Security & Compliance

Securing your account, services & applications

- Account Security: It’s More Than IAM
- Securing Applications, Traffic & Data
- Reacting To Threats & Handling Incidents

ACADEMIND

Security Matters – Everywhere

Account Protection

- Account must not get compromised
- Prevent malicious account / service usage
- Secure cross-account service usage

Compliance & Standardization

- Single Sign-On, service config, compliance reports

Application Protection

- Detect application / software vulnerabilities
- Detect insecure configurations
- Investigate security issues & incidents

Network Protection

- Detect malicious network traffic
- Protect against DDoS attacks

Data Protection

- Encrypt data at rest & in transit
- Protect code secrets
- Prevent unintended data exposure

Security Matters – Everywhere

Account Protection

- IAM & SSO
- CloudTrail
- GuardDuty
- RAM
- Organizations

Compliance & Standardization

- Artifact
- Config, Audit M.

Application Protection

- Inspector
- Detective

Network Protection

- WAF
- Network Firewall
- Firewall Manager
- Shield

Data Protection

- KMS, CloudHSM
- Secrets Manager
- ACM
- Macie

Managing Permissions with IAM

Manage Identities & Access Rights

Define & Manage Identities	Control Permissions
Users, user groups & roles	Permissions are defined via policies
Attach permissions (policies) to identities	Pre-defined policies provided by AWS
By default: No permissions are added to any identity	You can create your own policies
Explicit deny > explicit allow	Multiple policies can be combined

