aws marketplace

How to prioritize security controls for sensitive AWS assets

Today's speakers

Sounil Yu
Creator of the Cyber Defense Matrix

Josh Thurston
Sr. Category Lead, Security at AWS

Sagar Khasnis
Partner Solutions Architect at AWS

Today’s Agenda

- Cloud opportunities and considerations
- Tools that can help protect your sensitive assets
- How to apply these tools to manage “pets” and to design for “cattle”
- Mapping capabilities to requirements
- Relevant AWS services and solutions in AWS Marketplace
- Customer success stories

Managing the Security of Your Pets and Cattle in the Cloud

SOUNIL YU

AWS provides a fundamentally different model for how we can build and operate IT infrastructure and applications, but we need to be mindful of new security considerations

Opportunities		Considerations
Everything is highly configurable	→	More room for configuration errors
Wide array of discrete services can be mixed and matched	→	Cloud sprawl with many more individual resources that need to be tracked
Consolidated environments provides unified API enabling easier management and economies of scale	→	Erosion of network perimeter and network centric boundaries

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

These considerations require approaches that adapt to this new operating model and can scale

Considerations	Approach
More room for configuration errors	Prevent misconfigurations at scale
Cloud sprawl with many more individual resources that need to be tracked	Automatically discover cloud misconfigurations and exploits against them
Erosion of network perimeter and network centric boundaries	Enable rapid remediation of any discovered misconfiguration

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

Sponsored by: aws marketplace

SOUNIL YU

@sounilyu

These risks can be addressed through native AWS capabilities and through AWS Marketplace vendors

AWS Native

(non-exhaustive)

- Amazon GuardDuty
- Amazon Macie
- AWS WAF
- AWS Shield
- AWS IAM
- AWS Secrets Manager
- AWS CloudTrail
- AWS Systems Manager
- Amazon Inspector
- AWS CloudHSM
- Amazon CloudWatch
- AWS Config
- AWS KMS
- AWS Security Hub
- Amazon Detective
- AWS Trusted Advisor

AWS Marketplace

(non-exhaustive)

- TREND MICRO
- DIGITAL GUARDIAN
- paloalto NETWORKS
- sysdig
- SOPHOS Cloud Optix
- tenable
- aqua
- bitglass Next-Gen CASB
- alcide
- DivvyCloud
- netskope
- Check Point SOFTWARE TECHNOLOGIES LTD.
- StackRox
- RAPID7

Sponsored by: aws marketplace

SOUNIL YU

@sounilyu

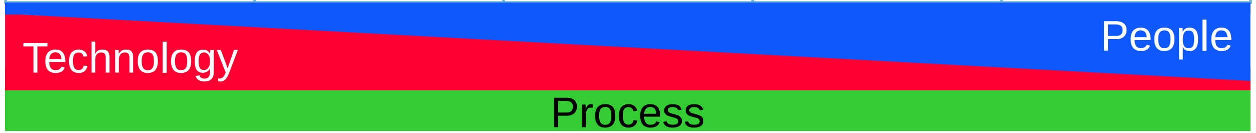
*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

The Cyber Defense Matrix is an adaptation of the CSF

https://cyberdefensematrix.com

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

Degree of Dependency



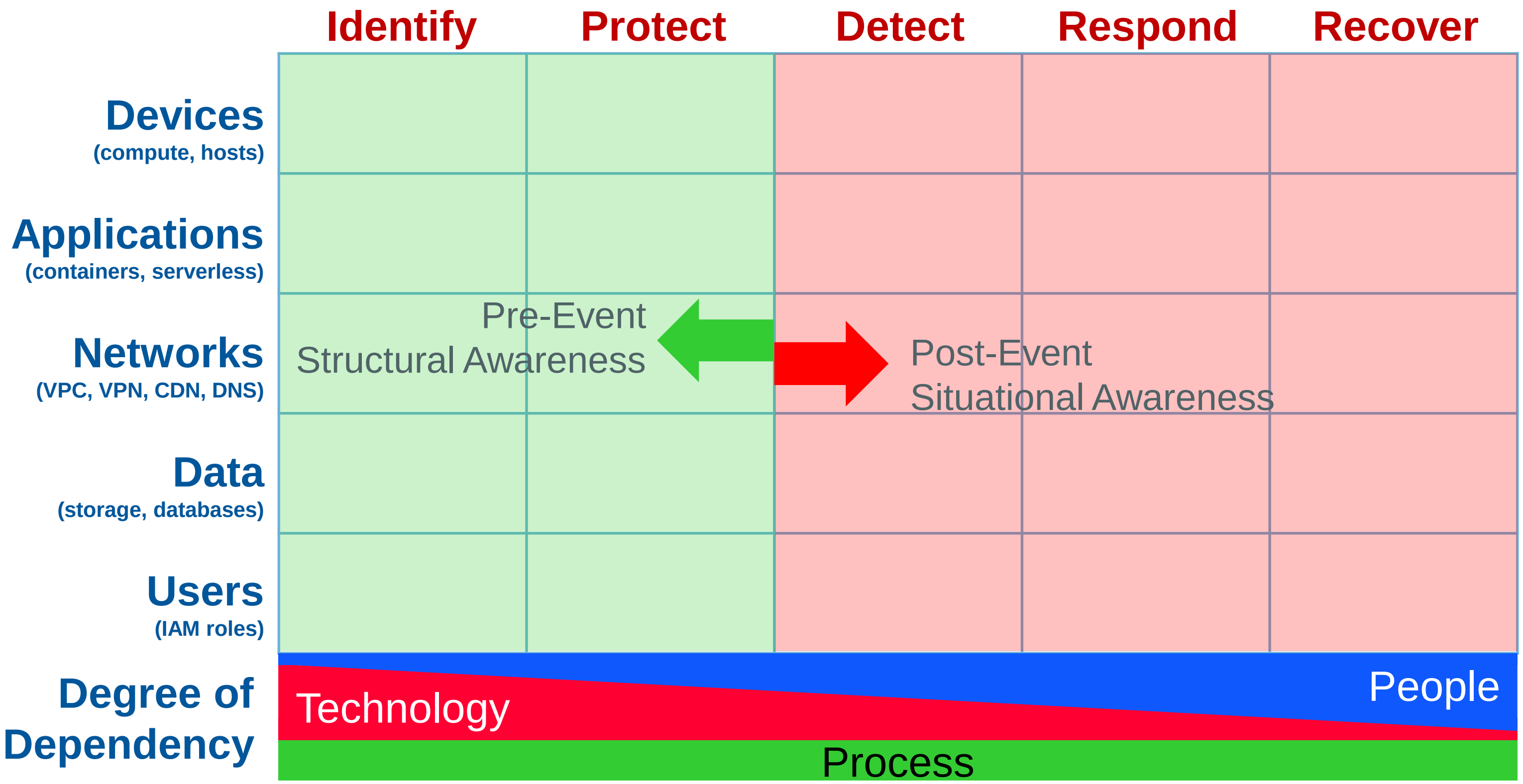
Sponsored by: aws marketplace

SOUNIL YU

@sounilyu

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

This webinar will focus on cloud security on the left of boom



	Identify	Protect	Detect	Respond	Recover
Devices (compute, hosts)	🟩	🟩	🟥	🟥	🟥
Applications (containers, serverless)	🟩	🟩	🟥	🟥	🟥
Networks (VPC, VPN, CDN, DNS)	🟩	🟩	🟥	🟥	🟥
Data (storage, databases)	🟩	🟩	🟥	🟥	🟥
Users (IAM roles)	🟩	🟩	🟥	🟥	🟥

Pre-Event
Structural Awareness

Post-Event
Situational Awareness

Degree of Dependency

Technology

People

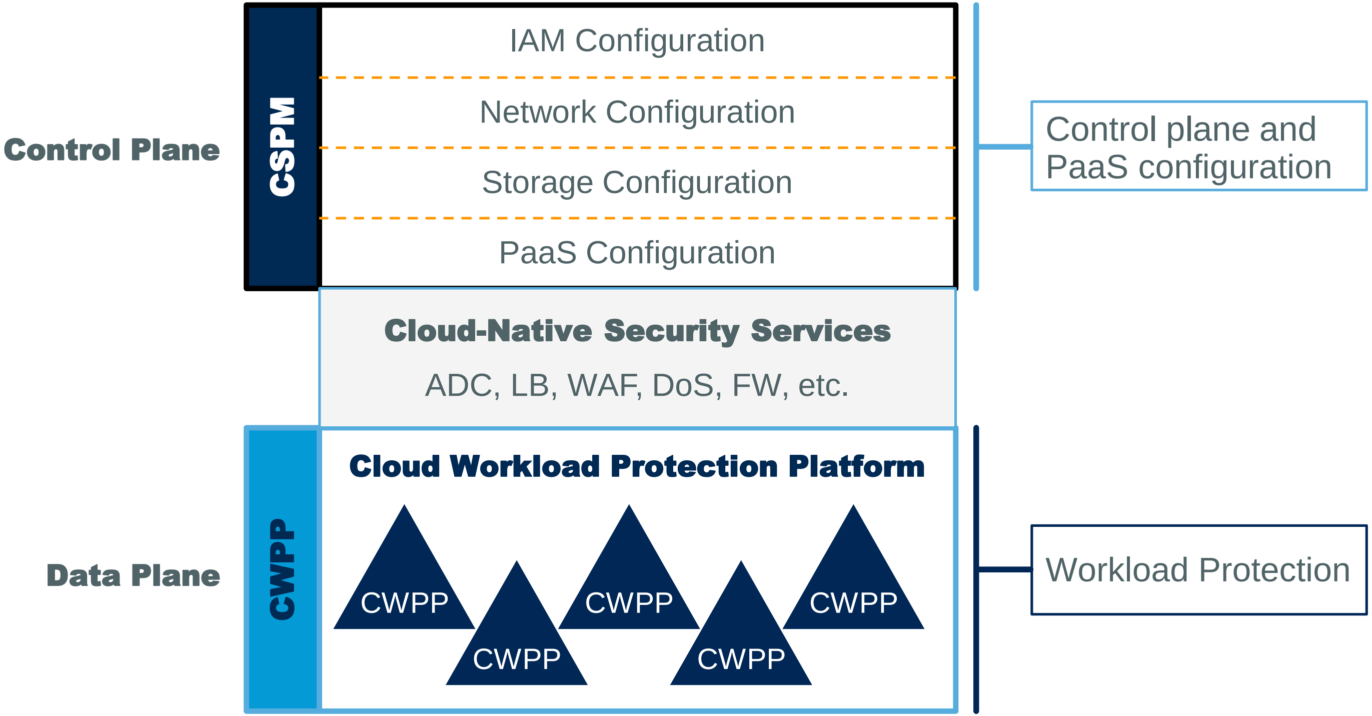
Process

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

Sponsored by: aws marketplace

SOUNIL YU
@sounilyu

Cloud Workload Protection Platforms (CWPP) and Cloud Security Posture Management (CSPM) capabilities are adjacent and complement each other



Control Plane

CSPM

IAM Configuration

Network Configuration

Storage Configuration

PaaS Configuration

Control plane and PaaS configuration

Cloud-Native Security Services

ADC, LB, WAF, DoS, FW, etc.

