Cloud Security and Cloud Compliance

Cloud Security services and mechanisms:

How can modern clouds provide secure and trusted environment for data and business applications?

Yuri Demchenko

Systems and Networking Lab, University of Amsterdam

Amsterdam Security Workshop

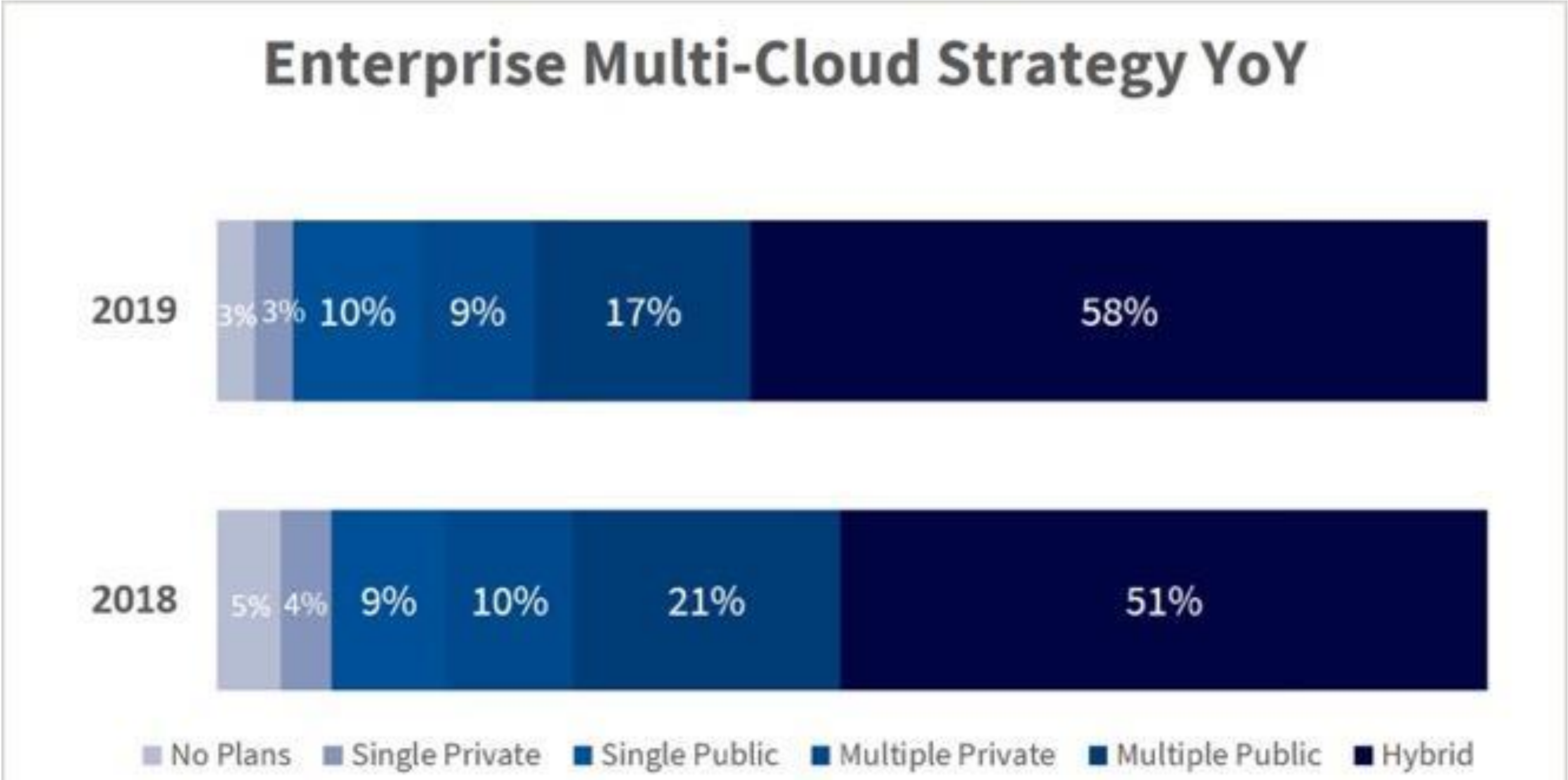
9 Oct 2019, UvA

Outline

- Introduction: Cloud adoption is growing
- Shared Responsibility Security Model in Cloud
- Case Study: AWS Security
- Cloud Compliance and Cloud Security Alliance (CSA)
  - CSA GRC Stack: Governance, Risk Management and Compliance
  - Consensus Assessment Initiative Questionnaire (CAIQ)
- DevSecOps = DevOps + SSDL (Security Services Development Lifecycle)
- Case Study: Trusted Data Market infrastructure and IDS Connector
- Discussion: Research topics in Cloud Security and Trust

