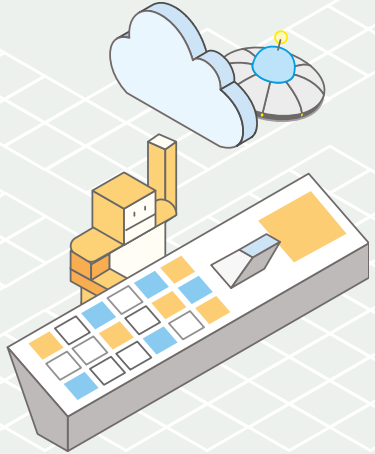
Enabling Compliance with the General Data Protection Regulation (GDPR) on AWS

Ronan Guilfoyle, Solutions Architect

April 2018



What is the GDPR?

What is the GDPR?

- The "GDPR" is the General Data Protection Regulation, a significant new EU Data Protection Regulation
- Introduces robust requirements that will raise and harmonize standards for data protection, security, and compliance across the EU
- The GDPR is enforceable **May 25th, 2018** and it replaces the EU Data Protection Directive (Directive 95/46/EC)
- Territorial scope: Organisations established in the EU and Organisations without an EU presence who target or monitor EU individuals

Content vs. Personal Data

Content

= anything that a customer (or any end user) stores, or processes using AWS services, including:

Software | Data | Text | Audio | Video

Personal Data

= information from which a living individual may be ***identified*** or ***identifiable*** (under EU data protection law)

- Customer's "content" might include "personal data"

What Else Comes With GDPR?

The Right to Data Portability | The Right to Be Forgotten | Privacy By Design | Data Breach Notification

Individuals have the right to a copy of all the personal data that **controllers** have regarding him or her. It also must be provided in a way that facilitates reuse.

What Else Comes With GDPR?

The Right to Data Portability | **The Right to Be Forgotten** | **Privacy By Design** | **Data Breach Notification**

This gives individuals the right to have certain personal data deleted so third parties can no longer trace them.

What Else Comes With GDPR?

The Right to Data Portability | **The Right to Be Forgotten** | **Privacy by Design** | **Data Breach Notification**

This helps to facilitate the inclusion of policies, guidelines, and work instructions related to data protection in the earliest stages of projects including personal data.

What Else Comes With GDPR?

The Right to Data Portability | **The Right to Be Forgotten** | **Privacy By Design** | **Data Breach Notification**

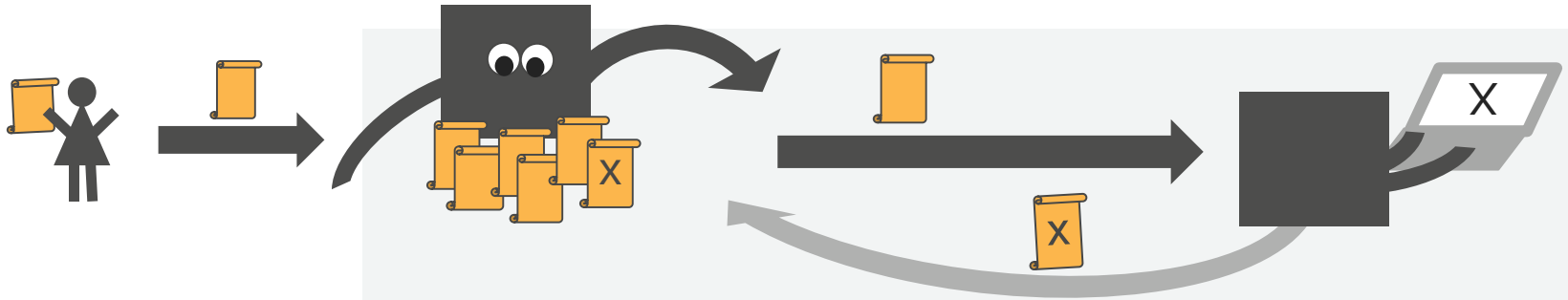
Controllers must report personal data breaches to the relevant supervisory authority within 72 hours. If there is a high risk to the rights and freedoms of data subjects, they must also notify the data subjects.

Potential Consequences

- Penalties – Apply to both controllers and processors
- Fines of up to **€20,000,000** or **4% of global turnover**
- Fines will be *dissuasive*
- Claims from individuals and class action suits

How AWS Can Help Customers Achieve GDPR Compliance

Security of Content and Data Breaches



Data Subject

Controller

Must implement appropriate technical and organizational measures (“TOMs”)

Must monitor own environment

Must notify regulators and data subjects

Processor

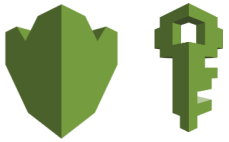
Content agnostic
Own TOMs

GDPR in Practice: Implementing TOMs

Under GDPR **Controllers** and **Processors** are required to implement appropriate Technical and Organization Measures (“TOMs”)

1) Pseudonymisation and encryption of personal data	**(2) Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services**
(3) Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident	**(4) Process for regularly testing, assessing, and evaluating the effectiveness of TOMs**