Data Plane

CWPP

Cloud Workload Protection Platform

CWPP

CWPP

CWPP

CWPP

CWPP

Workload Protection

Source: Gartner Market Guide for Cloud Workload Protection Platforms, 2020

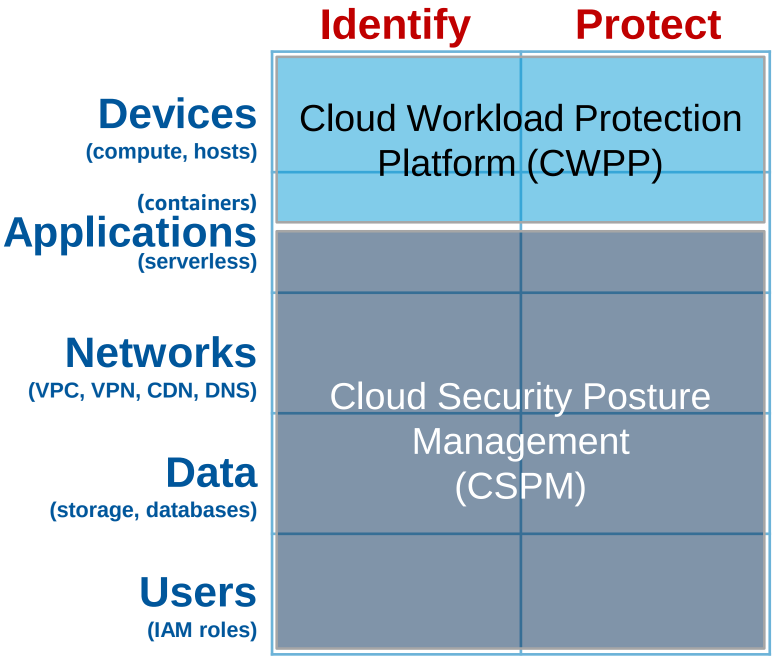
*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

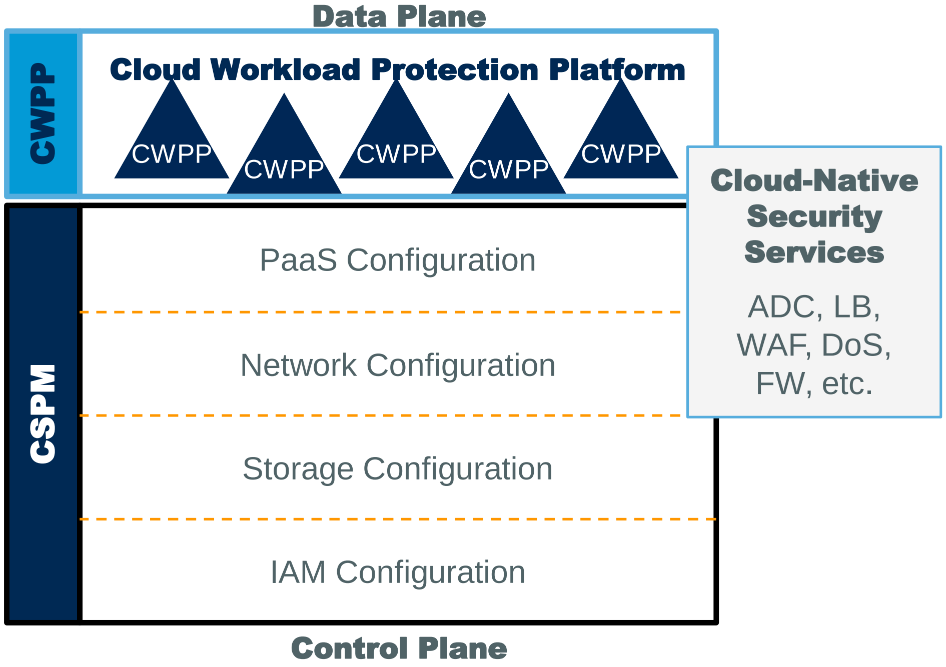
Sponsored by: aws marketplace

SOUNIL YU

@sounilyu

The Cyber Defense Matrix can show how cloud security can be addressed with CWPP and CSPM capabilities





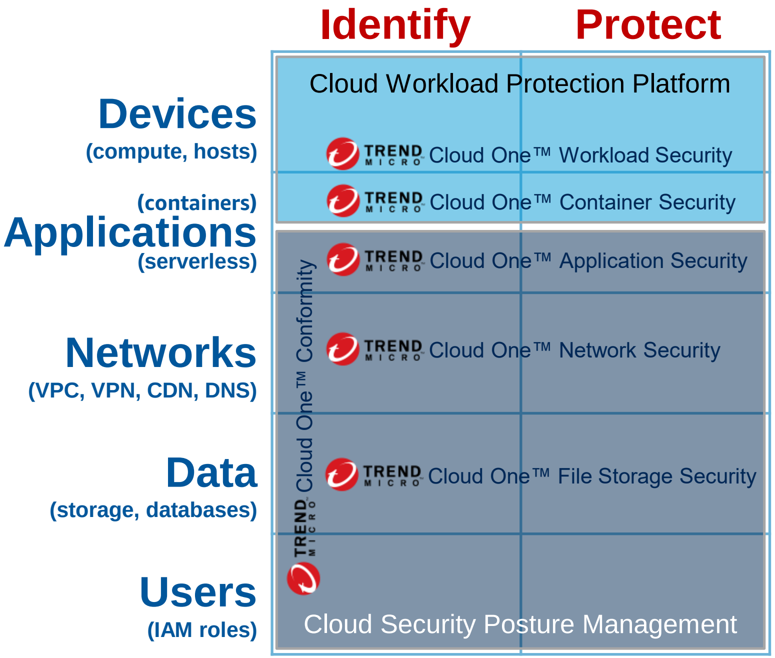
Source: Gartner Market Guide for Cloud Workload Protection Platforms, 2020 (slightly modified)

Sponsored by: aws marketplace

SOUNIL YU
@sounilyu

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

Mapping products, such as Trend Micro’s Cloud One, to the Cyber Defense Matrix can help understand coverage



Identify | Protect

Devices (compute, hosts)

(containers) Applications (serverless)

Networks (VPC, VPN, CDN, DNS)

Data (storage, databases)

Users (IAM roles)

Cloud Workload Protection Platform

TREND MICRO Cloud One™ Workload Security

TREND MICRO Cloud One™ Container Security

TREND MICRO Cloud One™ Application Security

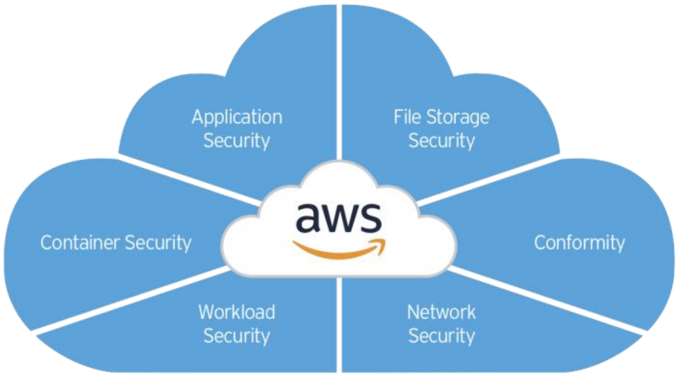
TREND MICRO Cloud One™ Network Security

TREND MICRO Cloud One™ File Storage Security

TREND MICRO Cloud One™ Conformity

Cloud Security Posture Management

TREND MICRO Cloud One™



Application Security

File Storage Security

Container Security

aws

Conformity

Workload Security

Network Security

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

Sponsored by: aws marketplace

SOUNIL YU

@sounilyu

A more detailed breakdown of underlying capabilities provide further insights on areas of need

		Devices (compute, hosts)	**Applications** (containers, serverless)	**Networks** (VPC, VPN, CDN, DNS)	**Data** (storage, databases)	**Users** (IAM Roles)
Identify	Inventory	EC2 Instances, Stopped Machines	Software Bill of Materials, Installed Applications	IP Addresses, VPCs, FWs	S3 Buckets, Databases	Accounts
	Classification	Unsupported O/S			Classification of viruses, malware, PII, PHI, PCI	Admin Accounts
	Vuln Assessment	O/S Vulnerabilities, Weak PWs, Insecure SSH Keys	OSS Library Vulnerabilities	Unintentionally Open Ports, Improper Routing	Unintentionally Open S3 Buckets, Exposed Keys	Weak Passwords, No MFA
	Identity Mgt	SSH Key Management	Secrets Management	DNS, DHCP, IP Address Management	Key Management	IAM Role Management
Protect	Access Mgt	EC2 Connect		Firewall Manager	S3 Bucket ACLs	IAM Role Management
	Patching / Fixing	O/S Patch	Code Fix, Component Update	Network Segmentation	Encryption	Password Reset, Access Revocation
	Exploit Mitigation	Memory Protection	Web Application Firewall	Network Intrusion Prevention System		MFA Enablement
	Logging, Monitoring	System Logs	Application Logs	Flow Logs	Access Logs	Account Activity History

