AWS Security Hub

Automate AWS security checks and centralize security alerts

Matias Dieguez

Solutions Architect
Amazon Web Services

Agenda

- ✓ Security and compliance challenges
- ✓ Threat detection, monitoring, and response
- ✓ What is AWS Security Hub?
- ✓ Elevate your security with AWS
- ✓ Security Hub use cases and customers
- ✓ Get started with Security Hub

Challenges security teams face

Lack of visibility into security risks and their impact

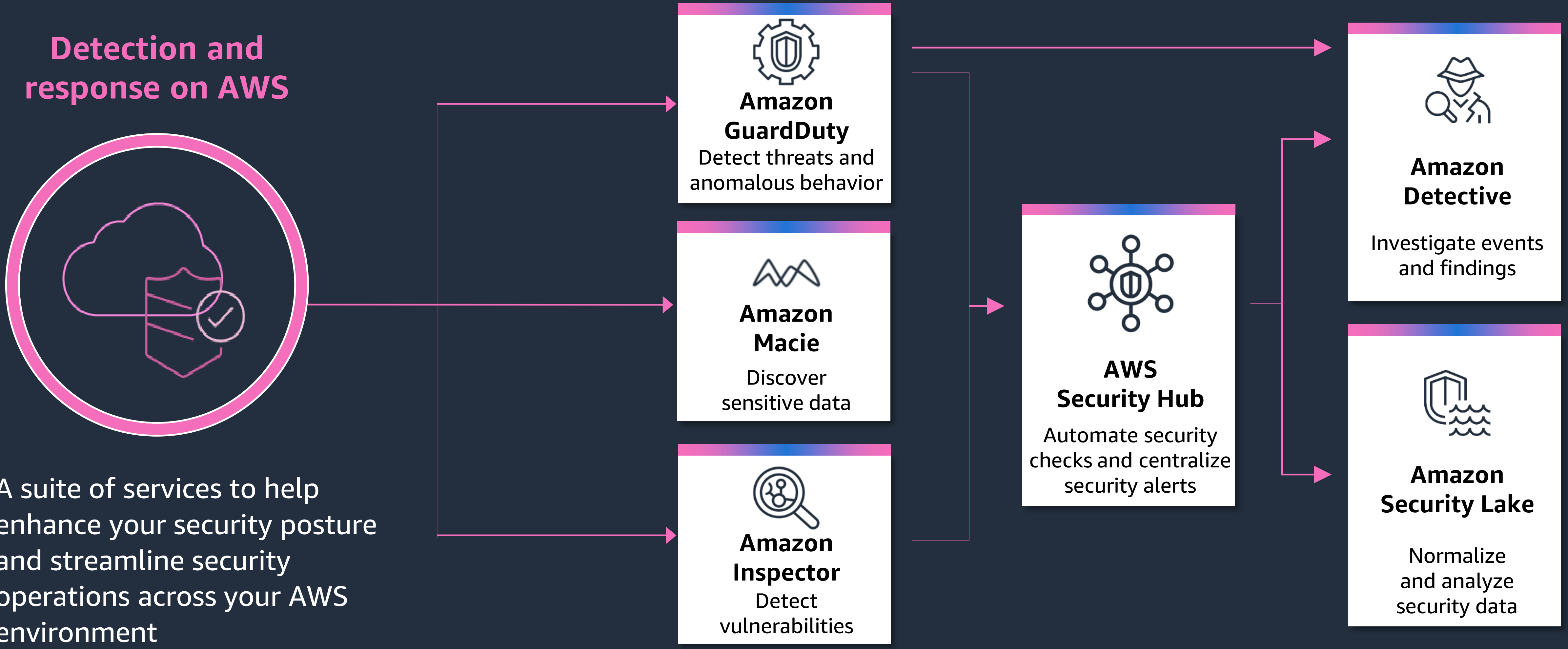
Adjust security measures **at scale** to meet the needs of the organization

Multiple sources of security alerts

Too many alerts, and not enough context

AWS detection and response services

Detection and response on AWS



Amazon GuardDuty
Detect threats and anomalous behavior

Amazon Macie
Discover sensitive data

Amazon Inspector
Detect vulnerabilities

AWS Security Hub
Automate security checks and centralize security alerts

Amazon Detective
Investigate events and findings

Amazon Security Lake
Normalize and analyze security data

A suite of services to help enhance your security posture and streamline security operations across your AWS environment

What is AWS Security Hub?