User Authentication

Single Sign-On & Active Directory

Single Sign-On

Simplify signing into AWS accounts

Use AWS credentials or other sources

AWS Directory Service

Use Active Directory for authentication

Helps with connection or migrating AD workloads

Track & Protect Account Usage

Prevent Malicious Usage

Track API Usage

CloudTrail allows you to track AWS API calls

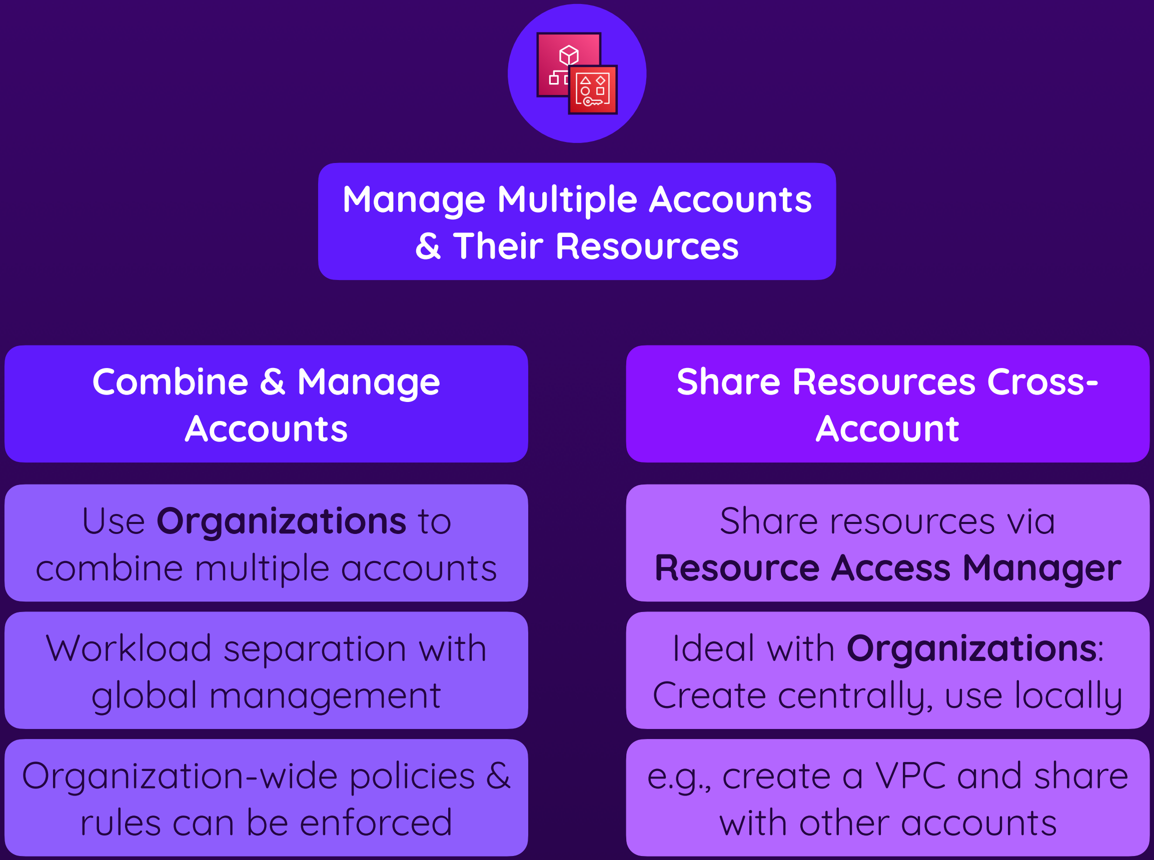
Identify identities and their actions

Detect Malicious Patterns

Detect suspicious behavior via **GuardDuty**

Uses machine learning to detect and surface issues

Cross-Account Service Usage



Manage Multiple Accounts & Their Resources

Combine & Manage Accounts

Use **Organizations** to combine multiple accounts

Workload separation with global management

Organization-wide policies & rules can be enforced

Share Resources Cross-Account

Share resources via **Resource Access Manager**

Ideal with **Organizations**: Create centrally, use locally

e.g., create a VPC and share with other accounts

Stay Compliant & Meet Legal Requirements

Enforce & Prove Compliance

Enforce Compliance & Best Practices

- Use **AWS Config** to define & track service configuration
- Enforce organization policies & guidelines
- Monitor & resolve configuration deviations