Non-Exhaustive

Sponsored by: aws marketplace

SOUNIL YU

@sounilyu

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

Another fundamental benefit of cloud-native security capabilities is that it helps us adhere to design patterns that look more like “cattle” and less like “pets”

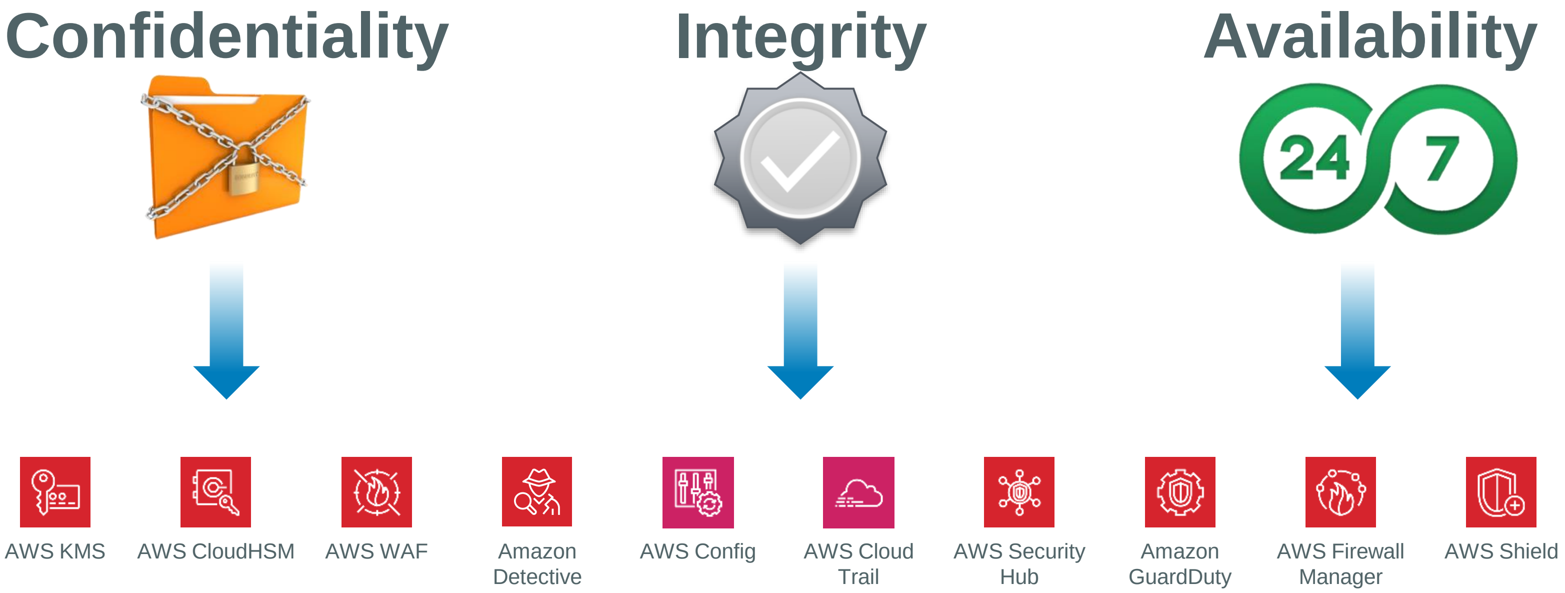
- Given a familiar name
- Taken to the vet when sick
- Hugged

- Branded with an obscure, unpronounceable name
- Culled from herd

amazon
4134 4755 6793 4833
D. BARRETT
VISA
Signature

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

We can leverage AWS native capabilities to secure our "pets" and address all three elements of the CIA Triad



Confidentiality

Integrity

Availability

AWS KMS

AWS CloudHSM

AWS WAF

Amazon Detective

AWS Config

AWS Cloud Trail

AWS Security Hub

Amazon GuardDuty

AWS Firewall Manager

AWS Shield

Sponsored by: aws marketplace

SOUNIL YU

@sounilyu

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

Adhering to the DIE Triad helps us build “cattle”

Amazon CloudFront

Distributed

DDoS Resistant

The best solution against a distributed attack is a distributed service

Availability

AWS CloudFormation

Immutable

Changes Easier to Detect and Reverse

Unauthorized changes stand out and can be reverted to known good

Integrity

AWS Lambda

Ephemeral

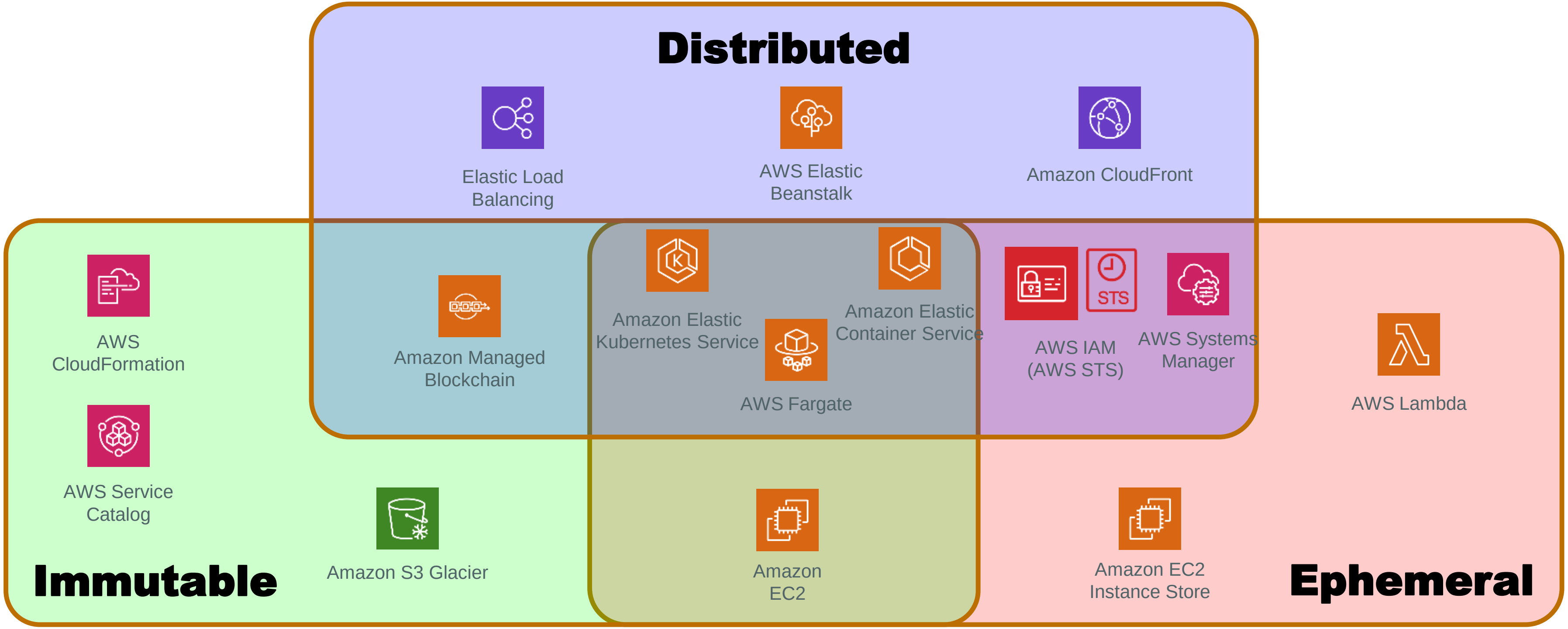
Drives Value of Assets Closer to Zero

Makes attacker persistence hard and reduces concern for assets at risk

Confidentiality

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

There are many AWS native capabilities that align to the DIE Triad to help us build "cattle"

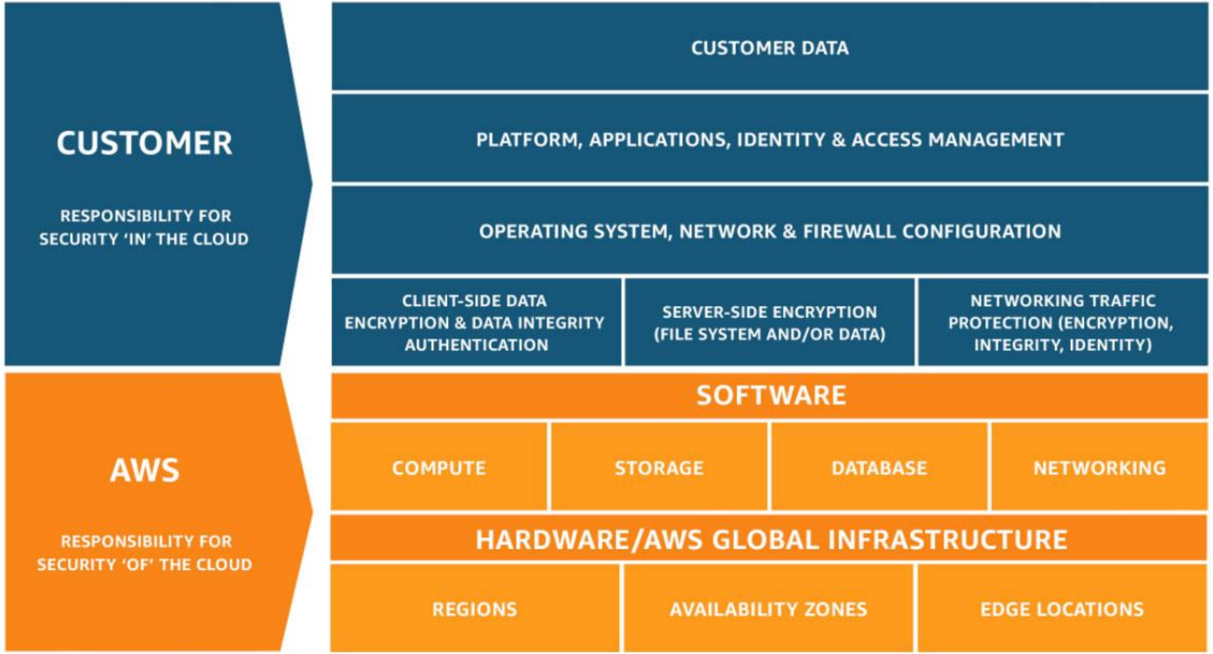


*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

Sponsored by: aws marketplace

SOUNIL YU
@sounilyu

The distribution of “Pets” and “Cattle” change across the Shared Responsibility Model and with cloud native maturity