Cloud Facts: Cloud adoption is growing

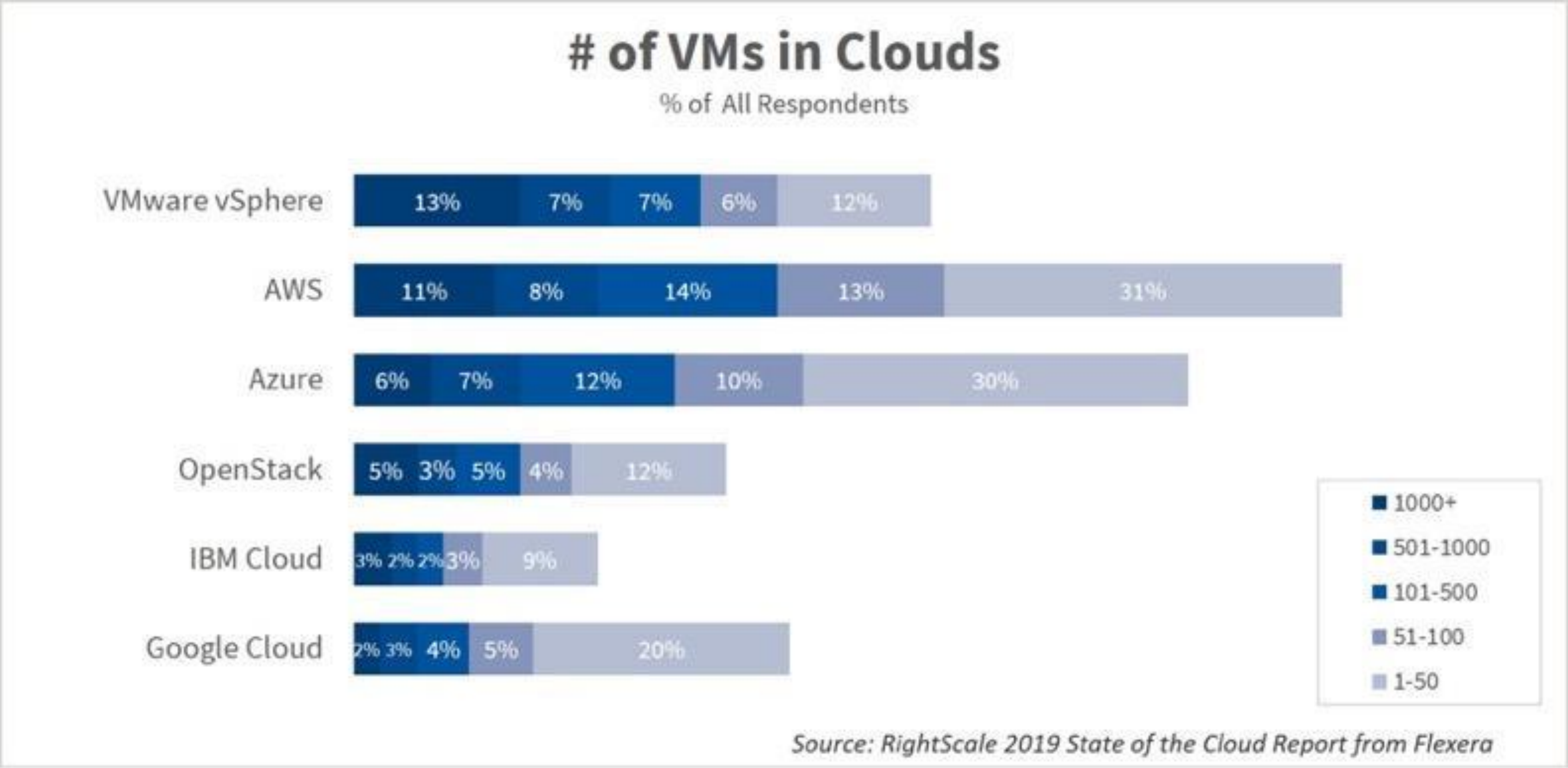
- Cloud adoption is growing: Enterprise Cloud Strategy 2019



http://googliers.net/static/media/uploads/download_files/2019_state_of_the_cloud_report.pdf