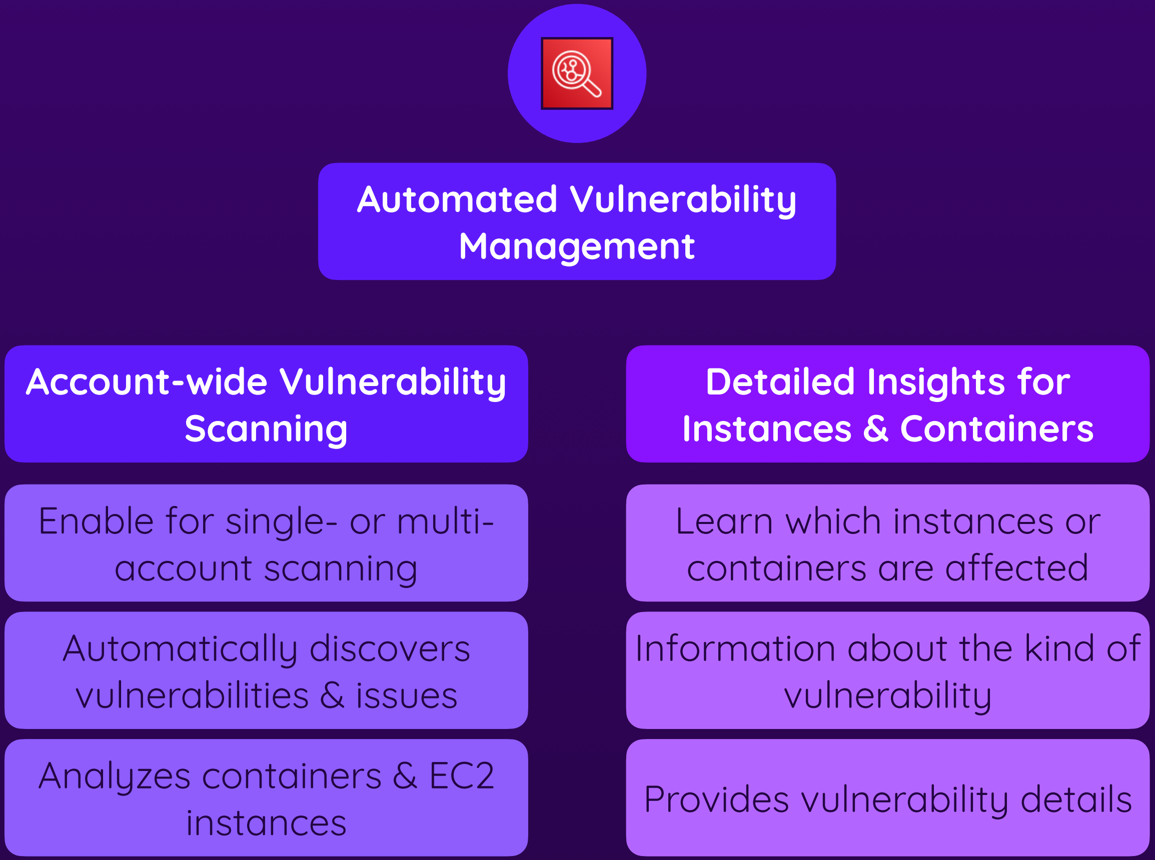
Prove AWS Compliance

- Download compliance reports via **AWS Artifact**
- Prove AWS compliance with regulations & rules

Prove Your Compliance

- Track compliance issues with **Audit Manager**
- Generate auditor-friendly reports
- Connect with AWS Config for data collection

Protecting Applications with Inspector



Automated Vulnerability Management

Account-wide Vulnerability Scanning

- Enable for single- or multi-account scanning
- Automatically discovers vulnerabilities & issues
- Analyzes containers & EC2 instances

Detailed Insights for Instances & Containers

- Learn which instances or containers are affected
- Information about the kind of vulnerability
- Provides vulnerability details

Manage Incidents with Detective