CUSTOMER

RESPONSIBILITY FOR SECURITY ‘IN’ THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY ‘OF’ THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

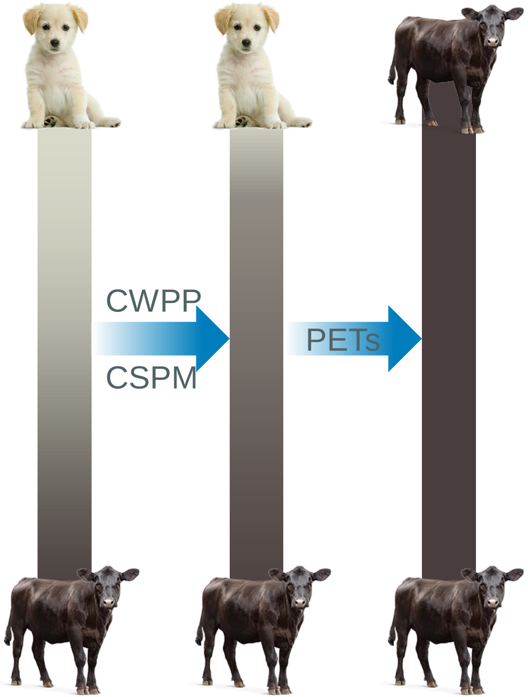
NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

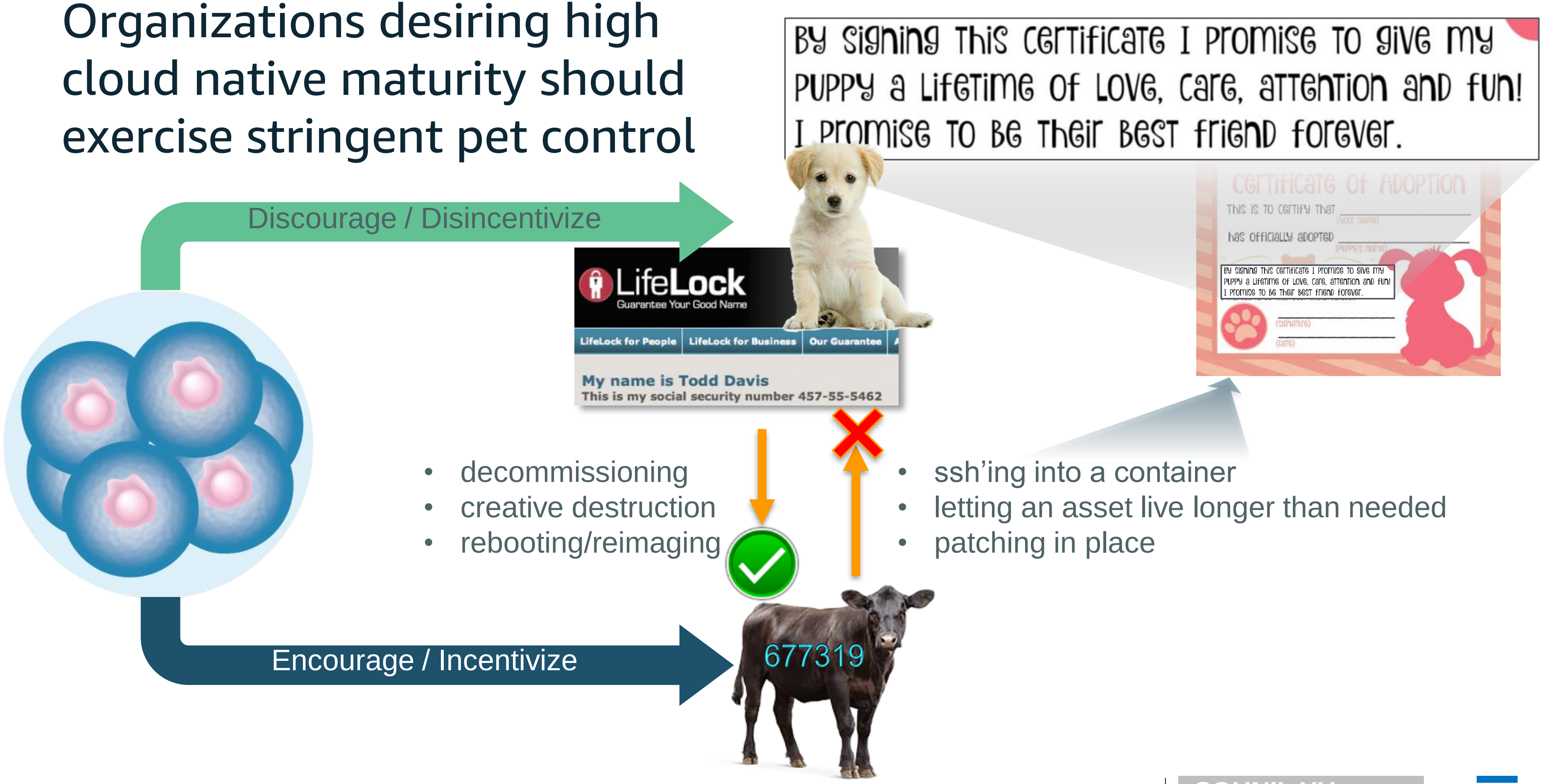
AVAILABILITY ZONES

EDGE LOCATIONS



*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

Organizations desiring high cloud native maturity should exercise stringent pet control



By signing this certificate I promise to give my puppy a lifetime of love, care, attention and fun! I promise to be their best friend forever.

Certificate of Adoption

This is to certify that ______________
(your name)

has officially adopted ______________
(puppy's name)

By signing this certificate I promise to give my puppy a lifetime of love, care, attention and fun! I promise to be their best friend forever.

____
(signature)

____
(date)

LifeLock
Guarantee Your Good Name

LifeLock for People | LifeLock for Business | Our Guarantee

My name is Todd Davis
This is my social security number 457-55-5462

- decommissioning
- creative destruction
- rebooting/reimaging

- ssh’ing into a container
- letting an asset live longer than needed
- patching in place

*The views and opinions of Sounil Yu are their own and do not necessarily reflect the positions of AWS or AWS Marketplace.

Sponsored by: aws marketplace

SOUNIL YU
@sounilyu

aws marketplace

Mapping security coverage from day one in AWS

Migration to AWS

Security Requirements

- Visibility
- Authority
- Capability
- Compliance

Organization Requirements

- Confidentiality
- Integrity
- Availability
- Distributed
- Immutable
- Ephemeral

CSPM and CWPP Facilitate

- Inventory of cloud assets
- Authority to access via IAM
- Capability to protect, monitor, measure compliance and risk

Development in AWS

Security Requirements

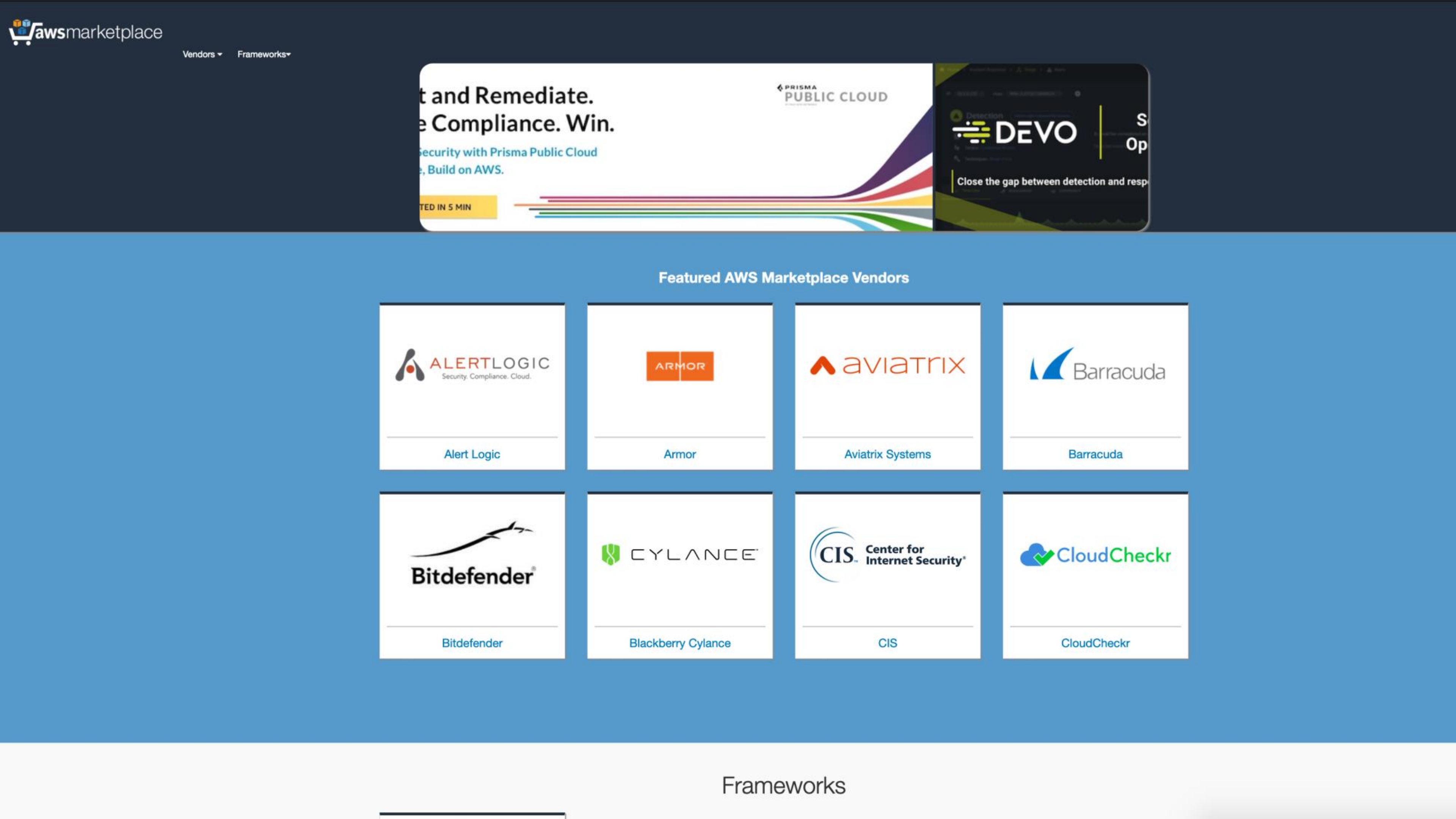
- Visibility
- Authority
- Capability
- Compliance

