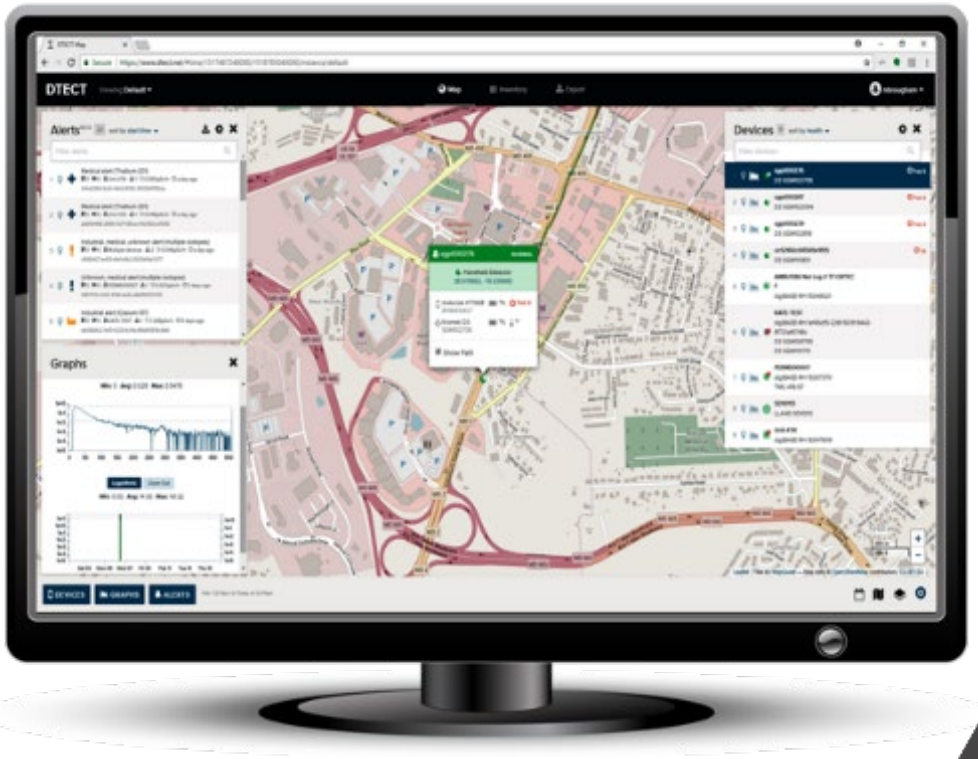
kromek
detect image identify



D3S NET Cloud System Information

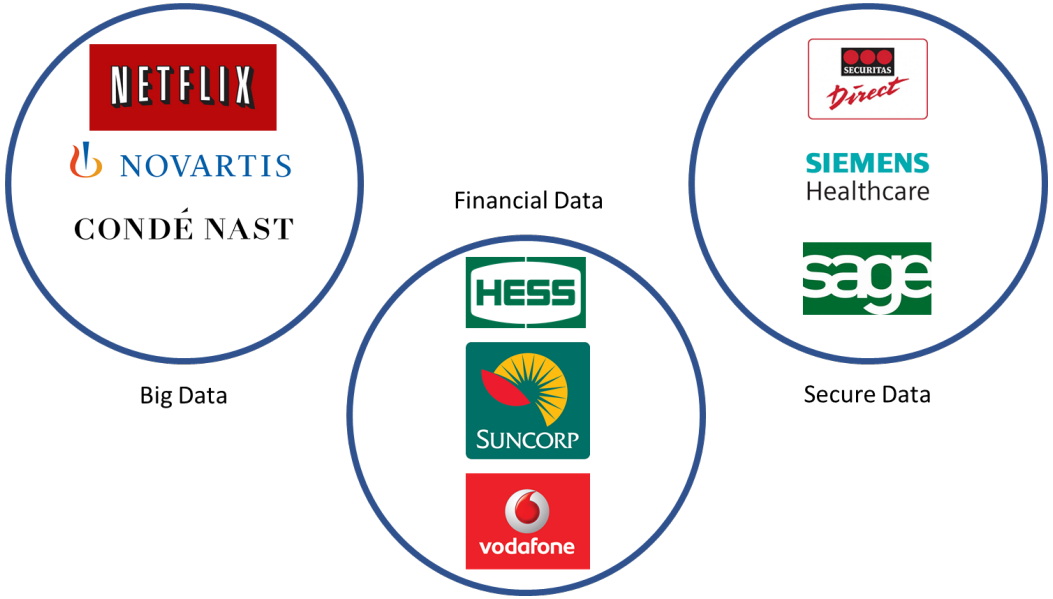
- D3S NET consists of D3S detector, SIGMA LE app and SIGMA Network
- D3S NET provides analysis and visualization for large network of detectors
- The data collected is stored in the D3S NET cloud system, which is currently hosted in the US-East Region of the Amazon Web Services (AWS)
- The system can be hosted in any of the AWS Regions