Security Hub is a cloud security posture management service that **continually** performs security best practice checks and **seamlessly** aggregates security findings from AWS and third-party services to enable automated response

Automated, continuous best practice checks

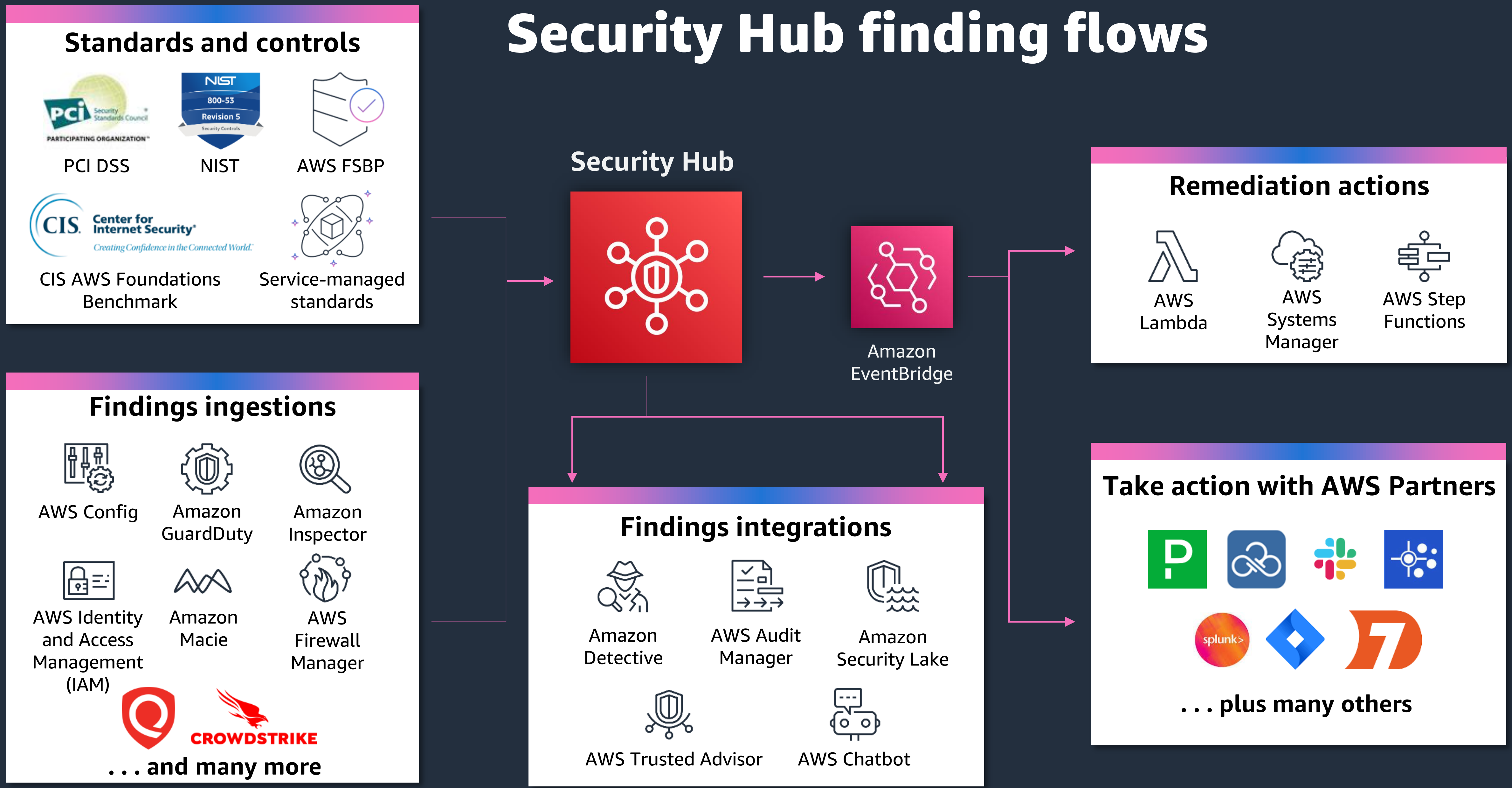
AWS Foundational Security Best Practices (FSBP) standard, CIS, and more

Simple deployment, scalable up to 10K accounts

AWS and 3rd-party services findings aggregation across accounts and Regions

Automated response, and enrichment actions

Security Hub finding flows



Standards and controls

PCI DSS

NIST

AWS FSBP

CIS AWS Foundations Benchmark

Service-managed standards

Findings ingestions

AWS Config

Amazon GuardDuty

Amazon Inspector

AWS Identity and Access Management (IAM)

Amazon Macie

AWS Firewall Manager

CROWDSTRIKE

. . . and many more

Security Hub

Amazon EventBridge

Remediation actions

AWS Lambda

AWS Systems Manager

AWS Step Functions

Take action with AWS Partners

. . . plus many others

Findings integrations

Amazon Detective

AWS Audit Manager

Amazon Security Lake

AWS Trusted Advisor

AWS Chatbot

This is not a complete list. To view all AWS Security Hub partners, visit the Security Hub console. This list of partners is current as of November 28, 2023.