DevOps Requirements

- Easy Access
- Speed / Agility
- Frictionless CI/CD pipeline

CSPM and CWPP Facilitate

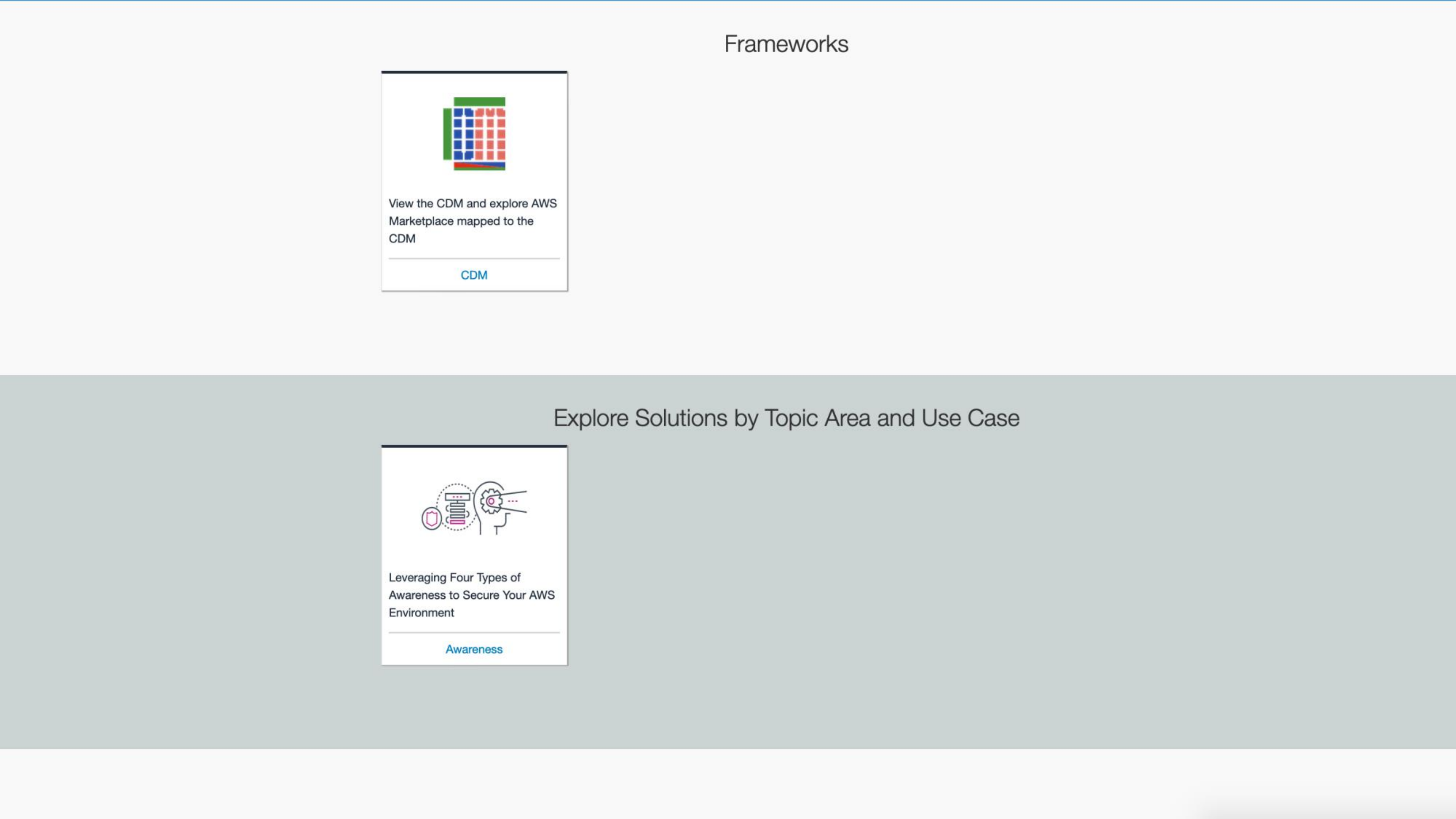
- Inventory of cloud assets
- Authority to access via IAM
- Capability to protect, monitor, measure compliance and risk



Featured AWS Marketplace Vendors

Alert Logic	Armor	Aviatrix Systems	Barracuda
Bitdefender	Blackberry Cylance	CIS	CloudCheckr

Frameworks



Frameworks

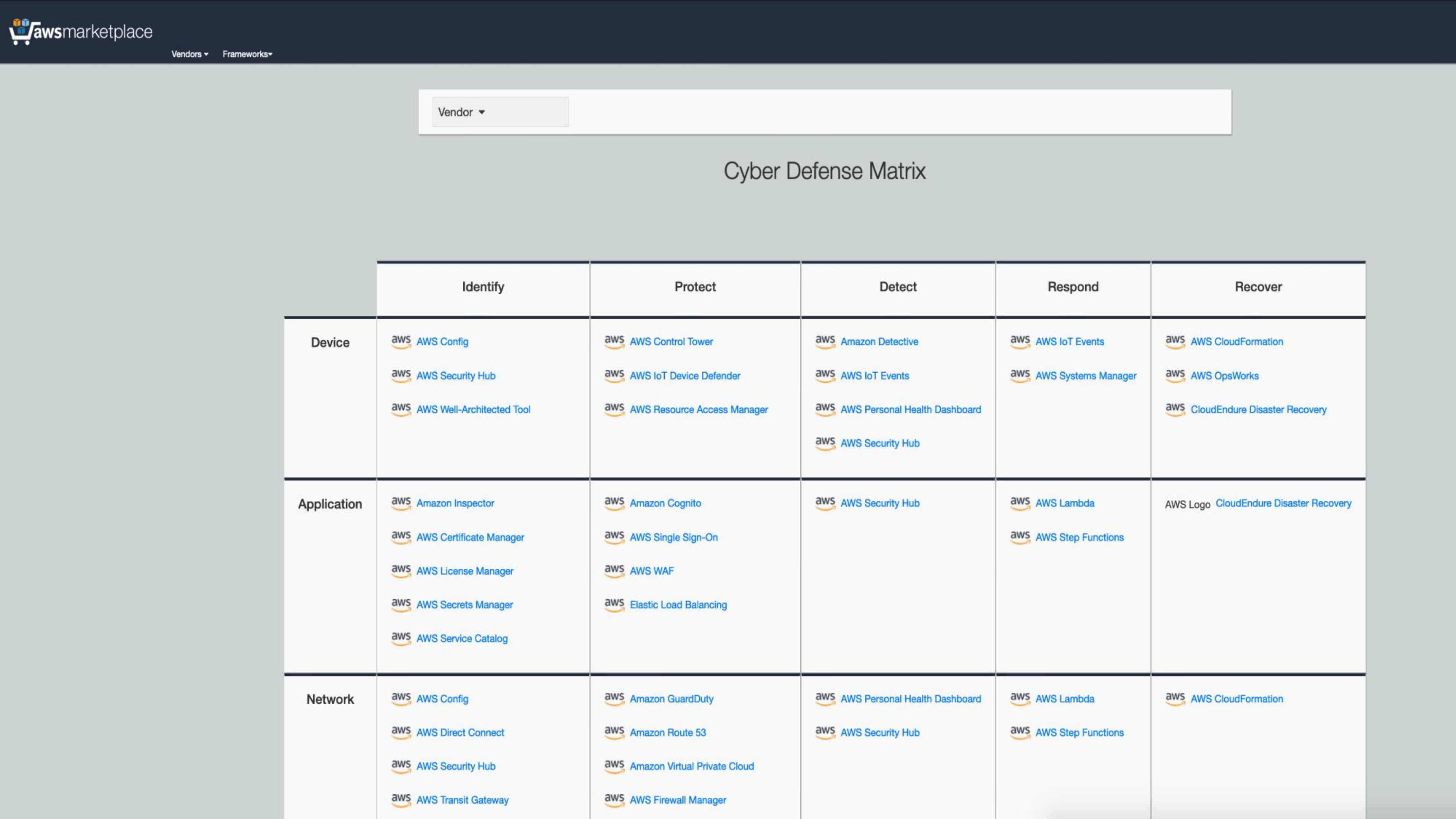
View the CDM and explore AWS Marketplace mapped to the CDM