D3S NET Cloud System

AWS Introduction

Amazon Web Service (AWS) provides on-demand cloud computing platforms globally

- ✓ Used by 80% of fortune 500 companies to host their infrastructure
- ✓ Provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)
- ✓ Exists within 18 geographic regions around the world

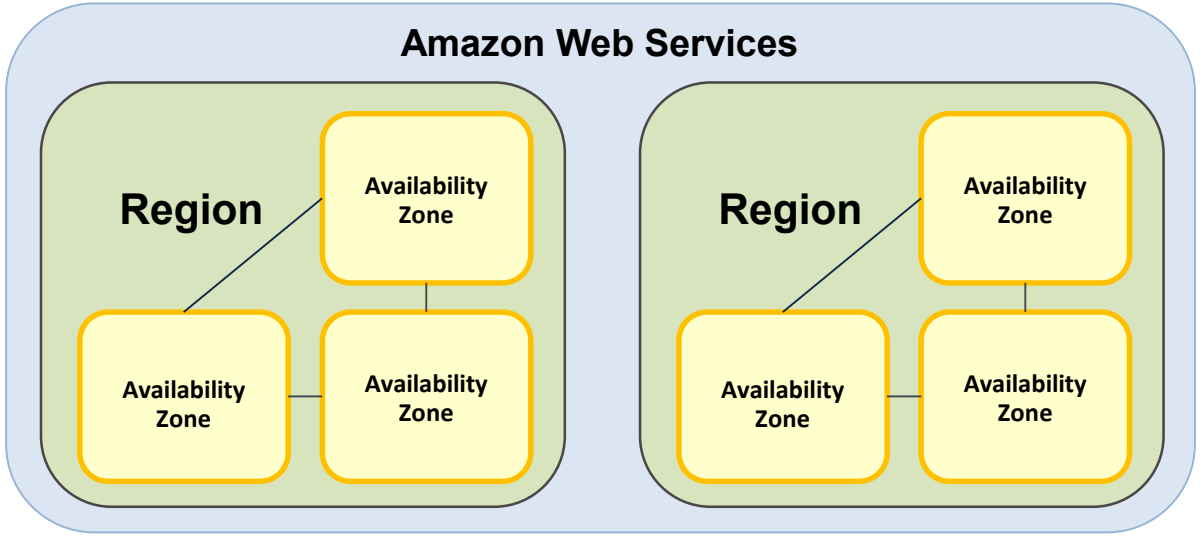


Amazon Web Service (AWS) provides on-demand cloud computing platforms globally

AWS Introduction

An AWS Region is a geographical location with a collection of availability zones mapped to physical data centres in that region

- ✓ Every Region is physically isolated from and independent of every other Region
- ✓ AWS is able to guarantee that customer data does not leave a particular geographic region unless requested by the customer
- ✓ Data protection laws compliant in each individual Region