What AWS Provides



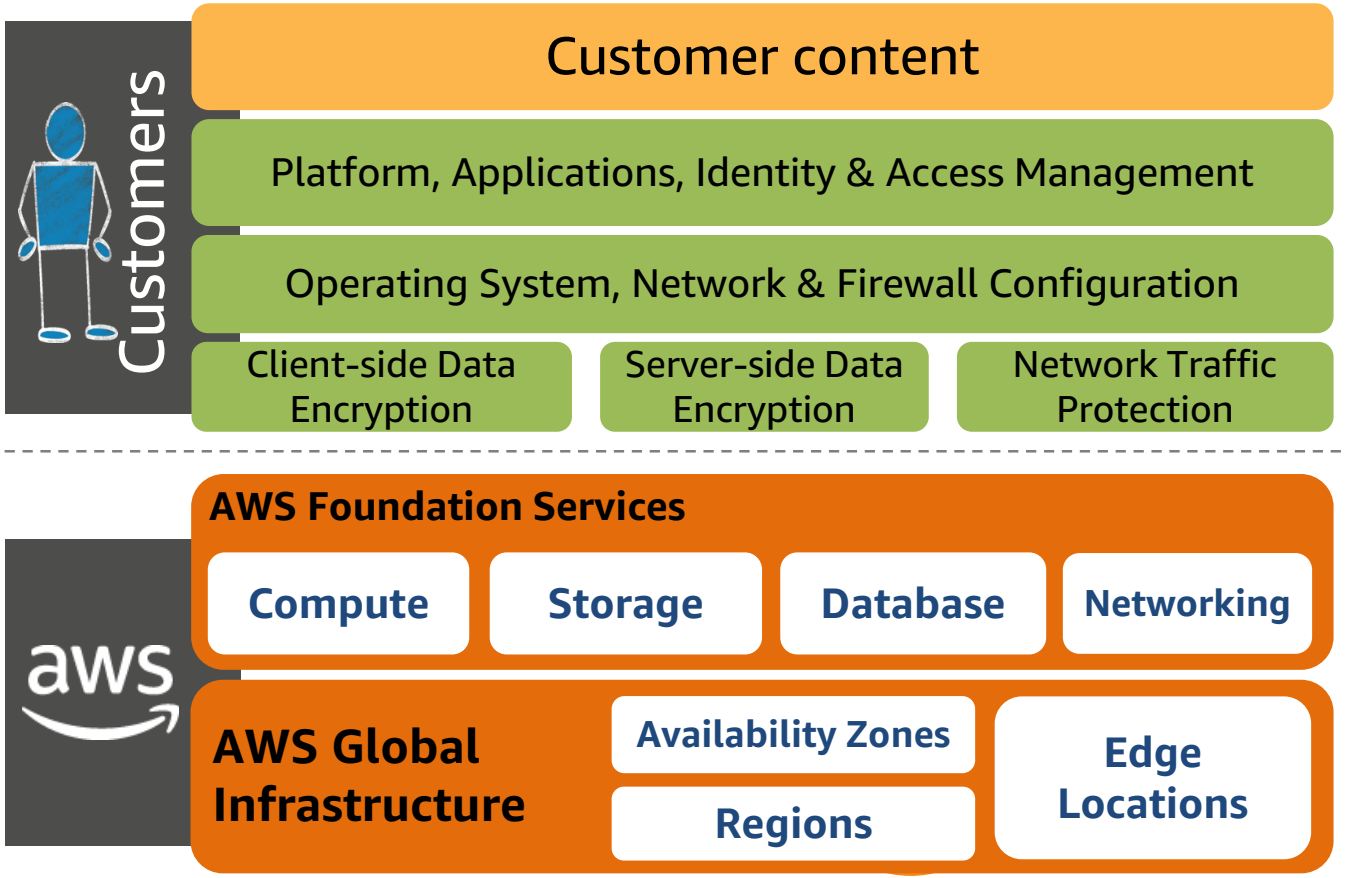
Tools and Services

Compliance Framework

Partner Network

Data Protection Contract

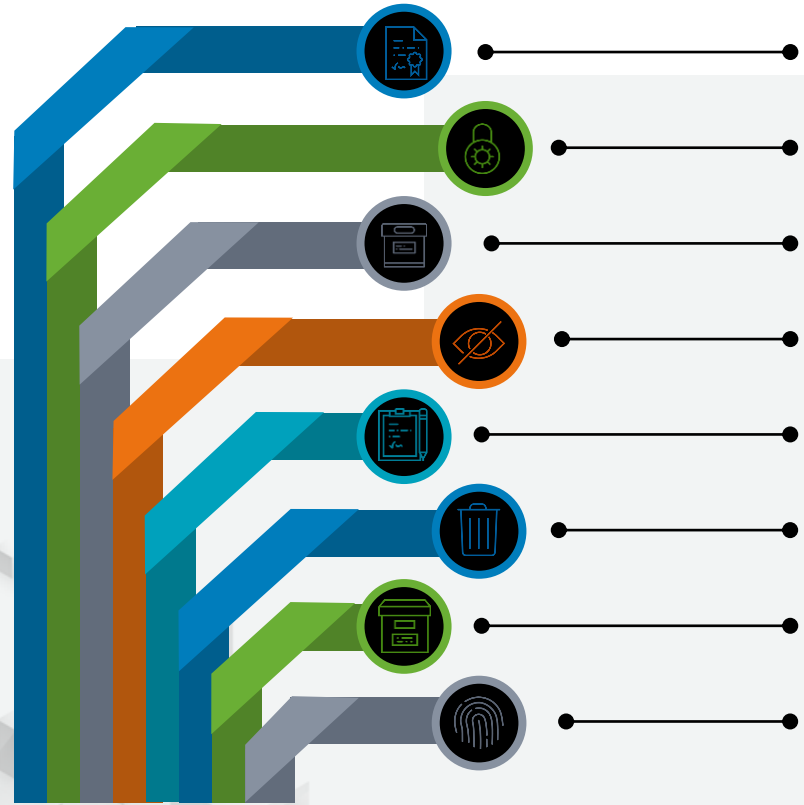
AWS Shared Responsibility Model



Customers are responsible for their security and compliance **IN** the Cloud

AWS is responsible for the security **OF** the Cloud

GDPR is also a “Shared Responsibility”



Legal Compliance
(both controllers and processors)

System Security and Data Protection by Design
(both controllers and processors; AWS has tooling to help)

Records of Processing Activities
(both controllers and processors; AWS has tooling to help)

Encryption
(both controllers and processors; AWS has have tooling to help)

Managing Data Subject Consent
(controller responsibility)

Managing Personal Data Deletion
(both controllers and processors; AWS has tooling to help)

Managing Personal Data Portability
(controller responsibility)

Security of Personal Data
(controller responsibility)

Navigating GDPR Compliance

'Data protection by design and default'

Amazon Snowball

Amazon API Gateway

Amazon Virtual Private Cloud (VPC)

AWS Identity and Access Management

Active Directory Integration

SAML Federation

'Security of processing'

AWS KMS

AWS CloudHSM

Server-side Encryption

'Records of processing activities'

AWS Service Catalog

AWS CloudTrail

AWS Config

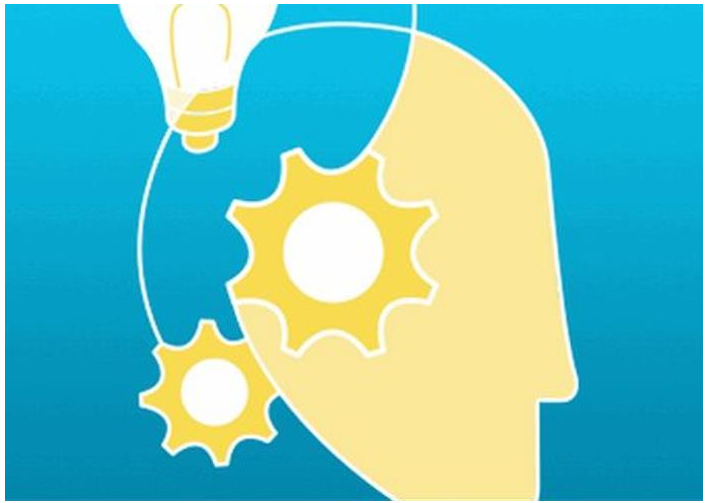
Automating Security

Goal

Ensure ongoing **confidentiality**, **integrity**, **availability**, and **resilience** of processing systems and services