CDM

Explore Solutions by Topic Area and Use Case

Leveraging Four Types of Awareness to Secure Your AWS Environment

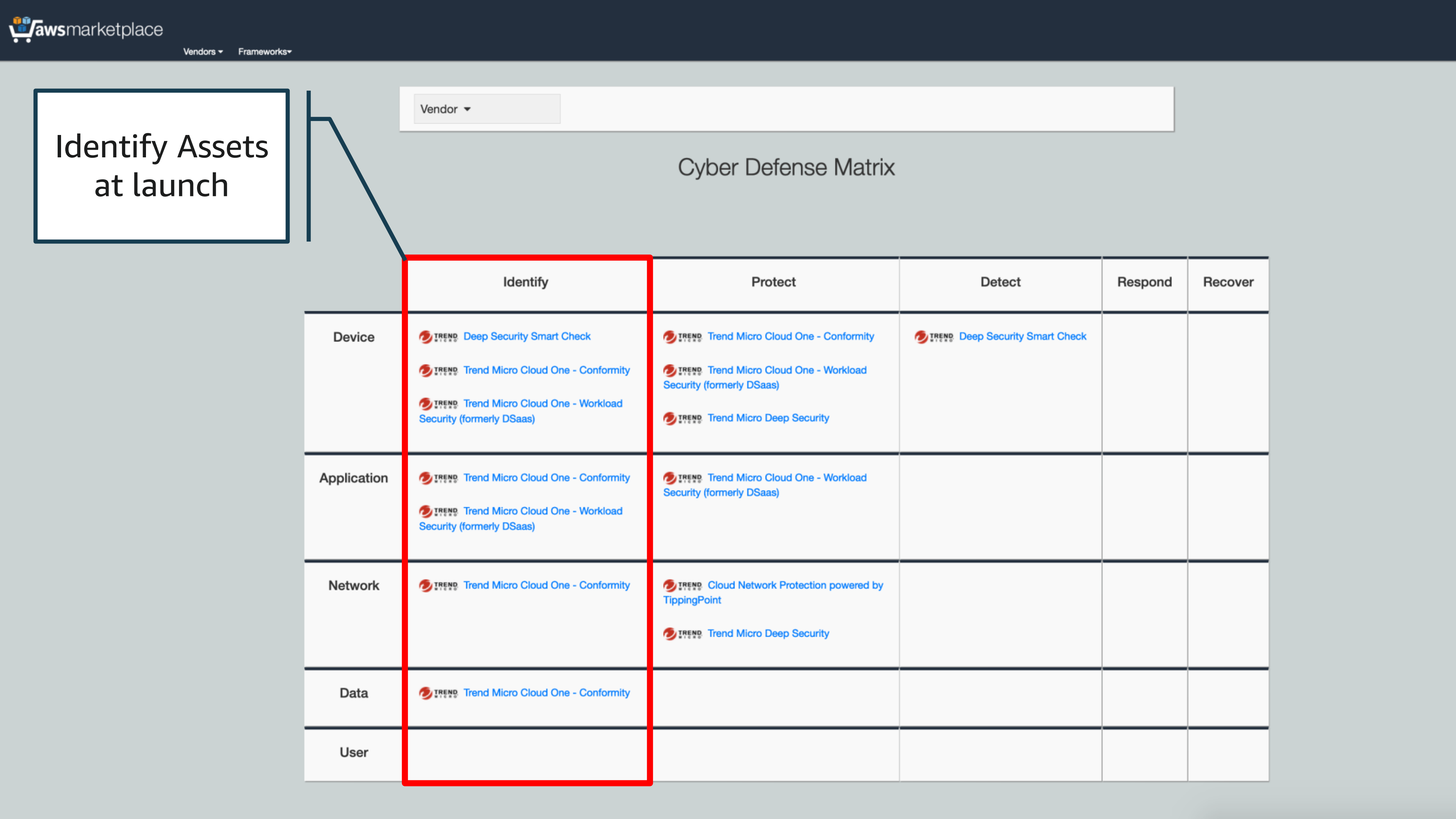
Awareness



Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Device	AWS Config AWS Security Hub AWS Well-Architected Tool	AWS Control Tower AWS IoT Device Defender AWS Resource Access Manager	Amazon Detective AWS IoT Events AWS Personal Health Dashboard AWS Security Hub	AWS IoT Events AWS Systems Manager	AWS CloudFormation AWS OpsWorks CloudEndure Disaster Recovery
Application	Amazon Inspector AWS Certificate Manager AWS License Manager AWS Secrets Manager AWS Service Catalog	Amazon Cognito AWS Single Sign-On AWS WAF Elastic Load Balancing	AWS Security Hub	AWS Lambda AWS Step Functions	AWS Logo CloudEndure Disaster Recovery
Network	AWS Config AWS Direct Connect AWS Security Hub AWS Transit Gateway	Amazon GuardDuty Amazon Route 53 Amazon Virtual Private Cloud AWS Firewall Manager	AWS Personal Health Dashboard AWS Security Hub	AWS Lambda AWS Step Functions	AWS CloudFormation

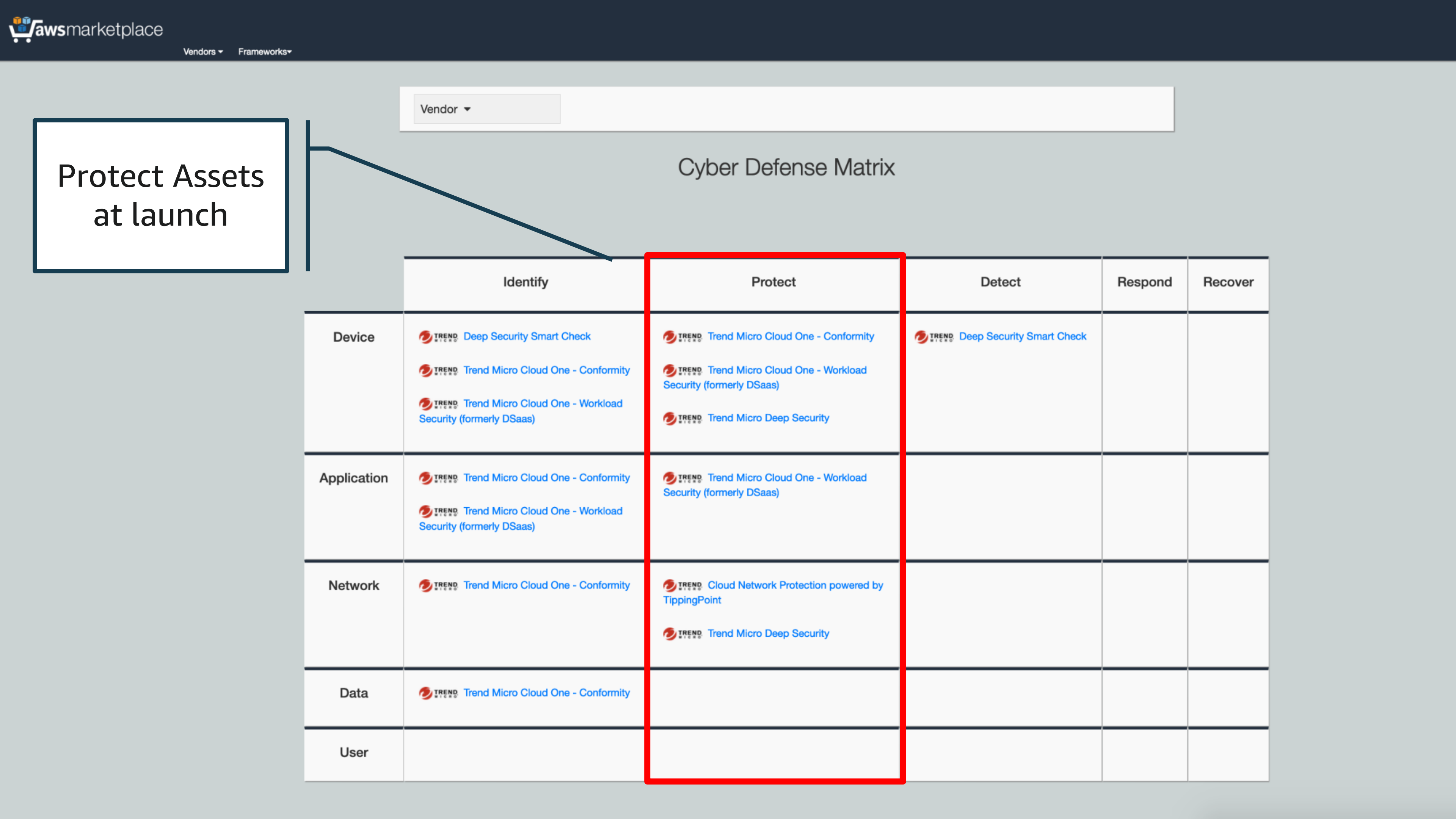
Identify Assets at launch



Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Device	Deep Security Smart Check Trend Micro Cloud One - Conformity Trend Micro Cloud One - Workload Security (formerly DSaas)	Trend Micro Cloud One - Conformity Trend Micro Cloud One - Workload Security (formerly DSaas) Trend Micro Deep Security	Deep Security Smart Check		
Application	Trend Micro Cloud One - Conformity Trend Micro Cloud One - Workload Security (formerly DSaas)	Trend Micro Cloud One - Workload Security (formerly DSaas)			
Network	Trend Micro Cloud One - Conformity	Cloud Network Protection powered by TippingPoint Trend Micro Deep Security			
Data	Trend Micro Cloud One - Conformity				
User					