AWS Regions

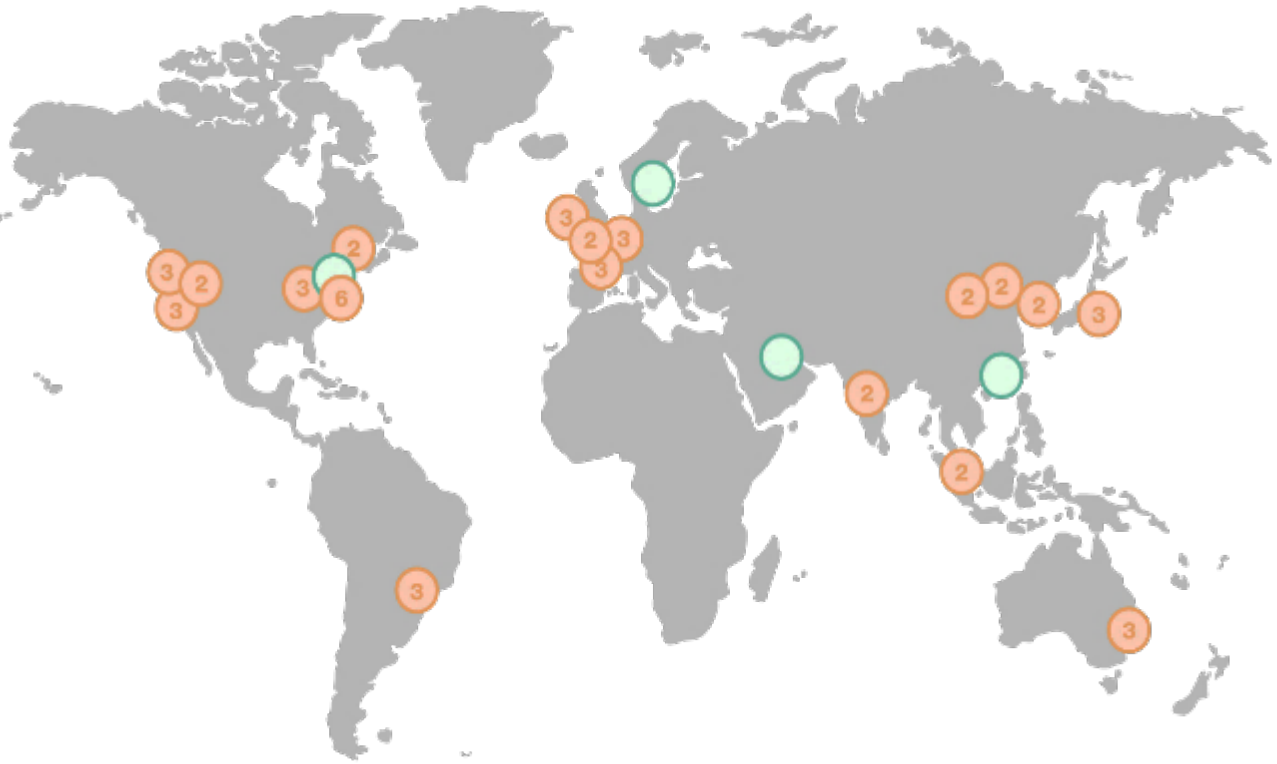
The AWS Cloud operates 49 Availability Zones within 18 geographic Regions around the world.

Region & Number of Availability Zones

- **US East** - N. Virginia (6), Ohio (3)
- **US West** - N. California (3), Oregon (3)
- **Asia Pacific** - Mumbai (2), Seoul (2), Singapore (2), Sydney (3), Tokyo (3)
- **Canada** - Central (2)
- **China** - Beijing (2), Ningxia (2)
- **Europe** - Frankfurt (3), Ireland (3), London (2), Paris (3)
- **South America** - São Paulo (3)
- **AWS GovCloud (US-West)** (2)

New Region (coming soon)

- Bahrain
- Hong Kong SAR, China
- Sweden
- AWS GovCloud (US-East)

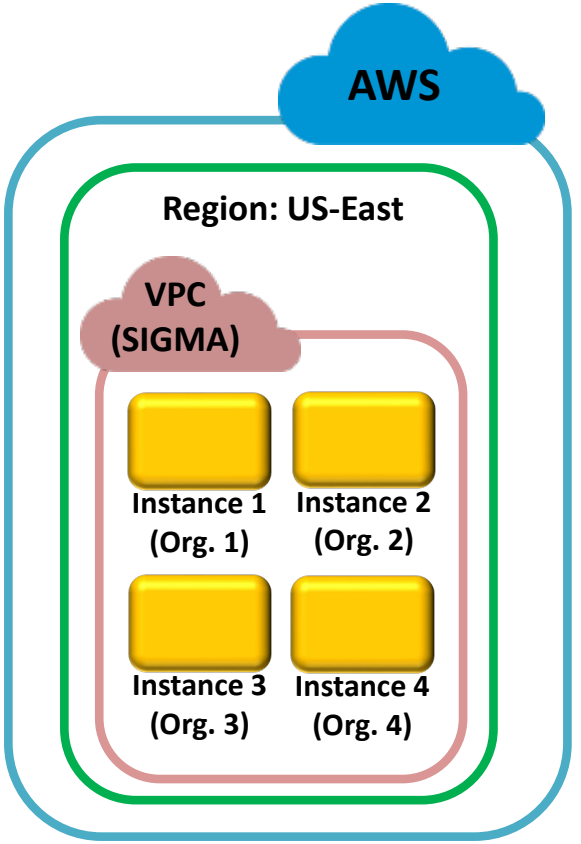


D3S NET Current System

- D3S NET backend SIGMA system is hosted in the US-East region within the AWS
  - ✓ Ensures 99.999% uptime, always ready to be accessed
  - ✓ Shared resources and auto update
  - ✓ Lower IT and maintenance costs

