE Add New

Questionnaire ID	Year
601854	2021
2531555	2022
3207842	2023

GENERAL INFORMATION

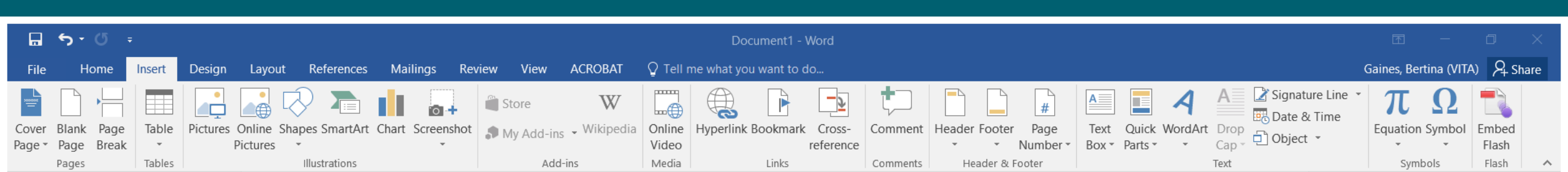
Agency Name: Virginia Information Technologies Agency Agency Acronym: VITA

Web Site: <http://www.vita.virginia.gov> Partnership Full Service Yes Customer:

Agency Number: 136 Number of Employees:

Agency Secretariat: Administration Government Branch: Executive

POWERED BY ARCHER Version 6.11 P2



Commonwealth Security and Risk Management | Content | Commonwealth Security and Risk Management | Service Catalog - VITA

https://itgrcs.vita.virginia.gov/apps/ArcherApp/Home.aspx?workspaceId=-1&requestUrl=-.%2fGenericContent%2fRecord.aspx%3fid%3d2124824%26moduleId%3d409#

VIRGINIA IT AGENCY ENTERPRISE GOVERNANCE RISK and COMPLIANCE

Search

Executive Workspace | Risk Management | Enterprise Management | Task Management | Threat Management | CSRM Analyst Workspace | Reports

Security Awareness Training Questionnaire : 3207842

EDIT VIEW

Created Date: 7/28/2022 12:41 PM Last Updated: 7/28/2022 12:42 PM

0 of 26 Completed

Record 3 of 3

Year: 2023 Agency: [Virginia Information Technologies Agency](#)

Planned Training Solutions

▼ PLANNING STATUS

Plan Submission Status:	Plan Review Status:
Plan Submission Date:	Plan Review Date:

▼ CURRICULUM REQUIREMENTS

Core Requirements: Indicate which solution your agency will be using in order to fulfill the core requirements for training.

▼ POLICY REVIEW AND ACCEPTANCE

Acceptable Use Policy: Indicate which solution your agency will be using in order to provide acceptable use policy training.

Remote Access Policy: Indicate which solution your agency will be using in order to provide remote access policy training.

All Other Applicable Policies: Indicate which solution your agency will be using in order to provide any other applicable policy training.

▼ ROLE BASED TRAINING

File Home Insert Design Layout References Mailings Review View ACROBAT Tell me what you want to do...

Clipboard Font Paragraph Styles Editing

Times-Romar 12 A A Aa A

B I U abc X₂ X² A ab A

AaBbCc AaBbCcI AaBbCcI AaBbCcI AaB AaBbCcD AaBbCcD AaBbCcD AaBbCcD AaBbCcD AaBbCcD AaBbCcD AaBbCcI

Heading 1 1 Normal 1 No Spac... Heading 2 Title Subtitle Subtle Em... Emphasis Intense E... Strong Quote

Find Replace Select



	<i>Payment Card Information (PCI)</i>								
	<i>Personal Health Information (PHI)</i>								
E	Phishing Exercise (required)								
F	Additional Training (optional)								

Identify Training Solution: please mark your agency's proposed solution to meet the training requirements identified in A, B, C and D.

*Other Software: If you are planning to use a software solution other than: Infosec / KnowB4 / SANS / Awareity / Security Mentor, please indicate it here. The use of any other training solution must be approved in advance.

QUESTIONS





UPCOMING EVENTS



- Audit was completed June 23, 2022
- It's published on the OSIG website:
 - <https://www.osig.virginia.gov/reports/#PerformanceAuditServicesReports>
- SCOPE: The scope of this review included an examination of information technology assets used by executive branch agencies to ensure that agencies and contractors sanitize Commonwealth of Virginia (COV) data as required by Virginia Information Technologies Agency (VITA) Information Technology Resource Management standards and best practices.



STATE INSPECTOR GENERAL AUDIT

FINDING 1:

Agency Internal Policies Did Not Fully Document Removal or Destruction in Accordance with COV Standards



STATE INSPECTOR GENERAL AUDIT

OSIG RECOMMENDATION:

Communicate to agencies to include in their annual risk assessment that their internal policies and procedures clearly address SEC501, SEC514-05 data removal requirements and ITRM Standard 514.



Communicate to agencies to include in their annual risk assessment that their internal policies and procedures clearly address SEC501, SEC514-05 data removal requirements and ITRM Standard 514.

All agencies must assure that your agency’s internal policies and procedures directly reference and align with the data removal requirements in *SEC 501 Information Security Standard and SEC 514 Removal of Commonwealth Data from Electronic Media Standard*.

This is already required in SEC501 MP-1 (media protection family)



Communicate to agencies to include in their annual risk assessment that their internal policies and procedures clearly address SEC501, SEC514-05 data removal requirements and ITRM Standard 514.

Additionally, when conducting IT risk assessments for your agency, a review of your agency’s internal policies should be included and any deficiencies should be documented for remediation.

Thank you!

REGISTRATION IS OPEN

148

2022 COMMONWEALTH VIRTUAL INFORMATION SECURITY CONFERENCE - AUG. 18, 2022

[HTTPS://WWW.VITA.VIRGINIA.GOV/INFORMATION-SECURITY/SECURITY-CONFERENCE/](https://www.vita.virginia.gov/information-security/security-conference/)



COMMONWEALTH OF VIRGINIA

INFORMATION SECURITY CONFERENCE

2022

VIRTUALLY, NOTHING IS IMPOSSIBLE:
SECURING THE HYBRID WORK ENVIRONMENT





Commonwealth of Virginia Innovative Technology Symposium
(COVITS)! Sept. 7, 2022

Location:

Greater Richmond Convention Center

403 N 3rd Street

Richmond, VA 23219

Register is now open:

[COVITS 2022 - LIVE! \(govtech.com\)](https://govtech.com)



The next ISOAG meeting will be held on:

Sept. 14, 2022 @ 1 p.m.

Presenters:

Brandon Lapetina – Varonis

Erin Mosely/Steve Orrin – Intel

David Ihrle – Virginia Innovation Partnership Corporation



IS Orientation

Remote - WebEx

Sept. 29, 2022

Start time: 1:00 p.m.

End time: 3:00 p.m.

Instructor: Marlon Cole

<https://covaconf.webex.com/covaconf/onstage/g.php?MTID=ecbe083f9321db08a0c81eca667f50575>



The next scheduled meeting for the IS Council:

Sept. 21, 2022

12 p.m. – 1 p.m. via Webex

If you would like an invite to the meeting, contact:

tina.gaines@vita.virginia.gov

MEETING ADJOURNED