Source: RightScale 2019 State of the Cloud Report from Flexera

Cloud Facts and Observations: AWS vs Azure



Source: RightScale 2019 State of the Cloud Report from Flexera

- Microsoft Azure is fasted growing cloud: now 85% of AWS (compare 70% in 2018)
- Quite popular in Netherlands

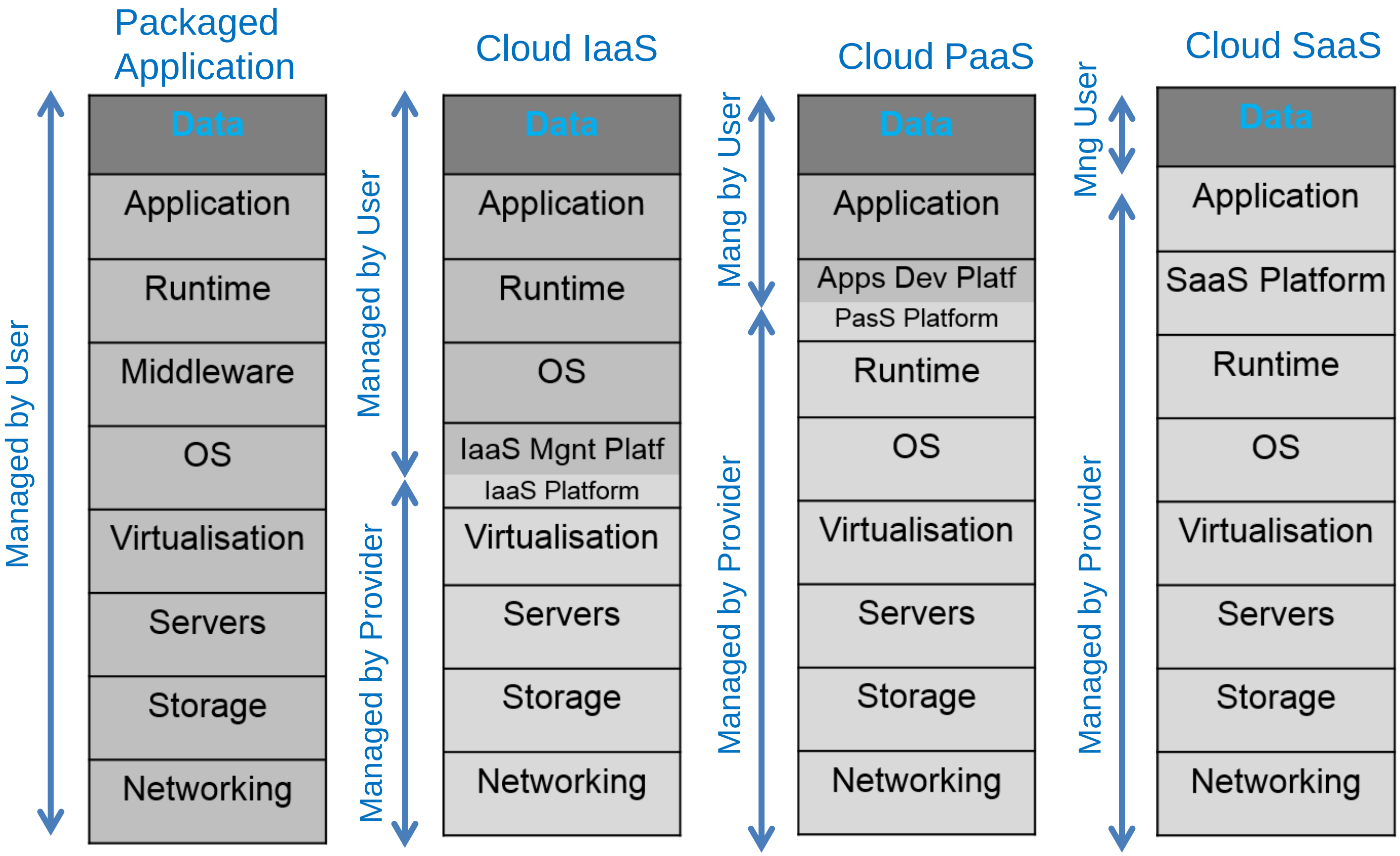
Cloud Observations

- Cloud is an ultimate platform for Big Data
  - Data gravity vs Investments gravity
    - Migration choice: 10 yrs of legacy data vs expected explosive data growth
  - Working with data and data analytics in cloud is much easier
    - Hybrid cloud and data analytics solution is growing
    - **Data Lakes**: heterogeneous data formats, namespaces, filesystems
- Migration to cloud takes 1-2 years, requires competence planning
  - Demand for cloud migration/integration services/companies
  - Growing adoption of the DevOps culture in services development and operation
- Most of new projects are in cloud

Part 1: Cloud Security and AWS Example

- Shared responsibility model
- AWS Security

Split of Responsibilities in Cloud IaaS, PaaS, SaaS



Packaged Application

Managed by User

Data
Application
Runtime
Middleware
OS
Virtualisation
Servers
Storage
Networking

Cloud IaaS

Managed by User
Managed by Provider

Data
Application
Runtime
OS
IaaS Mgnt Platf
IaaS Platform
Virtualisation
Servers
Storage
Networking

Cloud PaaS

Mang by User
Managed by Provider

Data
Application
Apps Dev Platf
PasS Platform
Runtime
OS
Virtualisation
Servers
Storage
Networking

Cloud SaaS

Mng User
Managed by Provider

Data
Application
SaaS Platform
Runtime
OS
Virtualisation
Servers
Storage
Networking

Data is always responsibility of Customer

Cloud Provider provides tools for assisting customers in secure deployment, operation and testing

Security management responsibilities split between Customer and Provider for IaaS, PaaS, SaaS service models

- Updating firmware and software for platform and for customer managed components
- Firewall is intrusion prevention and a responsibility of the cloud provider
- Certification and compliance of the cloud platform doesn’t imply security and compliance of the customer controlled components