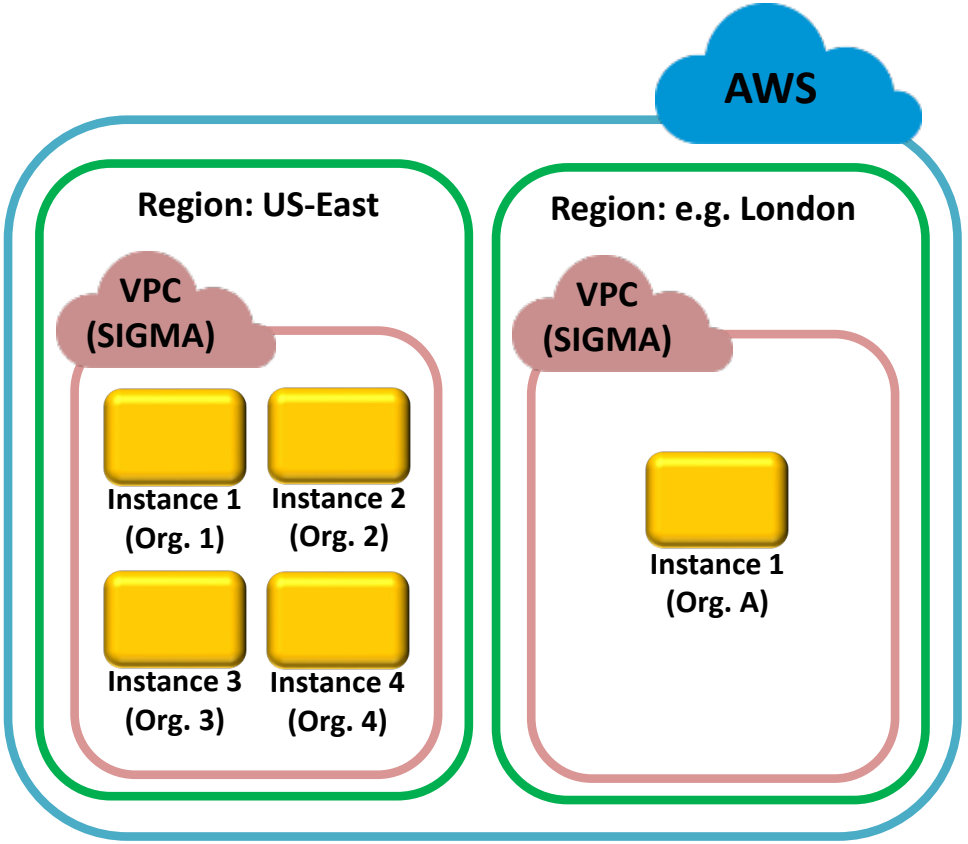
- SIGMA backbone ingests and catalogs sensor feeds from connected sensors, then partitions data by *instance*
  - ✓ *Instances* are logical partitions which can represent an organization or a single site in a larger organisation
  - ✓ Instances exist within the SIGMA VPC (Virtual Private Cloud)

- Access to instance data is restricted, ensuring your deployment is accessible only to authorized personnel
  - ✓ Configurable role-based access controls, including admin rights
  - ✓ SSL encryption and two-factor authentication
  - ✓ Stringent policy and contractual assurance
  - ✓ Disk-level encryption of the data stores
  - ✓ Extensively certified cloud backend