Investigate Incidents

Explore AWS Resources

- Search for users, instances, roles & more
- Explore actions by / on resource
- Get a list of automatic findings

Analyze Findings & Actions

- Explore finding details (date, involved resources, …)
- Explore details for suspicious activity

Analyzing Network Traffic with Firewalls

Blocking Unwanted Traffic

Web App Firewall (WAF)	Network Firewall
Inspect HTTP(S) traffic and block it based on content	Inspect any traffic and protect entire networks
Analyze metadata & request bodies	Analyze IPs, ports, protocol etc.
Define rules for blocking traffic	Define stateful or stateless rules for blocking traffic

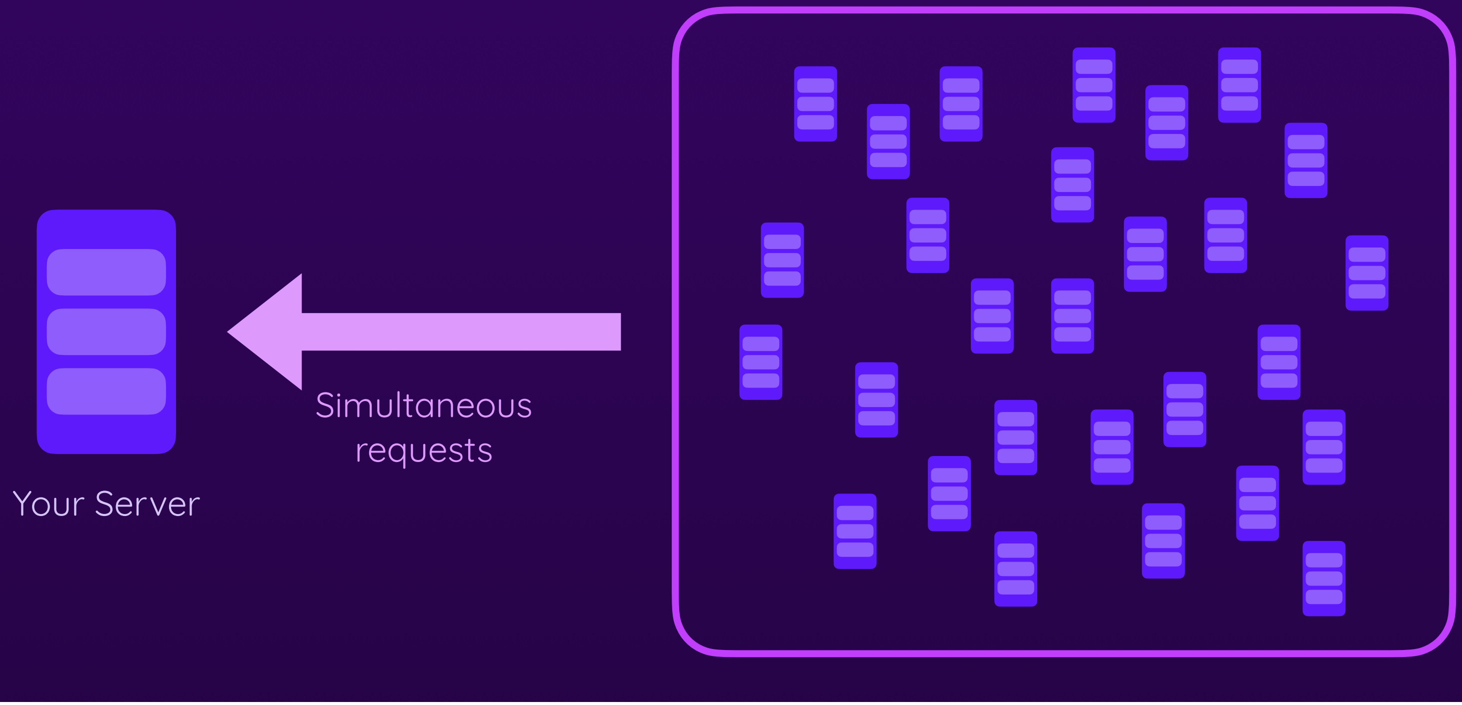
Global Firewall Management via **Firewall Manager**