Automating Security

There are multiple ways to assess and evaluate infrastructure against best practices …

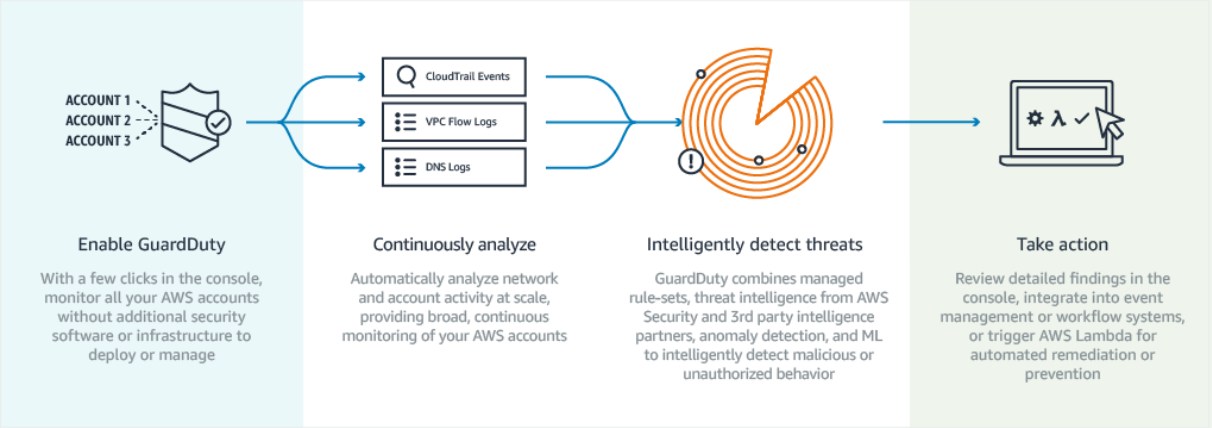


How?

AWS & The GDPR

Amazon GuardDuty

Managed threat detection service that continuously monitors for malicious or unauthorized behavior



AWS & The GDPR

Amazon GuardDuty

Detects items such as:

- Unusual API calls
- Potentially unauthorized deployments that indicate a possible account compromise
- Potentially compromised instances or reconnaissance by attackers

AWS & The GDPR

Amazon GuardDuty

Integrate with Amazon CloudWatch Events for:

- Alerting
- Remediation

AWS & The GDPR

Amazon Macie

Security service that uses machine learning to continuously and automatically discover, classify, and protect sensitive data in AWS

AWS & The GDPR

Amazon Macie

Recognizes and classify sensitive data such as:

- Personally identifiable information (PII)
- Intellectual property
- Sensitive AWS Account information

AWS & The GDPR

Amazon Macie

Powerful research functionality

- Find individual record types
    - Where do I have IPv4 addresses?
- Tie research to Alerting
    - Tell me when you find source code
    - Tell me when you find open S3 bucket

AWS & The GDPR

Amazon Macie

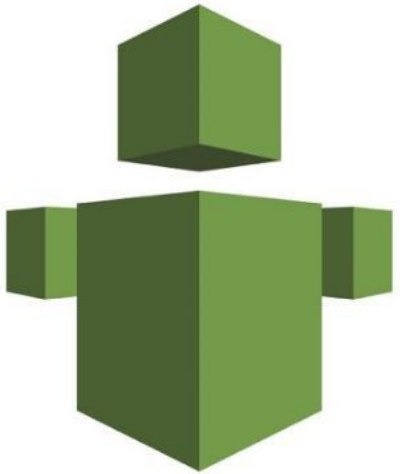
Automation

- Tie Research -> Alerting -> Automation
- If AWSCred: disable keys

AWS & The GDPR

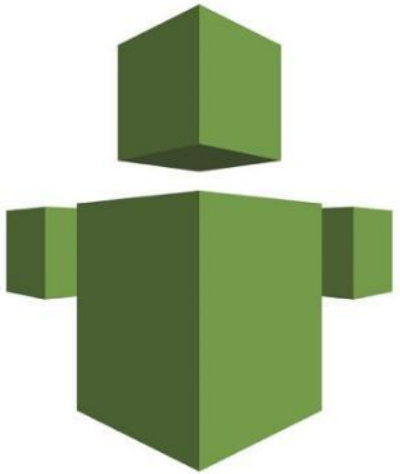
Amazon Trusted Advisor

Helps you reduce cost, increase performance, and improve security by providing real-time guidance to help you provision your resources following AWS best practices



AWS & The GDPR

Amazon Trusted Advisor

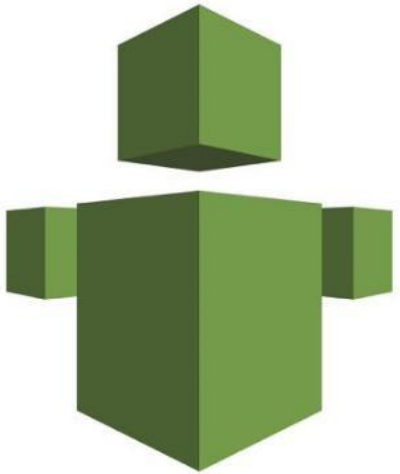


Comes with pre-baked controls around

- Unrestricted security groups
- MFA not on root accounts
- Publically exposed AWS credentials

AWS & The GDPR

Amazon Trusted Advisor



Integrated with CloudWatch Events

Build automation for things like

- Exposed keys
    - Auto disable?
- Security Groups
    - Alert?