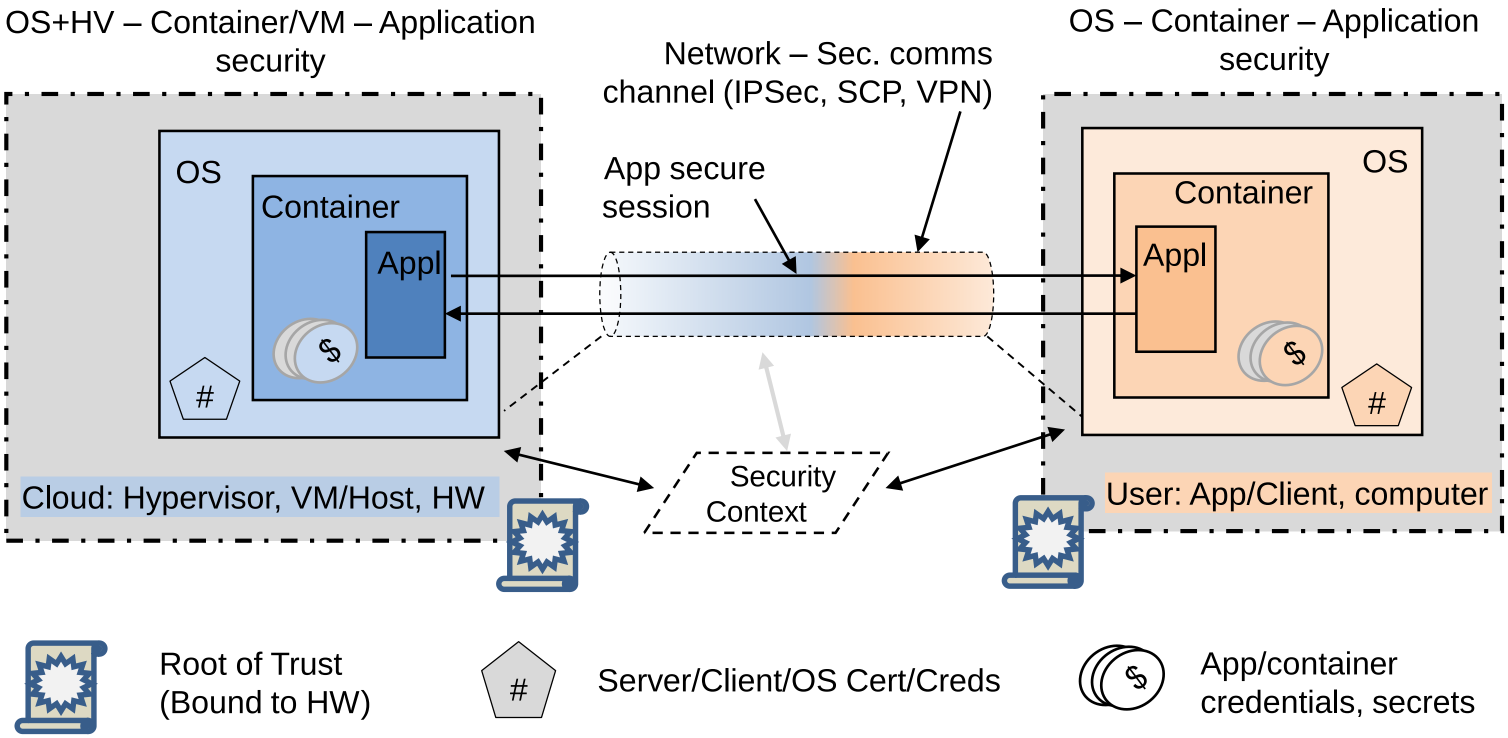
Cloud Computing Security – Challenges

- Fundamental security challenges and main user concerns in clouds
  - Data security: Where are my data? Are they protected? What control has cloud provider over data security and location?
  - Identity management and access control: Who has access to my personal/ID data?

- Two main tasks in making cloud secure and trustworthy
  - Secure operation of the cloud (provider) infrastructure
  - User controlled access control (security) infrastructure
    - Provide sufficient amount of security controls for competent user