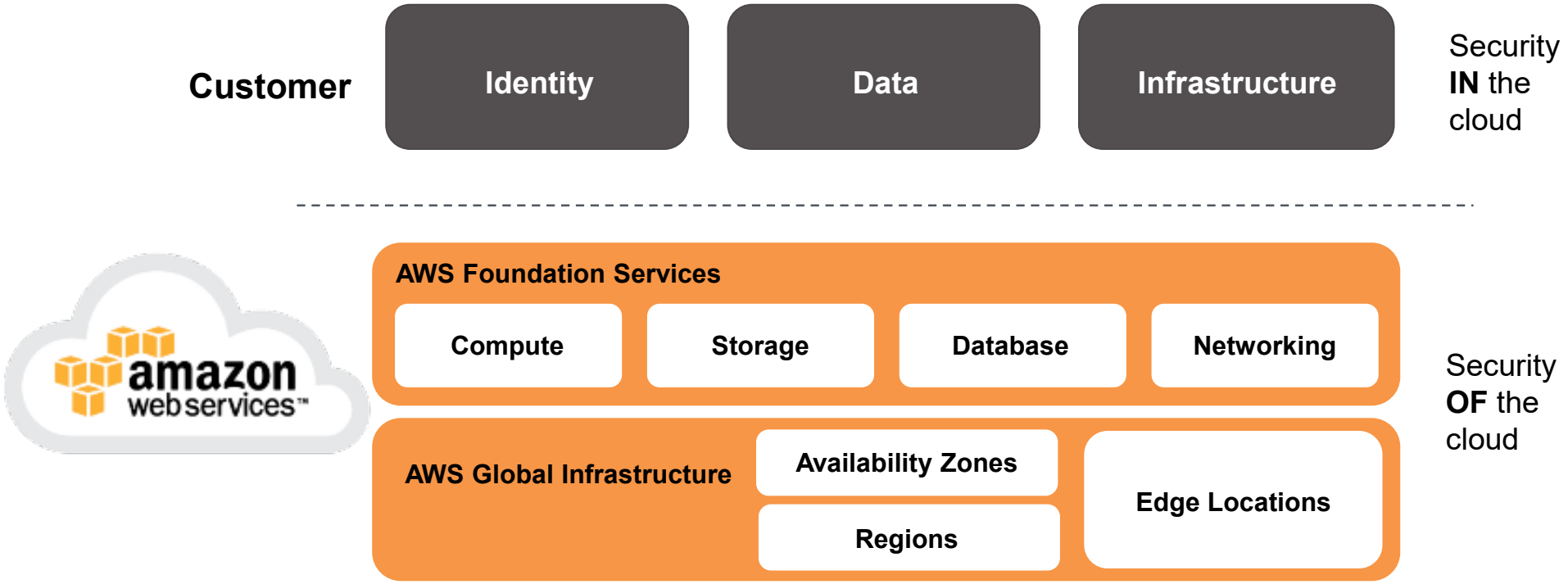
Alternatives to Current System

- D3S and Sigma LE App as a standalone system
  - ✓ Ability to choose when to transfer data
  - ✓ Ability to choose what to transfer
  - ✓ Limitation: No real time data
- Set up a physical data centre on site
  - ✓ Complete control and ownership of data centre
  - ✓ Limitations:
    - High setup and maintenance cost
    - Limited functionality with self-support
- Provision a VPC in one of European regions of AWS
  - ✓ Geographical data location reassurance
  - ✓ EU Data protection
  - ✓ EU regions: Frankfurt, Ireland, London, Paris
  - ✓ Limitations: greater share of fixed cost due to low population of detectors