AWS & The GDPR

Amazon and OSS

Example:

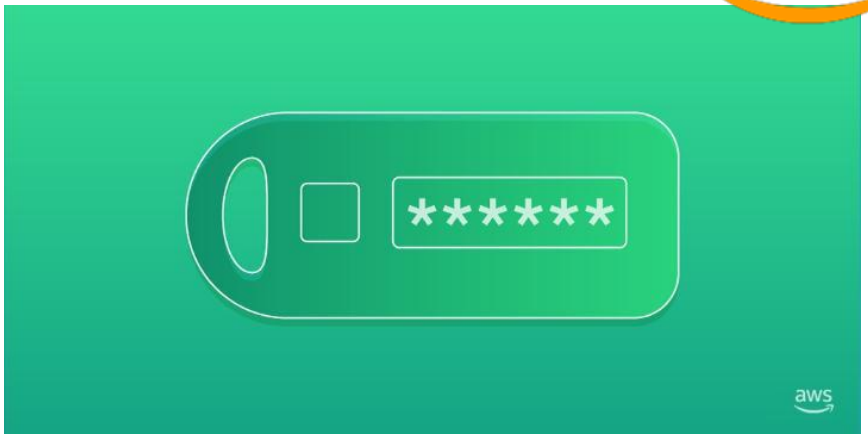
CIS AWS benchmarks

Purpose:

Allows you to continuously or spot evaluate the configuration of resources and account settings of an AWS account against the CIS AWS Foundation Benchmark

AWS & The GDPR

Amazon and OSS



Example:
CIS AWS benchmark assessment

Provides:
Assess against 48 control statements. Including

- No multi-factor authentication (MFA) usage on the root account
- Overly open IAM policies
- Lack of enabled logging on the account

AWS & The GDPR

Amazon and OSS

Example:

CIS AWS benchmark assessment

Provides:

Single report with assessment resu

AWS CIS Foundation Framework

Report date: Wed Dec 7 11:47:34 2016
Benchmark version: 1.1
Whitepaper location: https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf
{"Failed":["1.3", "1.4", "1.5", "1.6", "1.7", "1.8", "1.9", "1.10", "1.11", "1.14", "1.16", "1.22", "1.23", "2.2", "2.4", "2.5", "2.6", "2.6", "2.8", "3.1", "3.2", "3.3", "3.4", "3.5", "3.6", "3.7", "3.8", "3.9", "3.10", "3.11", "3.12", "etc"]}

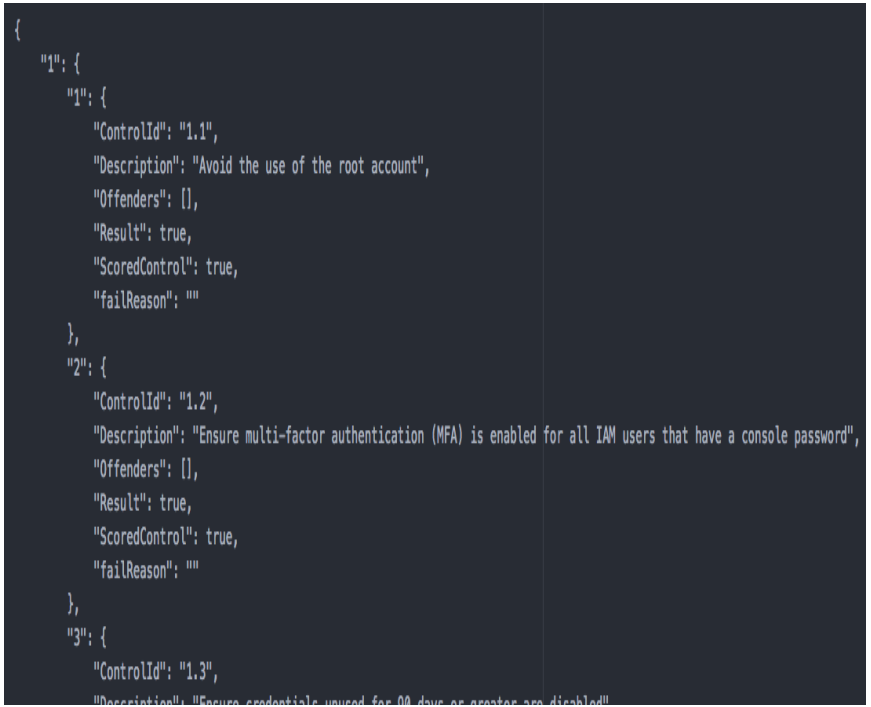
1		
	1	
		ControlId 1.1
		Description Avoid the use of the root account
		failReason
		Offenders []
		Result True
		ScoredControl True
	2	
		ControlId 1.2
		Description Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
		failReason
		Offenders []
		Result True
		ScoredControl True
	3	
		ControlId 1.3
		Description Ensure credentials unused for 90 days or greater are disabled
		failReason Credentials unused > 90 days detected.
		Offenders ['arn:aws:iam::111111111111:user/IAM-API-RO:key1', 'arn:aws:iam::111111111111:user/IAM-API-RW:key2', 'arn:aws:iam::111111111111:user/IAM-Demo:key1', 'arn:aws:iam::111111111111:user/IAM-SWF-SecLab:key1']
		Result False

AWS & The GDPR

Amazon and OSS

Example:
CIS AWS benchmark assessment

Provides:
Ability to integrate with other tools using standard JSON output



AWS & The GDPR

Amazon and OSS

Plenty of Code Out There!