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

How customers use Security Hub

✓ Conduct Cloud Security Posture Management (CSPM)

✓ Initiate Security Orchestration, Automation, and Response (SOAR) workflows

✓ Save time and money by simplifying integrations

✓ Visualize security findings to discover new insights

Siemens Strengthens Security and Enhances Productivity Using AWS

> "Pulling data individually from each source and doing our own correlations was difficult. **Migrating to AWS Security Hub and Amazon GuardDuty gave us a central view** into that data, which was very desirable."

Scott Schwartz

Senior Infrastructure Engineer, Siemens

https://aws.amazon.com/solutions/case-studies/siemens-security

SIEMENS

Southwest Airlines Invests in Its Security Posture Using AWS Security Hub

Southwest

CHALLENGE

Southwest Airlines (Southwest) wanted to invest in its security posture to protect the many integrated applications that keep the airline running safely and smoothly.

APPROACH & SOLUTION

Southwest adopted AWS Security Hub, a key part of a broader automated and scalable integration that provides users with a comprehensive view of their security alerts and security posture across AWS accounts.

- ✓ Improved visibility into its security posture
- ✓ Reduced time and labor when implementing 350+ automated security controls
- ✓ Scans 600,000 resources with 98% compliance across 350+ security control objectives
- ✓ Reduced implementation time for new controls from 5–6 weeks to 1 week

https://aws.amazon.com/solutions/case-studies/southwest-case-study/

GoDaddy Centralizes Security Findings and Gains Insights Using AWS Security Hub

CHALLENGE

GoDaddy was looking for a way to streamline the time-consuming processes of parsing and normalizing data from multiple security tools into a common format for search, analytics, and response and remediation.

APPROACH & SOLUTION

Using Security Hub, GoDaddy manages security from a serverless, customizable, centralized location that has increased visibility and coverage while saving GoDaddy significant overhead and maintenance costs.

- ✓ Centralized and streamlined security findings
- ✓ Created customized dashboards for users
- ✓ Alleviated maintenance and overhead by automating processes
- ✓ Saved cost by not paying for downtime between scans
- ✓ Reduced mean time to remediate with continual vulnerability scanning

https://aws.amazon.com/solutions/case-studies/godaddy-case-study/

Get started with Security Hub

Try Security Hub for 30 days at no cost
Estimate your monthly spend across AWS accounts and Regions.

Explore Security Hub features
Learn more about accurate, account-level threat detection, optimized for cloud.

Consult the documentation
Learn more about standards and controls, managing findings, and integrations.

Discover more resources
Get hands-on, find an AWS Partner, or find answers to frequently asked questions.

Thank you!

Matias Dieguez

Appendix

AWS security, identity, and compliance solutions

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

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 manage 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

AWS security, identity, and compliance solutions

Identity and access management

- AWS Identity and Access Management (IAM)
- AWS IAM Identity Center
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager
- Amazon Verified Permissions

Detective controls

- AWS Security Hub
- Amazon GuardDuty
- Amazon Security Lake
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs
- AWS IoT Device Defender

Infrastructure protection

- AWS Firewall Manager
- AWS Network Firewall
- AWS Shield
- AWS WAF
- Amazon VPC
- AWS PrivateLink
- AWS Systems Manager
- AWS Verified Access

Data protection

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Private CA
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption

Incident response

- Amazon Detective
- Amazon EventBridge
- AWS Backup
- AWS Security Hub
- AWS Elastic Disaster Recovery

Compliance

- AWS Artifact
- AWS Audit Manager

Large community of security partners & solutions

Network and infrastructure security

- ALERT LOGIC Security. Compliance. Cloud.
- APPGATE
- ARMOR
- Barracuda
- Check Point SOFTWARE TECHNOLOGIES LTD.
- CISCO
- ExtraHop
- FORTINET
- Guardicore
- paloalto NETWORKS
- PROTECTWISE
- SKinfosec co.,ltd.
- SOPHOS
- zscaler