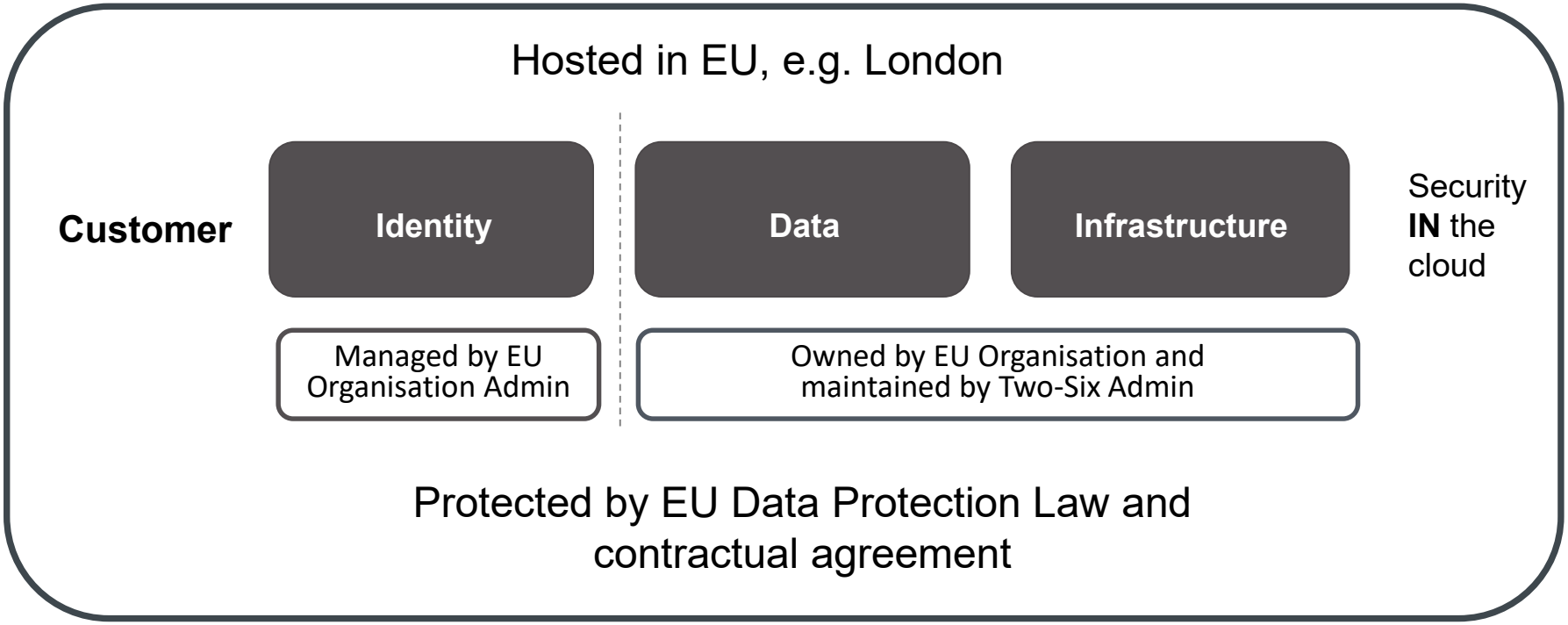


Note: *Currently the SIGMA VPC in US-East is provisioned to handle thousands of sensor feeds. Pricing for the cloud service leverages the shared nature of the cluster.*

Shared Security Responsibility



Shared Security Responsibility



Note: *Administrator rights will be managed by the EU Organisation. System maintenance and updates will be done by Two-Six Labs with access granted by the EU Organisation.*

SIGMA System Security

- Cybersecurity framework for cloud-based services, requiring:
  - ✓ Implementation of 300+ security controls across 17 control groups (NIST 800-53)
  - ✓ Creation of a System Security Plan detailing cybersecurity policies, procedures, standards, and controls
  - ✓ Official approval from the U.S. Government resulting in an Authority to Operate usable by Federal Agencies
  - ✓ Third-party independent audit

- Federal Risk and Authorization Management Program (FedRAMP) certification at the Moderate level
  - ✓ U.S. Government cybersecurity program
  - ✓ Objective: Standardise the approach to security assessment, authorisation, and continuous monitoring for cloud-based products and services
  - ✓ Compliant with:
    - National Institute of Standards and Technology (NIST) Special Publication 800-53
    - Cybersecurity triad: Confidentiality, Integrity, and Availability

SIGMA System Security – FedRAMP

- FedRAMP ensures the cloud service is auditable and accountable for its information security
  - ✓ Independent assessor must be used to perform initial and ongoing verification and validation of data security
  - ✓ A detailed and standardized framework ensures the cloud service provider security can be measured effectively
  - ✓ Auditable evidence control measures in place
    - Audit and Accountability Policy and Procedures
    - Auditable Events
    - Content of Audit Records
    - Audit Storage Capacity
    - Response to Audit Processing Failures
    - Audit Review, Analysis, and Reporting
    - Audit Reduction and Report Generation
    - Time Stamps
    - Protection of Audit Information
    - Non-Repudiation
    - Audit Record Retention
    - Audit Generation
  - ✓ Ensures data is recoverable and changes can be traced-back and rolled-back in the event of system crashes, hacked data, or inaccurate data entry

SIGMA System Security – FedRAMP

- FedRAMP Access Control
  - ✓ Ensures limited access to various resources within the environment to appropriate individuals
  - ✓ Various activities required to be implemented to address and mitigate access control related risks:
    - Access Control Policy and Procedures
    - Account Management
    - Access Enforcement
    - Information Flow Enforcement
    - Separation of Duties
    - Least Privilege
    - Unsuccessful Login Attempts
    - System Use Notification
    - Concurrent Session Control
    - Session Lock
    - Permitted Actions Without Identification/ Authentication
    - Security Attributes
    - Remote Access
    - Wireless Access
    - Access Control for Mobile Devices
    - Use of External Information Systems
    - Publicly Accessible Content