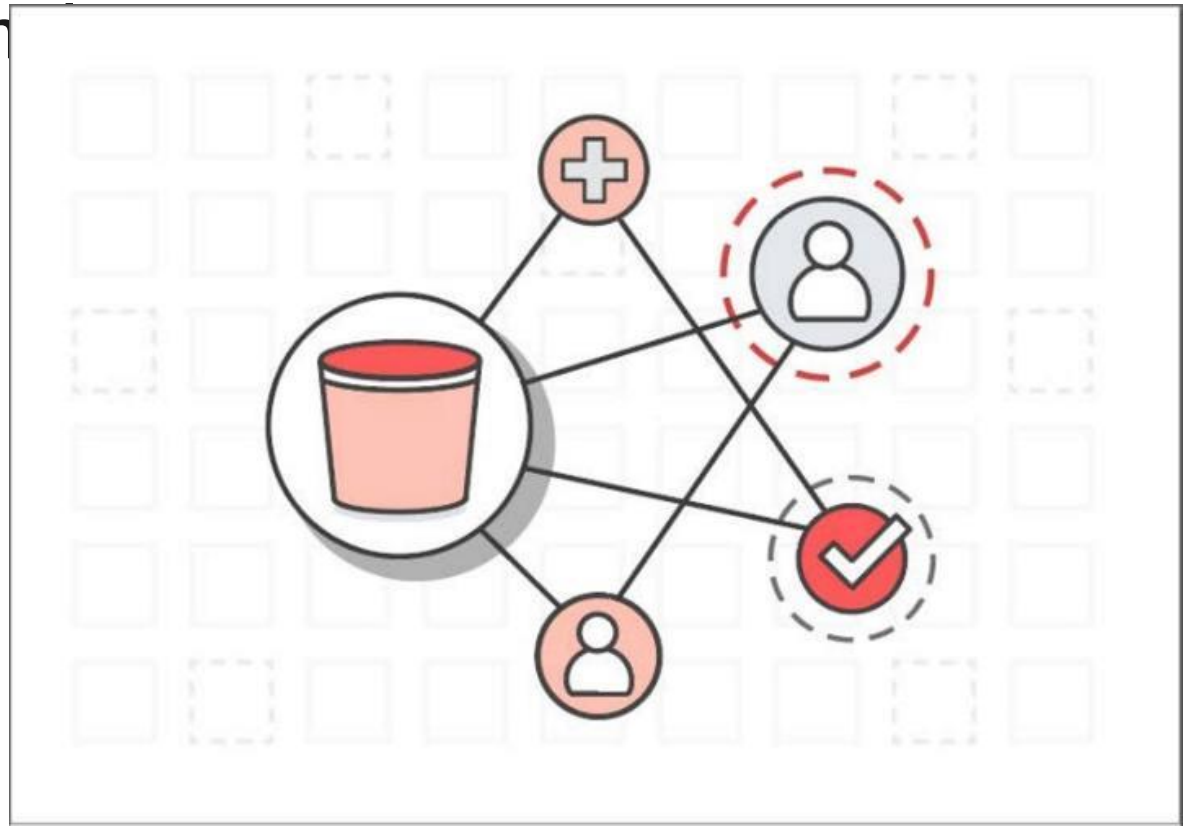
AWS

http://github.com/awslabs
http://github.com/awslabs/aws-security-automation
https://github.com/awslabs/aws-security-benchmark

Non-AWS

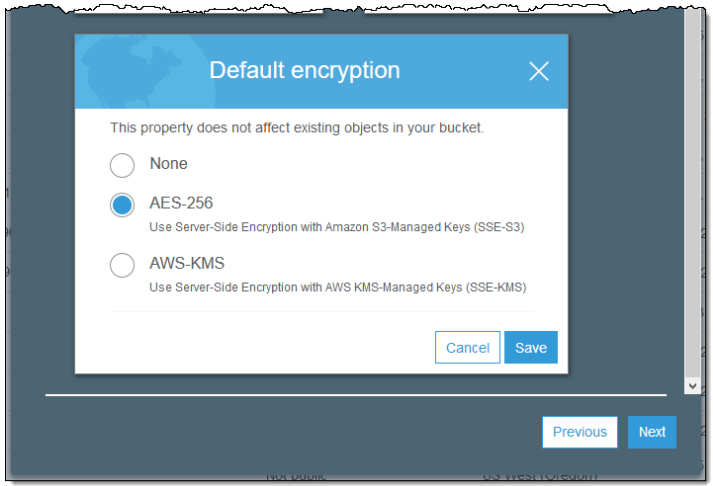
- ThreatResponse.cloud - https://threatresponse.cloud
- Cloud Custodian- https://github.com/capitalone/cloud-custodian
- Security Monkey - https://github.com/Netflix/security_monkey
- FIDO - https://github.com/Netflix/Fido
- CloudSploit - https://github.com/cloudsploit
- Prowler - https://github.com/Alfresco/prowler
- StreamAlert - https://github.com/airbnb/streamalert

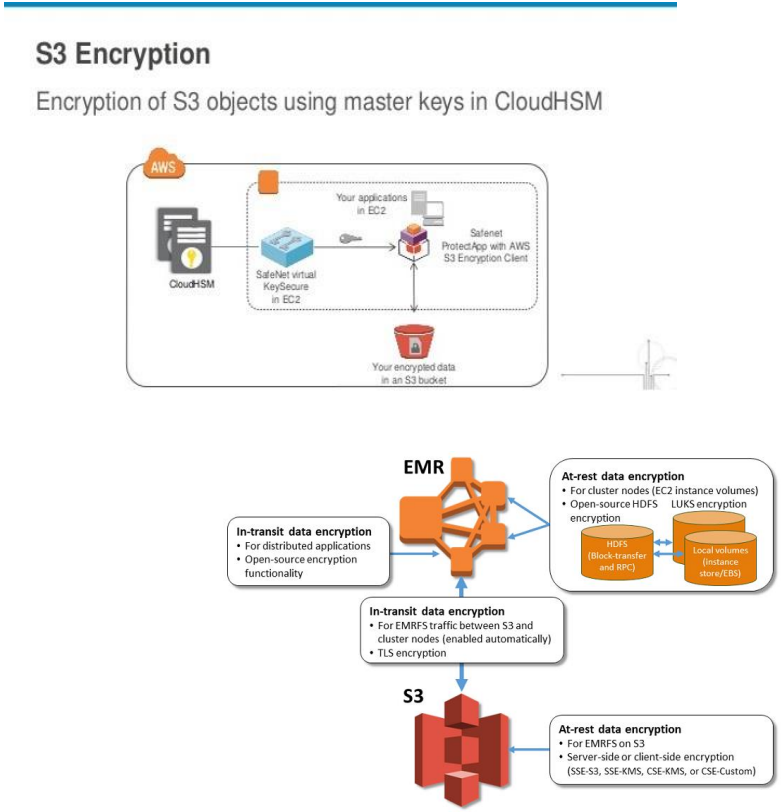
AWS & The GDPR – Addition



AWS & The GDPR

Encryption





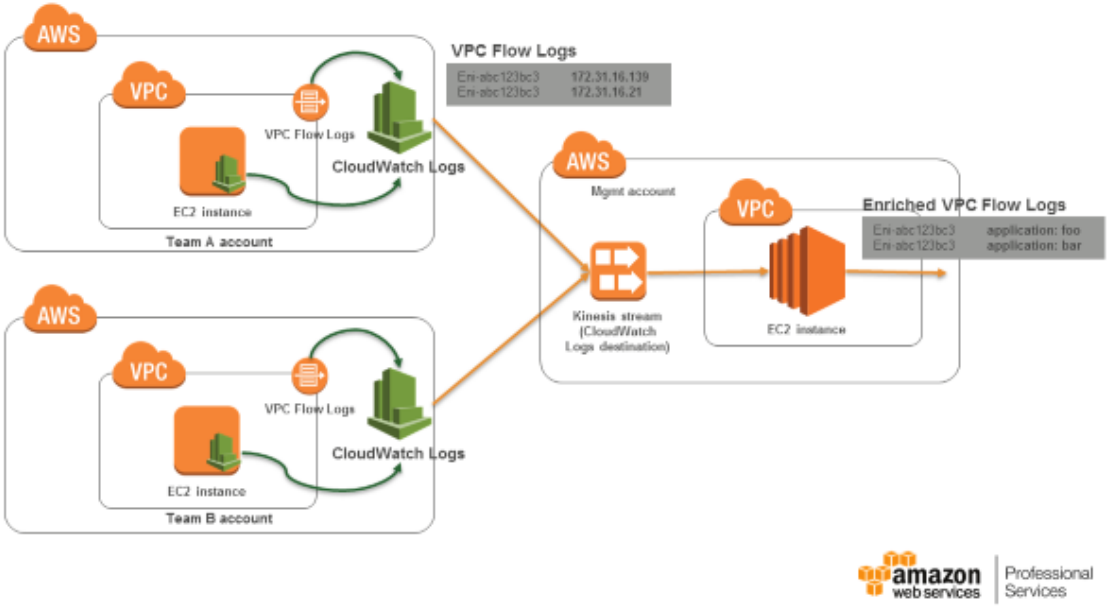
AWS & The GDPR

Amazon Key Management Service (KMS)