- Security services are provisioned **on-demand** (as part of virtualised infrastructure) and require **bootstrapping (federation)** with the customer services and trust domain

Cloud, OS, Network and Applications Trust Layers



OS+HV – Container/VM – Application security

Network – Sec. comms channel (IPSec, SCP, VPN)

OS – Container – Application security

OS

Container

Appl

#

App secure session

Security Context

Cloud: Hypervisor, VM/Host, HW

OS

Container

Appl

#

User: App/Client, computer

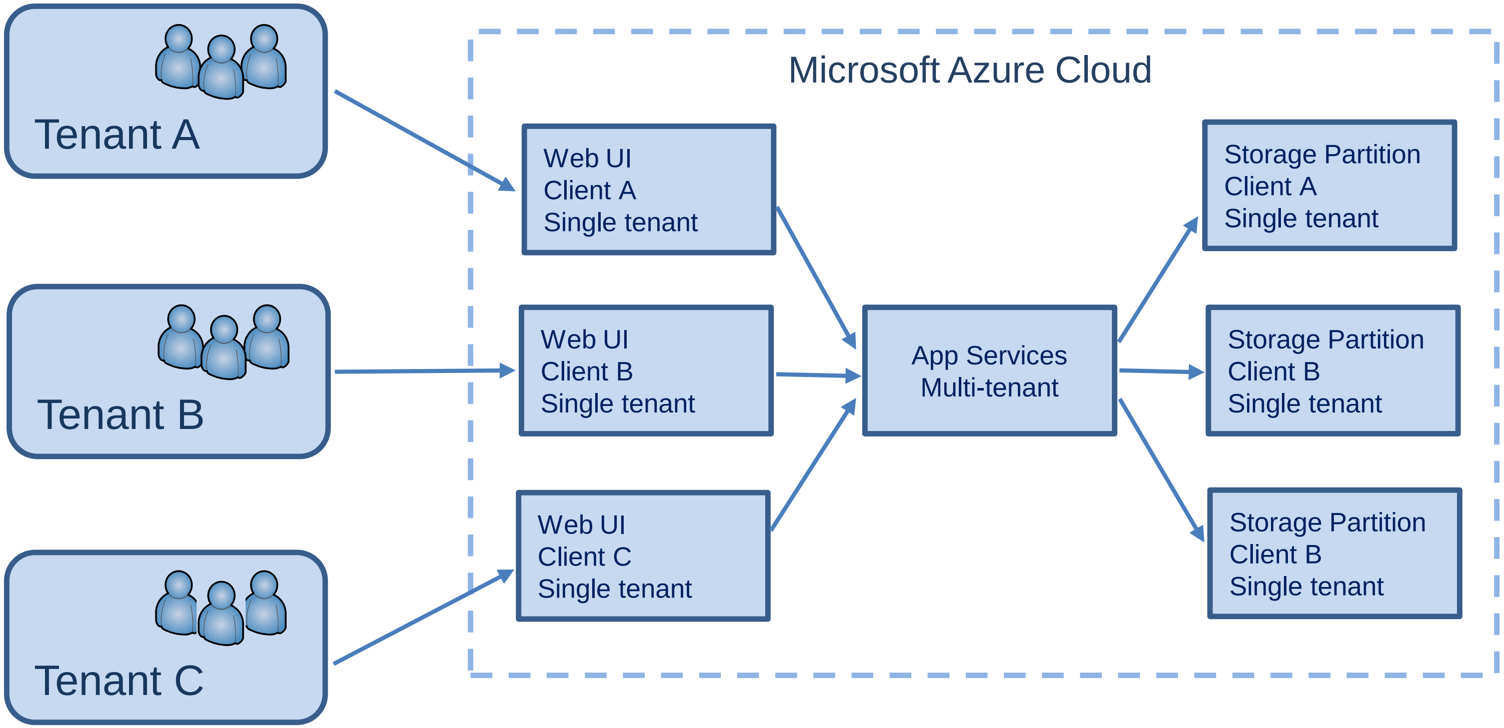
Root of Trust (Bound to HW)