Identity and access control

- okta
- onelogin
- Ping Identity
- SAVIYNT

Vulnerability and configuration analysis

- bridgecrew
- ExtraHop
- Qualys.
- RAPID7
- tenable
- threat stack

Logging, monitoring, SIEM, threat detection, and analytics

- ALIEN VAULT
- LACEWORK
- McAfee Together is power.
- SECURONIX Security Analytics. Delivered.
- splunk>
- sumo logic

Host and endpoint security

- CROWDSTRIKE
- Symantec
- TREND MICRO
- SentinelOne

Application security

- Barracuda
- Checkmarx
- f5

Data protection and encryption

- CYBERARK
- DataSunrise Data & Database Security
- gemalto security to be free
- HashiCorp
- PRIVITAR
- THALES
- COHESITY

aws

Consulting and technology competency partners

Security engineering

- 8K Miles
- accenture High performance. Delivered.
- AllCloud
- CMD SOLUTIONS
- CLOUDZONE by matrix
- CLOUDTEN
- Deloitte.
- ECCOiii 华 讯 网 络
- escala 24x7
- FOGHORN
- GUIDEPOINT SECURITY
- HELECLOUD
- Hewlett Packard Enterprise
- ltoc
- lightstream
- logicworks
- NRI
- pwc
- Smartronix CLOUD ASSURED
- Telefonica
- VERSENT
- direktgruppe dg
- HITACHI Inspire the Next

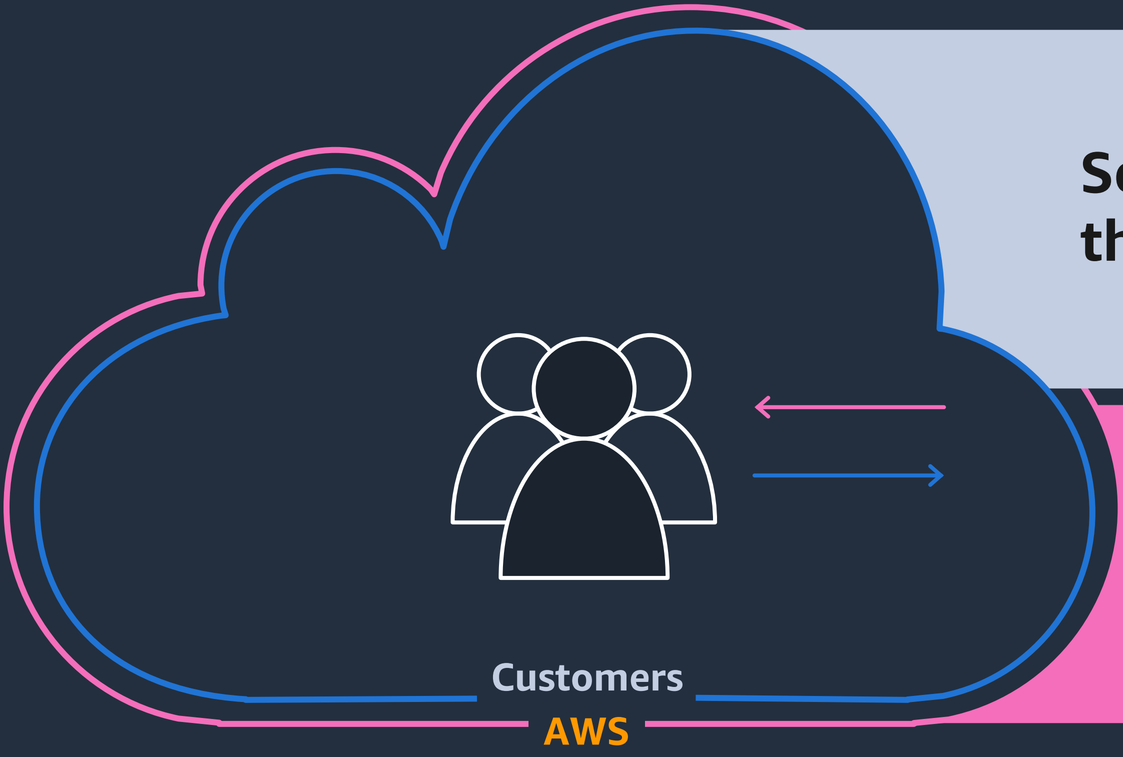
Governance, risk, and compliance

- Booz | Allen | Hamilton
- Cloudgotech
- cavirin
- CloudCheckr
- CloudHealth by vmware
- CloudPassage
- COALFIRE
- DivvyCloud Cloud Automation Reimagined
- ECCOiii 华 讯 网 络
- NTT Data Services
- KindlyOps
- OPTIV
- pwc
- ScaleSec
- Telos
- TREND MICRO
- turbot
- wirewheel
- direktgruppe dg
- stackArmor
- KPMG