Protect Assets at launch

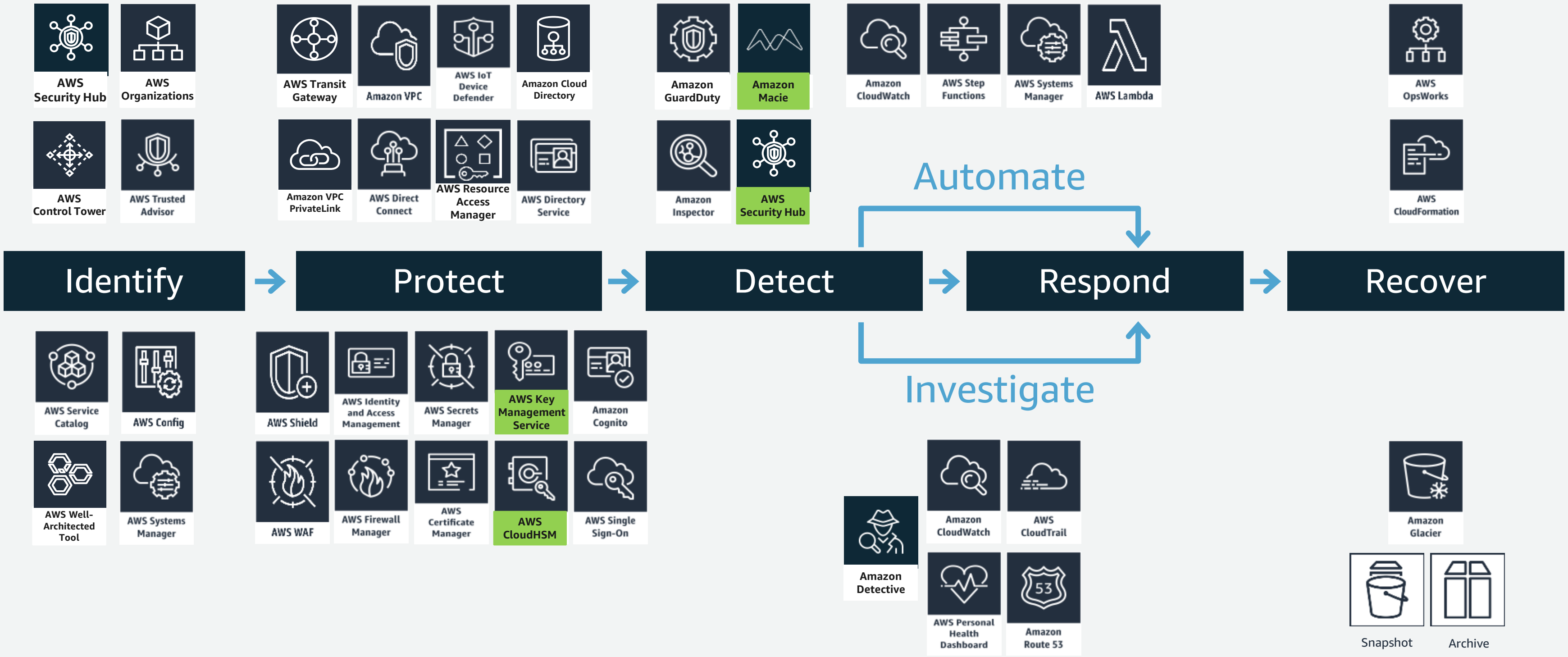


Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Device	TREND MICRO Deep Security Smart Check TREND MICRO Trend Micro Cloud One - Conformity TREND MICRO Trend Micro Cloud One - Workload Security (formerly DSaas)	TREND MICRO Trend Micro Cloud One - Conformity TREND MICRO Trend Micro Cloud One - Workload Security (formerly DSaas) TREND MICRO Trend Micro Deep Security	TREND MICRO Deep Security Smart Check		
Application	TREND MICRO Trend Micro Cloud One - Conformity TREND MICRO Trend Micro Cloud One - Workload Security (formerly DSaas)	TREND MICRO Trend Micro Cloud One - Workload Security (formerly DSaas)			
Network	TREND MICRO Trend Micro Cloud One - Conformity	TREND MICRO Cloud Network Protection powered by TippingPoint TREND MICRO Trend Micro Deep Security			
Data	TREND MICRO Trend Micro Cloud One - Conformity				
User					

Protecting sensitive assets in AWS

AWS services that enable sensitive asset protection



Identify

AWS Security Hub

AWS Organizations

AWS Control Tower

AWS Trusted Advisor

AWS Service Catalog

AWS Config

AWS Well-Architected Tool

AWS Systems Manager

Protect

AWS Transit Gateway

Amazon VPC

AWS IoT Device Defender

Amazon Cloud Directory

Amazon VPC PrivateLink

AWS Direct Connect

AWS Resource Access Manager

AWS Directory Service

AWS Shield

AWS Identity and Access Management

AWS Secrets Manager

AWS Key Management Service

Amazon Cognito

AWS WAF

AWS Firewall Manager

AWS Certificate Manager

AWS CloudHSM

AWS Single Sign-On

Detect

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Security Hub

Automate

Amazon CloudWatch

AWS Step Functions

AWS Systems Manager

AWS Lambda

Respond

Investigate

Amazon Detective

Amazon CloudWatch

AWS CloudTrail

AWS Personal Health Dashboard

Amazon Route 53

Recover

AWS OpsWorks

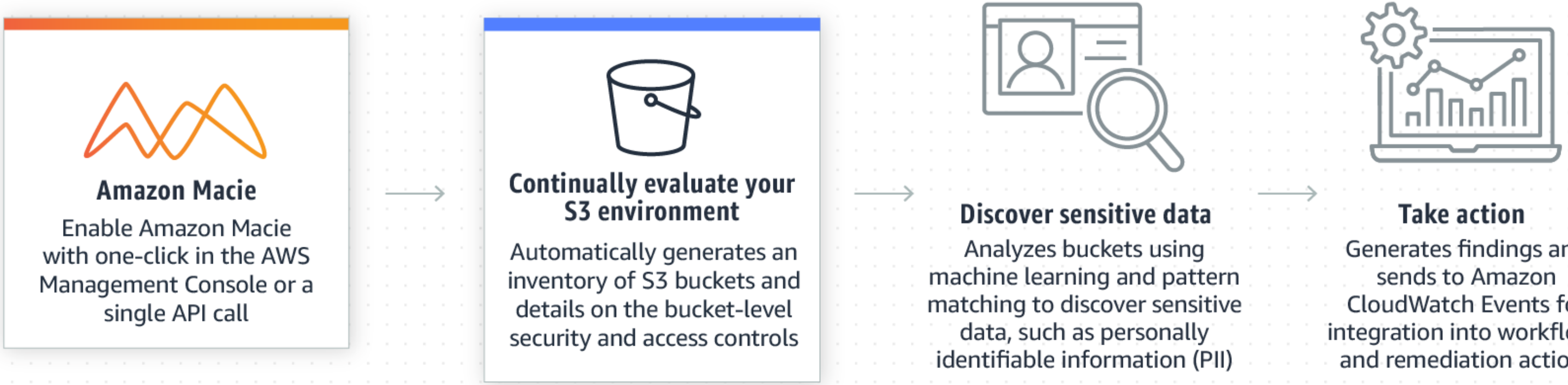
AWS CloudFormation

Amazon Glacier

Snapshot

Archive

Discover your sensitive data with machine learning



Amazon Macie

Enable Amazon Macie with one-click in the AWS Management Console or a single API call

Continually evaluate your S3 environment

Automatically generates an inventory of S3 buckets and details on the bucket-level security and access controls

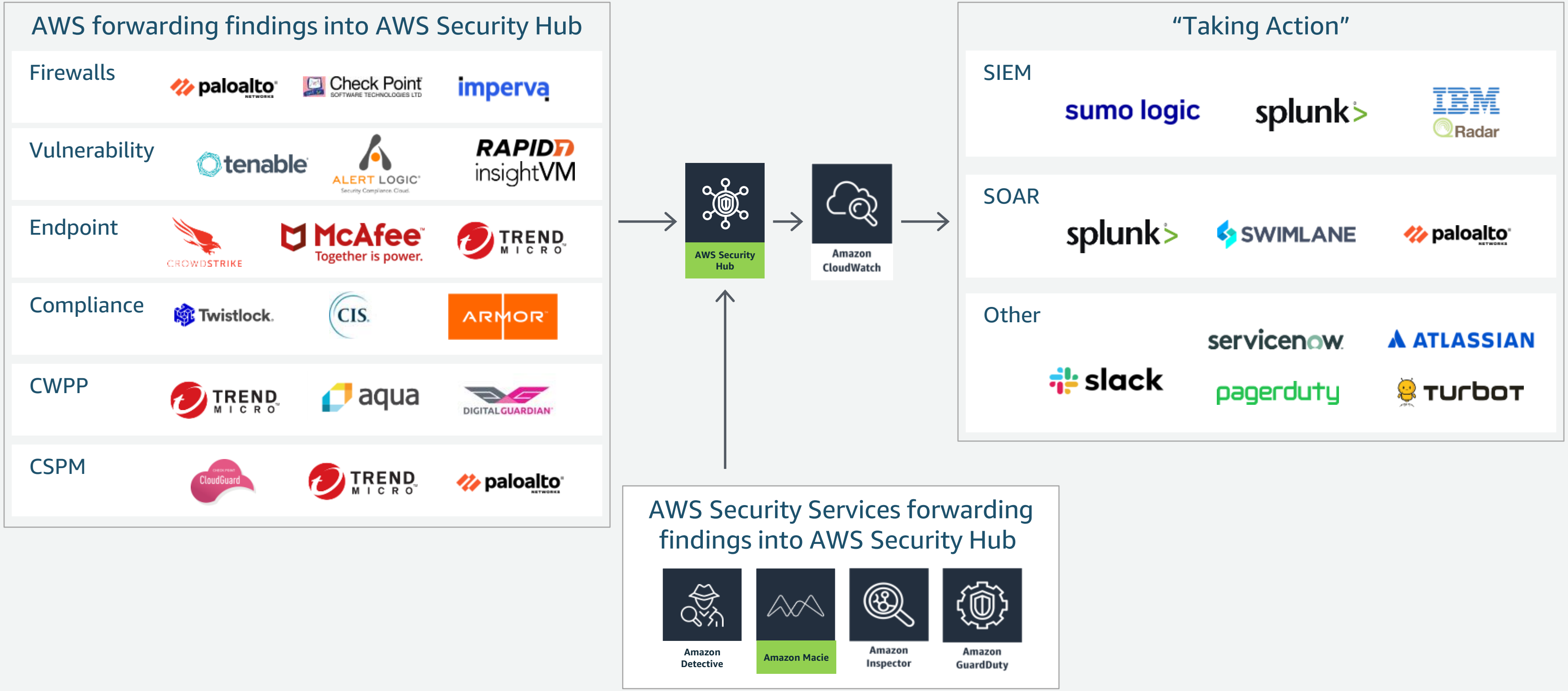
Discover sensitive data

Analyzes buckets using machine learning and pattern matching to discover sensitive data, such as personally identifiable information (PII)

Take action

Generates findings and sends to Amazon CloudWatch Events for integration into workflows and remediation actions

Increase visibility and secure sensitive assets



AWS forwarding findings into AWS Security Hub

Firewalls

Vulnerability

Endpoint

Compliance

CWPP

CSPM

“Taking Action”

SIEM

SOAR

Other

AWS Security Services forwarding findings into AWS Security Hub

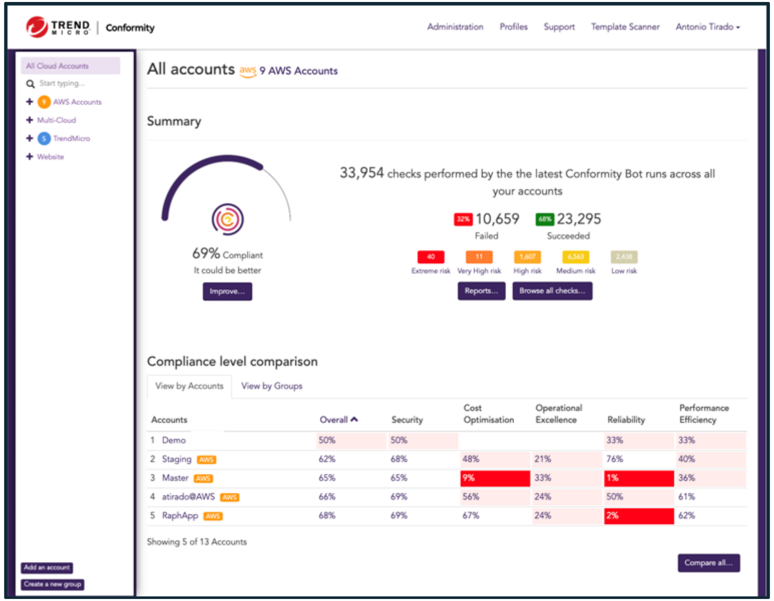
How are AWS customers leveraging Trend Micro?