Server/Client/OS Cert/Creds

App/container credentials, secrets

- Consistent security must provide security at all layers correspondingly relying on trust credentials at each layer
  - Application – Container - Operating systems (security kernel) + Cloud platform
  - Network/communication – Runtime - Storage
- Two security models: Trusted Computing Base (TCB) for cloud platform and OSI/Internet security cloud based applications
  - Client/server and Service Oriented Architecture vs OS and hypervisor run-time
- Root of trust is based on the security credentials bound to hardware mediated through OS to runtime environment

Multi-tenant Application: Example Implementation



Tenant A

Tenant B

Tenant C

Microsoft Azure Cloud

Web UI
Client A
Single tenant

Web UI
Client B
Single tenant

Web UI
Client C
Single tenant

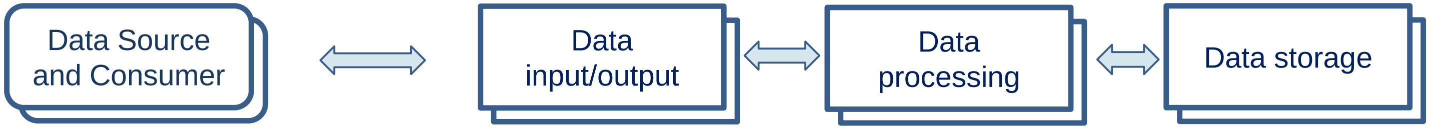
App Services
Multi-tenant

Storage Partition
Client A
Single tenant

Storage Partition
Client B
Single tenant

Storage Partition
Client B
Single tenant

Data transformation in multi-tier multi-tenant applications



Data Source
and Consumer

Data
input/output

Data
processing

Data storage

Access control

Processing
threads isolated

Data separation

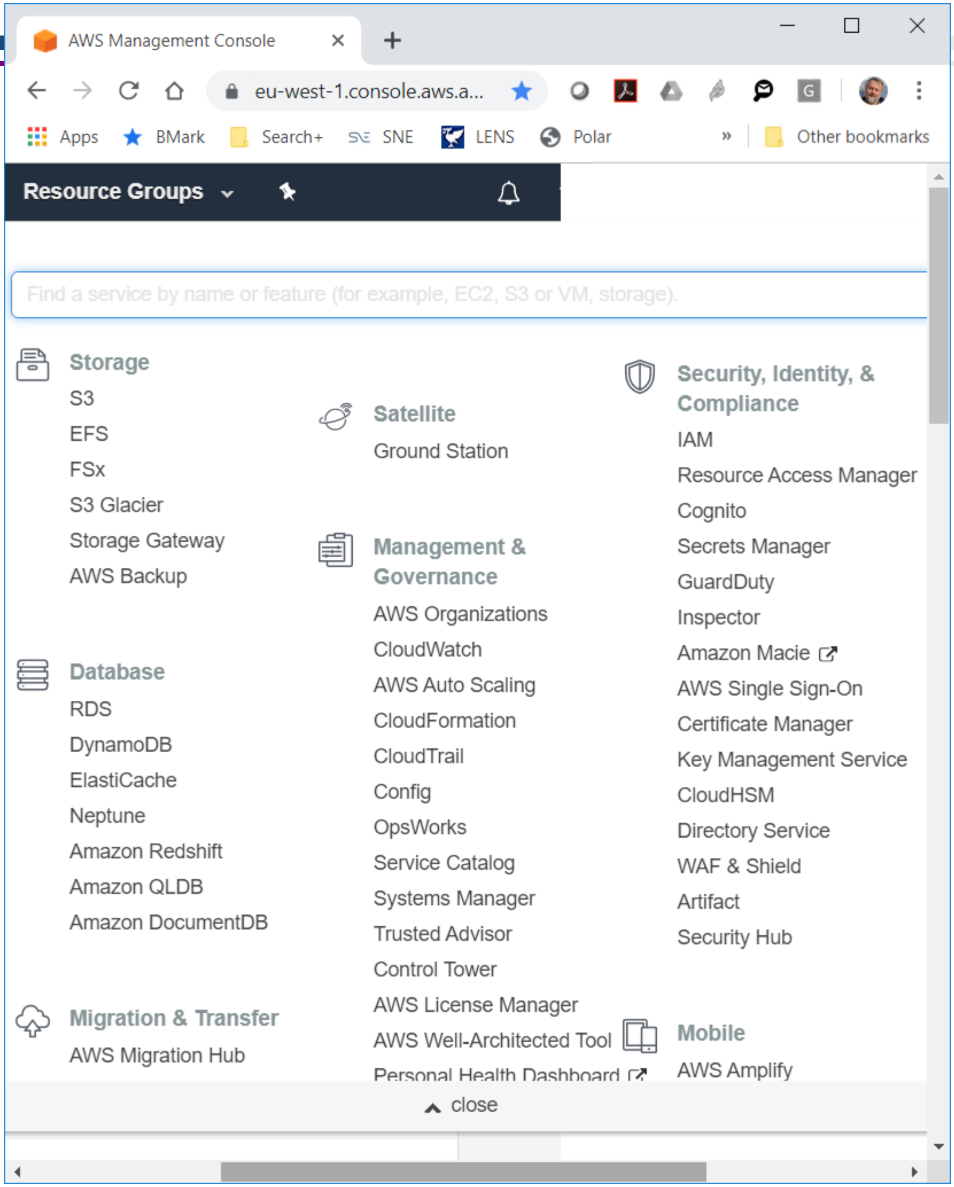
Generally reflects
Office 365 multitenancy model

Designing for Multi-tenancy in Cloud - Overview

- Data security and privacy is a primary concern and design target in multi-tenant applications
  - Cloud datacenter security – ensured by cloud provider