Keys managed centrally in Amazon KMS with permissions and auditing of usage

AWS & The GDPR

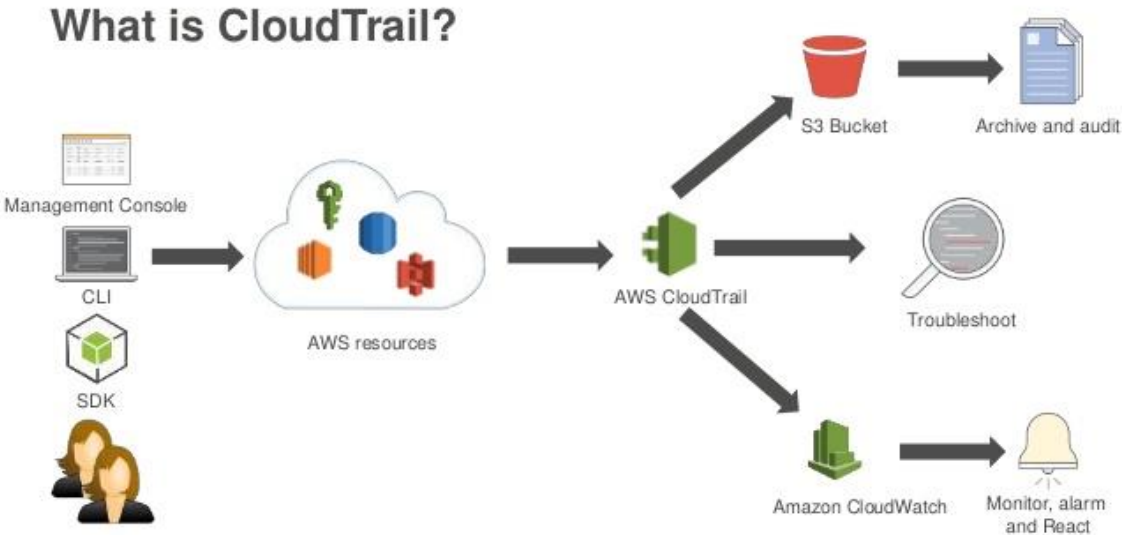
Monitoring & Logging



amazon web services | Professional Services

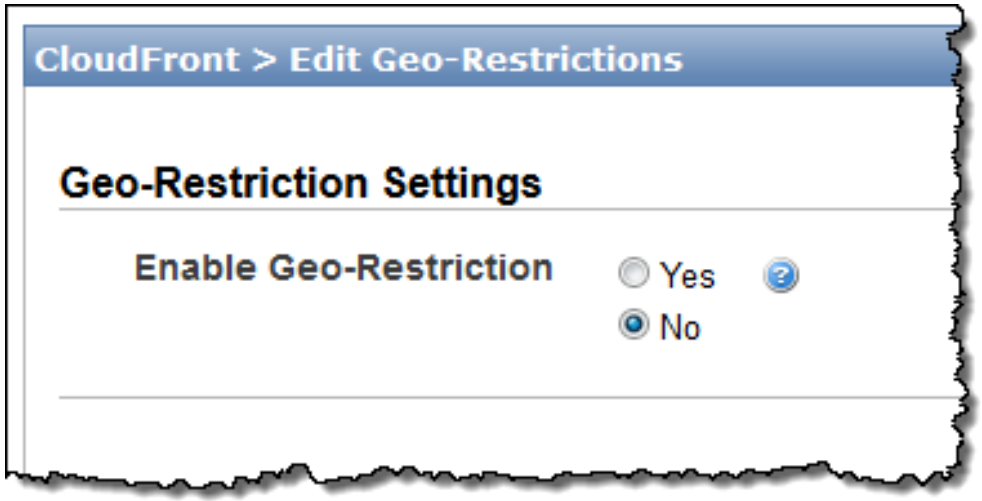
AWS & The GDPR

Monitoring & Logging



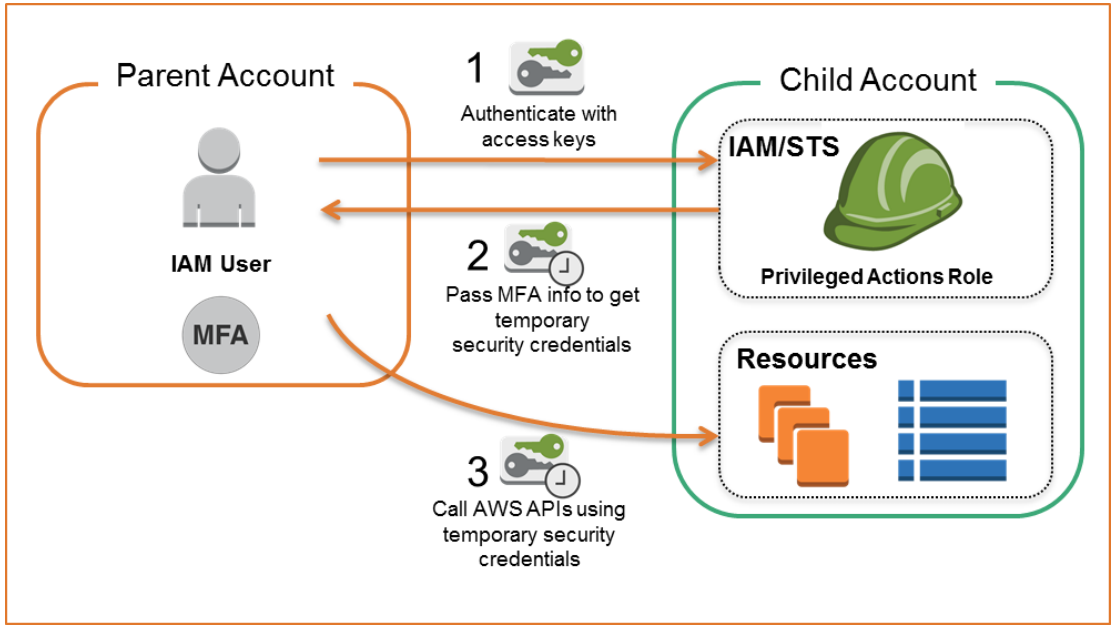
AWS & The GDPR

Access Control

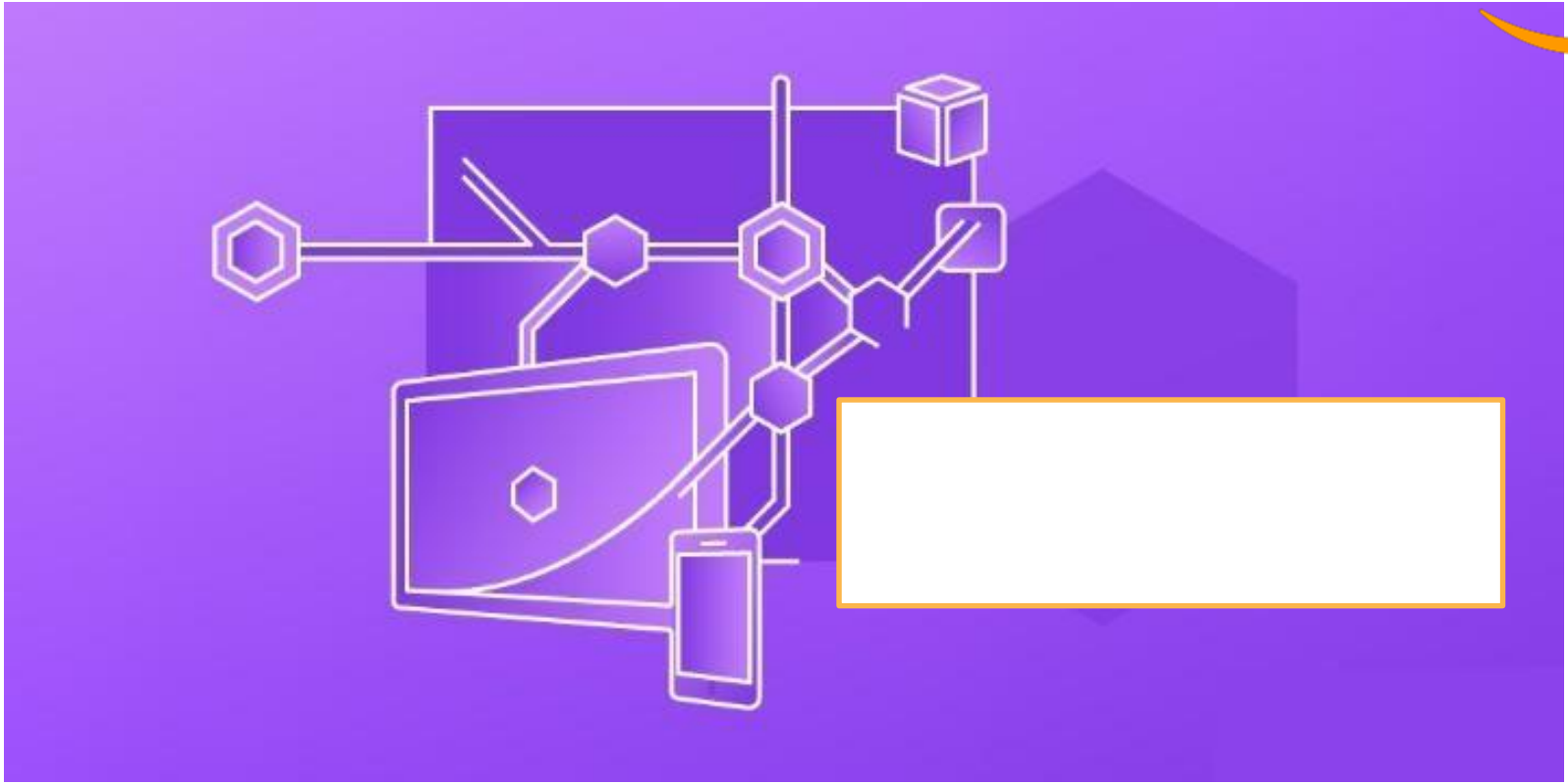


AWS & The GDPR

Access Control



AWS & The GDPR



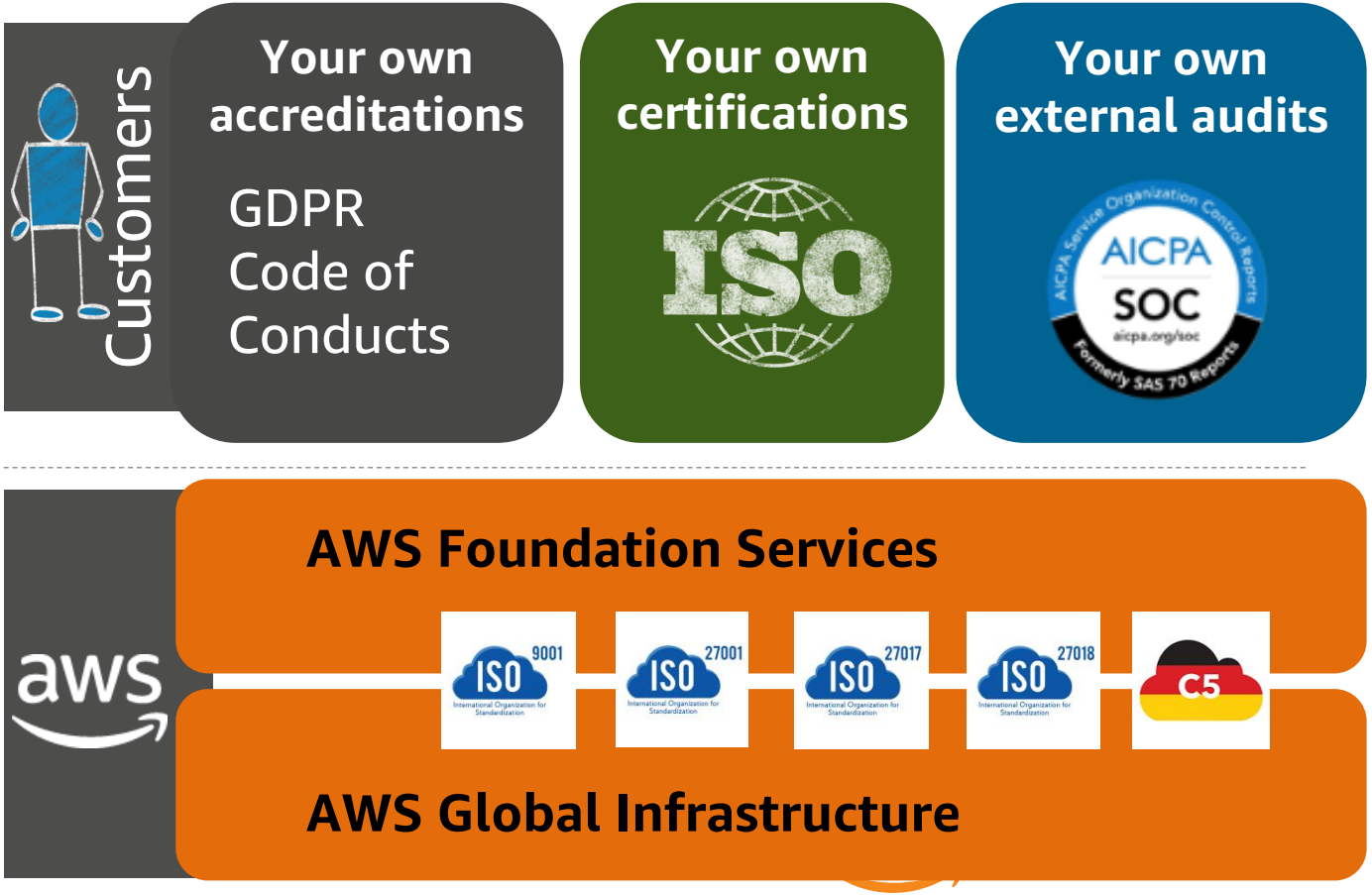
AWS & The GDPR

Data Protection by Default

We have developed a security assurance program using additional global privacy and data protection best practices