SIGMA System Security – Compliant to NIST 800-53

NIST 800-53 calls for 300+ security controls to be implemented across 17 different control groups

NIST 800-53 Security Control Groups		
Access Control	Identification & Authentication	Personnel Security
Awareness and Training	Incident Response	Risk Assessment
Audit & Accountability	System Maintenance	System & Services Acquisition
Security Assessment & Authorization	Media Protection	System & Communications Protection
Configuration Management	Physical & Environmental Protection	System & Information Integrity
Contingency Planning	Planning	

AWS Assurance Program

Certifications / Attestations	Laws, Regulations, and Privacy	Alignments / Frameworks
C5 [Germany] - Operational Security Attestation	**CISPE** - Data Protection Coalition	**CIS** - Center for Internet Security
Cyber Essentials Plus [UK] - Cyber-attack protection	**EU Model Clauses** - Data Processing Addendum	**CJIS** - Criminal Justice Information Services
DoD SRG - Department of Defence Data	**FERPA** - Educational Privacy Act	**CSA** - Cloud Security Alliance Controls
FedRAMP - Government Data Standards	**Gramm-Leach-Bliley Act [GLBA]** - Financial Data Security	**ENS [Spain]** - Esquema Nacional de Seguridad
FIPS - Government Security Standards	**HIPAA** - Protected Health Information	**EU-US Privacy Shield** - EU-US Data Transfer
IRAP [Australia] - Australian Security Standards	**HITECH** - Protected Health Transmission	**FFIEC** - Federal Financial Institutions Examination Council
ISO 9001 - Global Quality Standard	**IRS 1075** - Tax Information Encryption Requirements	**FISC [Japan]** - Financial Industry Information Systems
ISO 27001 - Security Management Standard	**ITAR** - International Arms Regulations	**FISMA** - Federal Information Security Management Act
ISO 27017 - Cloud Specific Controls	**My Number Act [Japan]** - Personal Information Protection	**G-Cloud [UK]** - UK Government Standards
ISO 27018 - Personal Data Protection	**U.K. DPA 1998** - Data Protection Act	**GxP (FDA CFR 21 Part 11)** - Quality Guidelines and Regulations

Source: https://aws.amazon.com/compliance/

AWS Assurance Program

Certifications / Attestations	Laws, Regulations, and Privacy	Alignments / Frameworks
MTCS Tier 3 [Singapore] - Multi-Tier Cloud Security Standard	**VPAT / Section 508** - Accessibility Standards	**ICREA** - International Computer Room Experts Association
PCI DSS Level 1 - Payment Card Standards	**EU Data Protection Directive** - Data Protection Framework	**IT Grundschutz [Germany]** - Baseline Protection Methodology
Glacier for SEC Rule 17a-4(f) - Financial Data Standards	**Privacy Act [Australia]** - Information Privacy Principles	**MITA 3.0** - Medicaid Information Technology Architecture
SOC 1 - Audit Controls Report	**Privacy Act [New Zealand]** - Information Privacy Principles	**MPAA** - Protected Media Content
SOC 2 - Compliance Controls Report	**PDPA - 2010 [Malaysia]** - Personal Data Protection Act	**NIST** - National Institute of Standards and Technology
SOC 3 - General Controls Report	**PDPA - 2012 [Singapore]** - Personal Data Protection Act	**PHR** - Personal Health Records
	PIPEDA [Canada] - Personal Data Protection	**Uptime Institute Tiers**
	Spanish DPA Authorization - Data Processing Addendum	**UK Cloud Security Principles**
		Cyber Security Principles

Source: https://aws.amazon.com/compliance/

Contact Information

Kromek Group Headquarters
NETPark,
Thomas Wright Way,
Sedgefield
County Durham,
TS21 3FD UK

T: +44 (0) 1740 626060
F: +44 (0) 1740 626061

E: sales@kromek.com
W: www.kromek.com

UK and European Operations

Neutron Research & Development Centre
Huddersfield UK

US Operations

NOVA R&D Inc
California, USA

Kromek
Pennsylvania USA