Avoid DDoS Attacks

Distributed Denial of Service

An attacker sends a huge amount of simultaneous requests to your server

Typically via a network of (hacked) bot machines

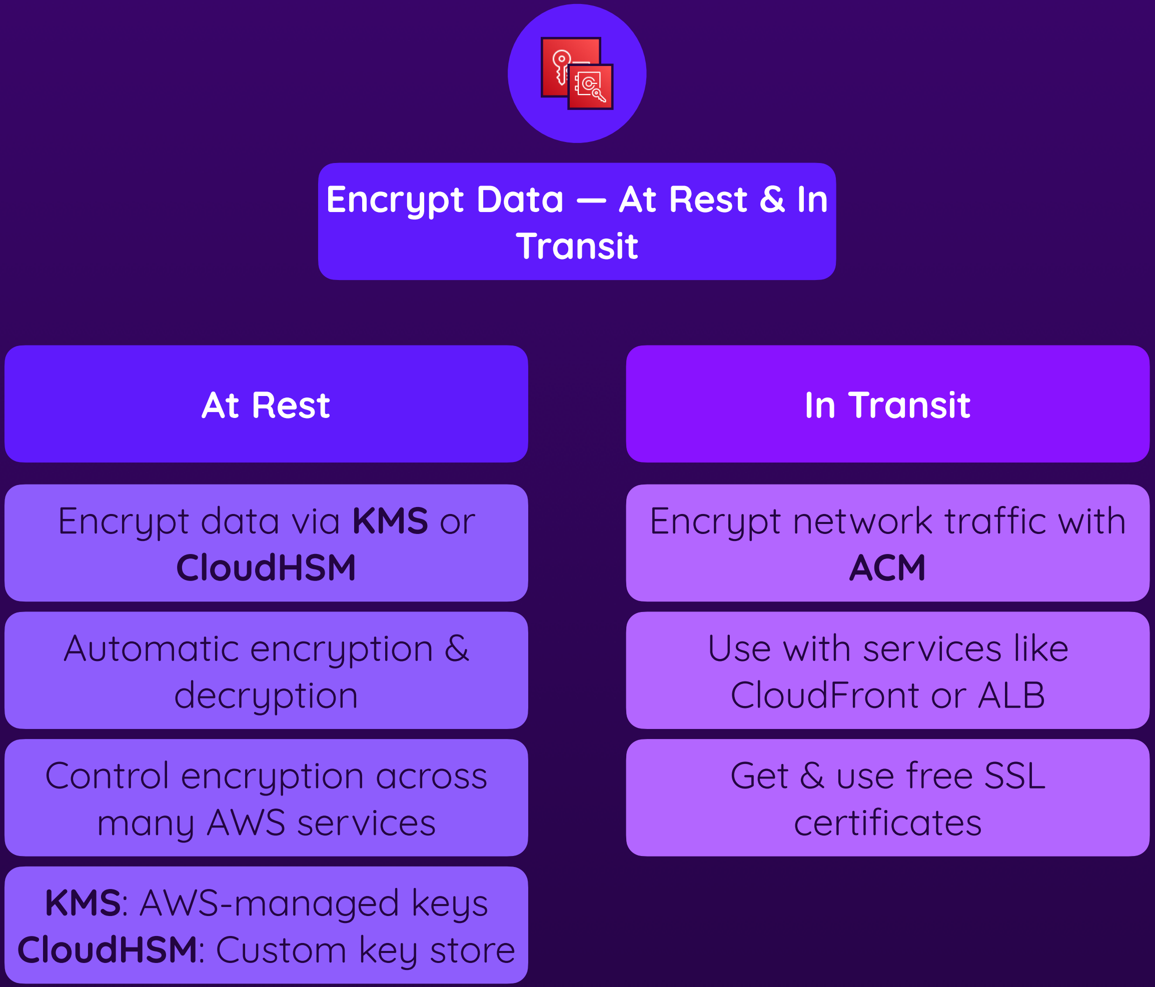


Protecting Against DDoS Attacks

DDoS Protection via Shield

AWS Shield Standard	AWS Shield Advanced
Free & enabled by default	Monthly cost, not enabled by default
Basic DDoS protection based on network flow	Customizable protection rules
No anomaly detection	Anomaly detection & dedicated AWS support

Encrypting Data



Encrypt Data — At Rest & In Transit

At Rest	In Transit
Encrypt data via **KMS** or **CloudHSM**	Encrypt network traffic with **ACM**
Automatic encryption & decryption	Use with services like CloudFront or ALB
Control encryption across many AWS services	Get & use free SSL certificates
KMS: AWS-managed keys **CloudHSM**: Custom key store	

Managing Code & Application Secrets

Securely manage Secret Parameter Values

Manage Secrets

- Securely store secret values with **Secrets Manager**
- Built-in auto-rotation support for RDS & more
- Control access permissions

Use Secrets

- Access secret values from inside application code
- Access or set secrets via other services

ACADEMIND

Protecting Sensitive Data with Amazon Macie

Discover Data Protection Issues with Amazon Macie

Configure & Use

- Detect sensitive data via machine learning
- Add custom-defined sensitive data types
- Scan data on demand or on a schedule

Monitor & Discover

- Macie highlights exposed or unprotected sensitive data
- e.g., detect unencrypted or public sensitive data

Using Security Hub

Consolidated Security Status Management

Consolidate Other Security Services

- Group GuardDuty, Inspector & Macie output
- Control security service behavior centrally

Take Action

- Take action across services & accounts
- Build customized actions

ACADEMIND

Summary

Security Matters — Always!

A secure cloud environment is a combination of things

Protect your account & ensure compliance

Protect applications, traffic & data (and therefore your users)

Use different services & service combinations for full protection

Account Security & Compliance

Use **IAM** for managing identities & permissions

Use **CloudTrail** & **GuardDuty** to detect & track suspicious actions

Use **SSO** & **Managed Directory Service** for advanced login

Use **Organizations** & **RAM** to manage multi-account setups

Be compliant with **Artifact**, **Audit Manager** & **AWS Config**

Application, Traffic & Data Security

Secure applications with **Inspector** & **Detective**

Secure traffic with Firewalls (**WAF**, **Network Firewall** & more)

Protect against DDoS with **Shield**

Encrypt your data with **KMS** or **CloudHSM**

Protect data with **Secrets Manager** & **Macie**