in order to help customers establish, operate and leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

- ISO 27001/9001 certified
- ISO 27017/27018 certified
- Cloud Computing Compliance Controls Catalog (C5)

Meet Your Own Security Objectives



Customer scope and effort is reduced

Better results through focused efforts

Built on AWS consistent baseline controls

AWS Marketplace: One Stop Shop for Familiar Tools

aws

Professional Services: Privacy-by-Design Offering

All AWS Services are now GDPR ready

Will your services be ready? What will that require?

AWS will help **educate** and **enable** customers to architect their AWS environment to support data protection and privacy

Scope of Work Includes

Review current AWS architecture
Educate on AWS services & defined controls
Recommend Partners and Solutions who can support/provide technical solutions

Contact Us: aws-proserve-src-gdpr@amazon.com

AWS Partner Network (APN) & GDPR

Consulting Partners

APN consulting partners can help your customers get ready for GDPR.

Technology Partners

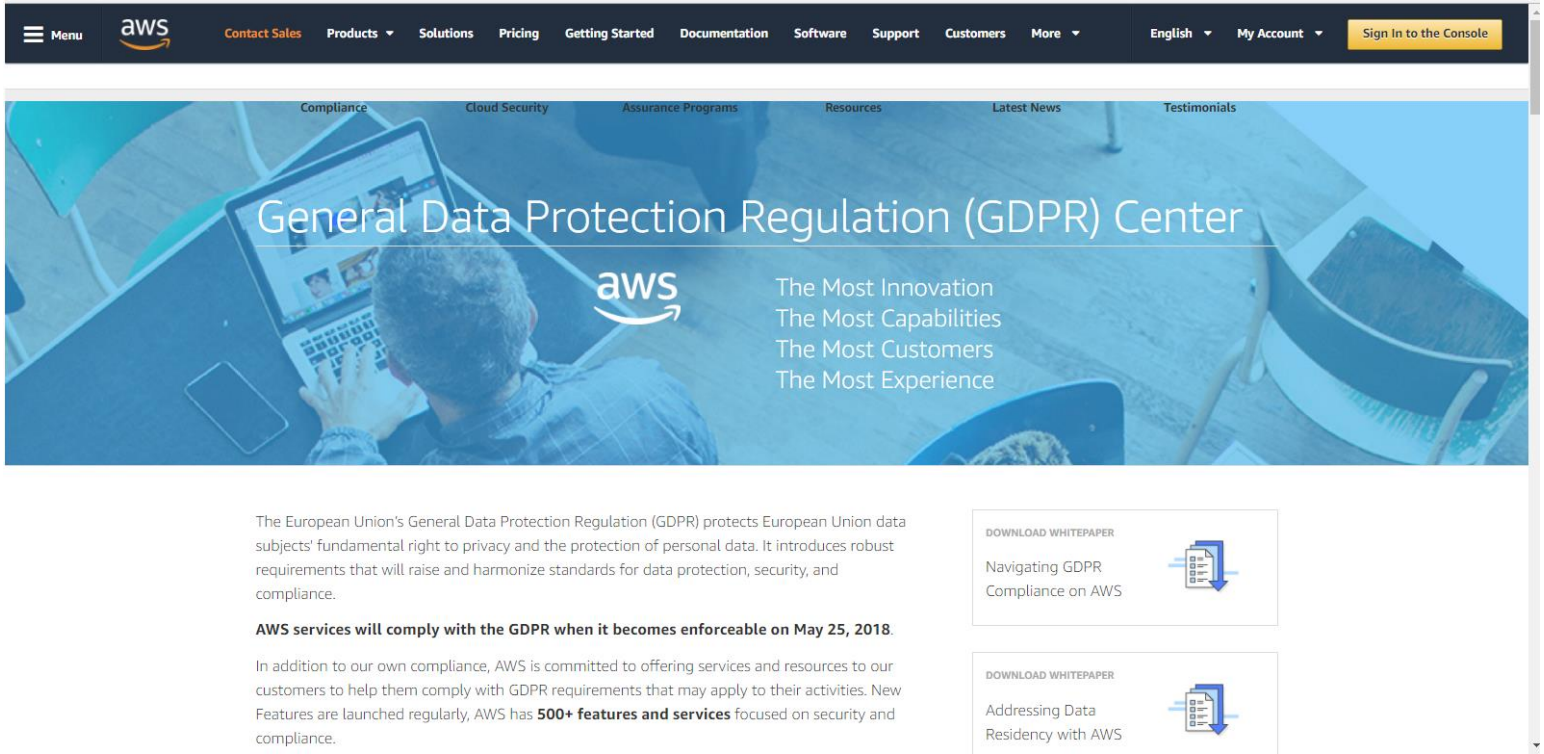
APN technology partners offer security & identity solutions.

Deloitte. direktgruppe dg sopra steria

/

BigID FORTINET evident.io

AWS & The GDPR



https://aws.amazon.com/compliance/gdpr-center/