TREND MICRO | Cloud One™ Conformity

Manage misconfigurations of cloud resources

Complete visibility with a single dashboard

Continuous assurance



All accounts aws 9 AWS Accounts

Summary

69% Compliant

It could be better

33,954 checks performed by the the latest Conformity Bot runs across all your accounts

32% 10,659	68% 23,295
Failed	Succeeded

40	11	1,607	6,563	2,438
Extreme risk	Very High risk	High risk	Medium risk	Low risk

Compliance level comparison

Accounts	Overall	Security	Cost Optimisation	Operational Excellence	Reliability	Performance Efficiency
1 Demo	50%	50%			33%	33%
2 Staging AWS	62%	68%	48%	21%	76%	40%
3 Master AWS	65%	65%	9%	33%	1%	36%
4 atirado@AWS AWS	66%	69%	56%	24%	50%	61%
5 RaphApp AWS	68%	69%	67%	24%	2%	62%

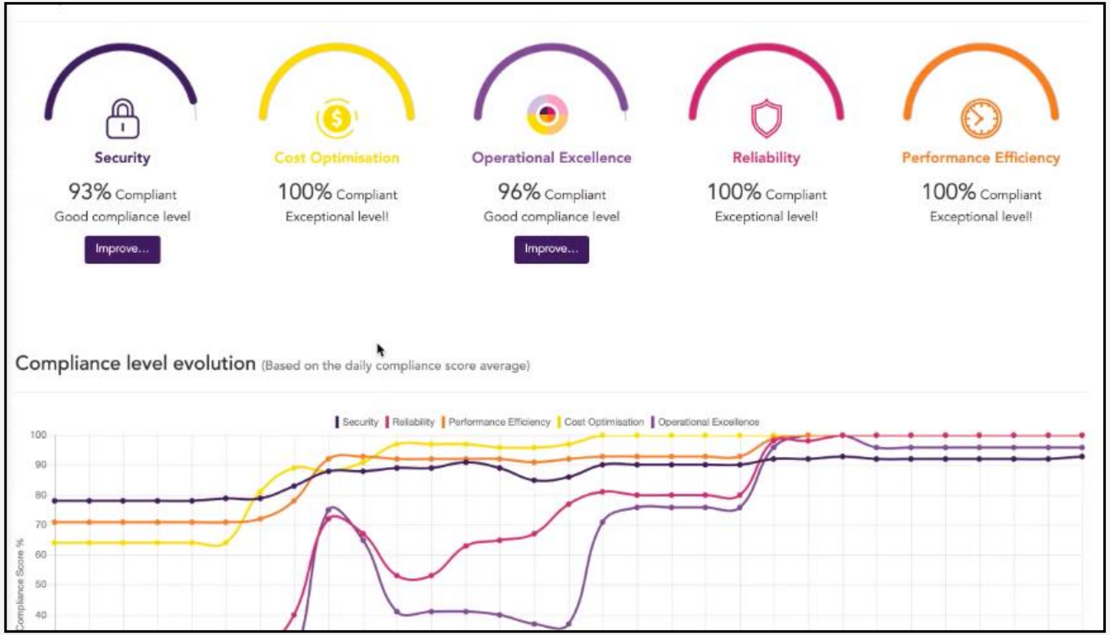
Showing 5 of 13 Accounts

Change Healthcare protects sensitive data

Using Trend Micro Cloud One™ Conformity

Benefits:

- Supports automation of compliance
- Simplifies the configuration and deployment of rules
- Able to quickly adopt new AWS services while maintaining compliance



Security
93% Compliant
Good compliance level
Improve...

Cost Optimisation
100% Compliant
Exceptional level!

Operational Excellence
96% Compliant
Good compliance level
Improve...

Reliability
100% Compliant
Exceptional level!

Performance Efficiency
100% Compliant
Exceptional level!

Compliance level evolution (Based on the daily compliance score average)

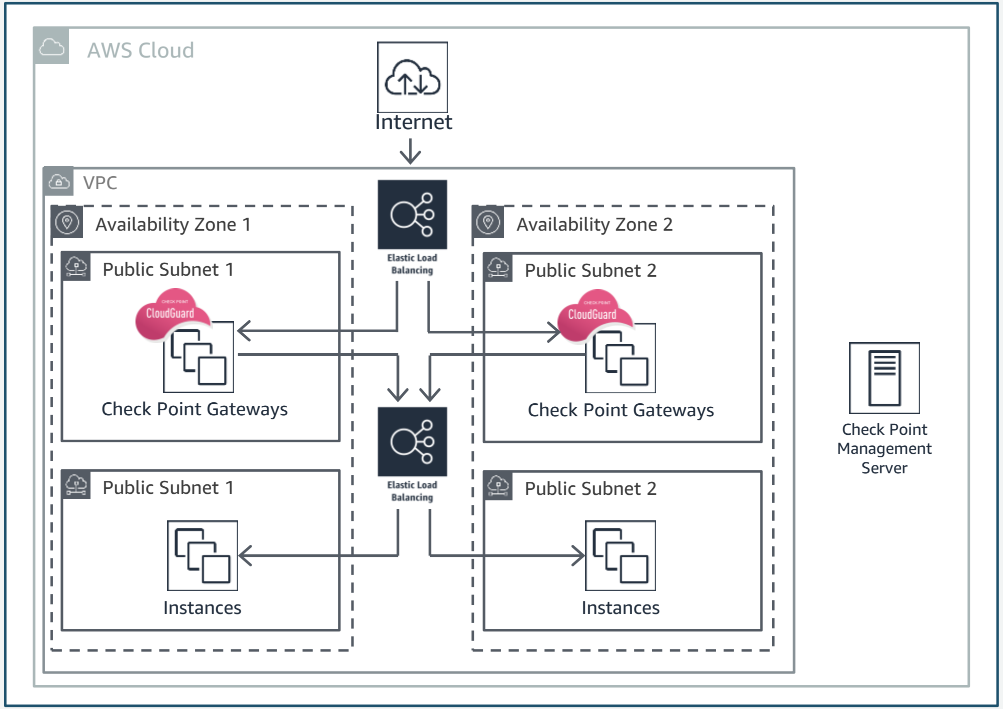
Example dashboard

Xero gains advanced security for sensitive assets

With Check Point CloudGuard IaaS

Benefits:

- Securely moved 700,000 customers, 59 billion records, and $1 trillion in transactions to AWS
- Automated security without slowing development

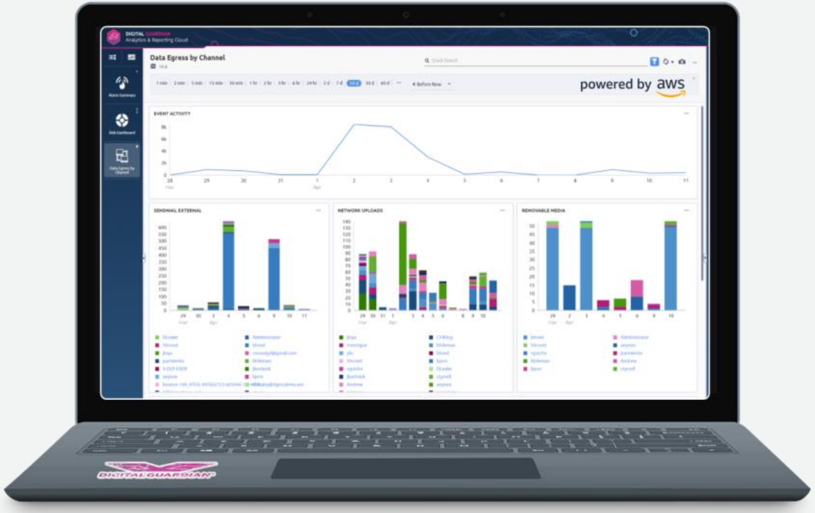


Jabil enhances sensitive data visibility and control

Leveraging Digital Guardian's Enterprise DLP Platform

Benefits:

- Gained visibility into all data access and usage across 52,000 workstations
- Identified and located critical IP as defined by each business unit and its customers
- Implemented more secure data workflows



Why AWS Marketplace?

Flexible consumption and contract models

Quick and easy deployment

Helpful humans to support you

How can you get started?

Find

A breadth of security solutions:

TREND MICRO

CHECK POINT CloudGuard Dome9

DIGITALGUARDIAN

paloalto NETWORKS

sumo logic

FORTINET

CROWDSTRIKE

splunk>

Buy

Through flexible pricing options:

Free trial

Pay-as-you-go

Hourly | Monthly | Annual | Multi-Year

Bring Your Own License (BYOL)

Seller Private Offers

Channel Partner Private Offers

Deploy

With multiple deployment options:

Software as a Service (SaaS)

Amazon Machine Image (AMI)

AWS CloudFormation (Infrastructure as Code)

Amazon Elastic Container Service (ECS)

Amazon Elastic Kubernetes Service (EKS)

Webinar summary

- Cloud Workload Protection Platforms and Cloud Security Posture Management solutions can help protect your most sensitive assets.
- Leverage AWS Services that integrate with your AWS environment and can enhance your network segmentation capabilities.
- Current tools? Bring your own license to leverage benefits of AWS Marketplace.
- New tools? Select solutions in AWS Marketplace for a curated list proven on AWS.

aws marketplace

Sounil Yu
Creator of the Cyber Defense Matrix

Josh Thurston
Sr. Category Lead, Security at AWS

Sagar Khasnis
Partner Solutions Architect at AWS

Thank you!