Security operations and automation

- Cloudreach
- ECCOiii 华 讯 网 络
- eCloud valley
- IBM Security
- Mphasis The Next Applied
- pwc
- SAMSUNG SAMSUNG SDS

Shared responsibility model



Security IN the Cloud

Customer responsibility is determined by the AWS Cloud services a customer selects.

Security OF the Cloud

AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud.

Identity and access management

Define, enforce, and audit user permissions across AWS services, actions, and resources

AWS Identity and Access Management (IAM)

Securely manage access to AWS services and resources

AWS IAM Identity Center

Centrally manage SSO access to multiple AWS accounts and business apps

AWS Directory Service

Managed Microsoft Active Directory in AWS

Amazon Cognito

Add user sign-up, sign-in, and access control to your web and mobile apps

AWS Organizations

Policy-based management for multiple AWS accounts

AWS Resource Access Manager

Simple, secure service for sharing AWS resources

Amazon Verified Permissions

Fine-grained permissions and authorization for your applications

Detective controls

Gain the visibility you need to spot issues before they impact your business, improve your security posture, and reduce the risk profile of your environment

AWS Security Hub

Automate AWS security checks and centralize security alerts.

Amazon GuardDuty

Protect your AWS accounts with intelligent threat detection.

Amazon Inspector

Automated and continual vulnerability management at scale.

Amazon CloudWatch

Observe and monitor resources and applications on AWS, on premises, and on other clouds.

AWS Config

Assess, audit, and evaluate configurations of your resources.

AWS CloudTrail

Track user activity and API.

VPC Flow Logs

Capture info about IP traffic going to and from network interfaces in your VPC.

Amazon Security Lake

Automatically centralize your security data in a few steps.

Infrastructure protection

Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS

AWS Firewall Manager

Centrally configure and manage firewall rules across your accounts.

AWS Network Firewall

Deploy network firewall security across your VPCs.

AWS Shield

Maximize application availability and responsiveness with managed DDoS protection.

AWS WAF

Protects your web applications from common exploits.

Amazon Virtual Private Cloud

Define and launch AWS resources in a logically isolated virtual network.

AWS PrivateLink

Establish connectivity between VPCs and AWS services without exposing data to the internet.

AWS Systems Manager

Gain operational insights into AWS and on-premises resources.

AWS Verified Access

Provide secure access to corporate applications without a VPN.

Data protection

A suite of services designed to automate and simplify many data protection and security tasks ranging from key management and storage to credential management.

Amazon Macie

Discover and protect your sensitive data at scale.

AWS Key Management Service (AWS KMS)

Create and control keys used to encrypt or digitally sign your data.

AWS CloudHSM

Manage single-tenant hardware security modules (HSMs) on AWS.

AWS Certificate Manager

Provision and manage SSL/TLS certificates with AWS services and connected resources.

AWS Secrets Manager

Centrally manage the lifecycle of secrets.

AWS VPN

Connect your on-premises networks and remote workers to the cloud.

Server-Side Encryption

Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys.

AWS Private CA

Create private certificates to identify resources and protect data.

Incident response

During an incident, containing the event and returning to a known good state are important elements of a response plan. AWS provides the following tools to automate aspects of this best practice.

Amazon Detective

Analysis and visualization of security data to get to the root cause of potential security issues quickly

Amazon EventBridge

Serverless event bus that makes it easier to build event-driven applications to scale your programmed, automated response to incidents

AWS Backup

Centrally manage and automate backups across AWS services to simplify data protection at scale

AWS Security Hub

Out-of-the-box integrations with ticketing, chat, SIEM, SOAR, threat investigation, incident management, and GRC tools to support your security operations workflows

AWS Elastic Disaster Recovery

Fast, automated, cost-effective disaster recovery

Compliance

AWS supports security standards and compliance certifications to help you satisfy compliance requirements for virtually every regulatory agency around the globe.

AWS Artifact

No-cost, self-service portal for on-demand access to AWS compliance reports

AWS Audit Manager

Continuously audit your AWS usage to simplify how you assess risk and compliance