  - Application security – ensured by the application developer and service operator
- Multi-layer and multi-tier multi-tenancy mechanism
  - Presentation, business logic, data structures
- Data isolation and segregation
  - Store client data with isolated URI or schema -> Data Lakes
  - Blob or Table storage: isolated URI
  - Azure SQL database: partitioning, separate schema
- Access control and Identity management
  - Microsoft Azure Active Directory and Windows Identity Foundation
  - AppFabric Access Control
  - Identity federation with the tenants’ home organisations
  - Custom Identity Solution
- Scalability up and down, horizontal scalability
- Services metering, accounting and billing

Case Study: AWS Security Mechanisms

- VPC – Virtual Private Cloud
  - VPN – Virtual Private Network
  - VPG – VPN Private Gateway
  - IGW – Internet Gateway
- HTTPS and TLS/SSL, SSH, KPI
- AIM – Access and Identity Management
- Other security services
  - AWS SSO
  - Cognito – Identity Federation
  - Macie - Data visibility security service
  - CloudHSM - Managed hardware security module (HSM)



AWS Management Console

eu-west-1.console.aws.a...

Apps BMark Search+ SNE LENS Polar » Other bookmarks

Resource Groups

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Storage
S3
EFS
FSx
S3 Glacier
Storage Gateway
AWS Backup

Database
RDS
DynamoDB
ElastiCache
Neptune
Amazon Redshift
Amazon QLDB
Amazon DocumentDB

Migration & Transfer
AWS Migration Hub

Satellite
Ground Station

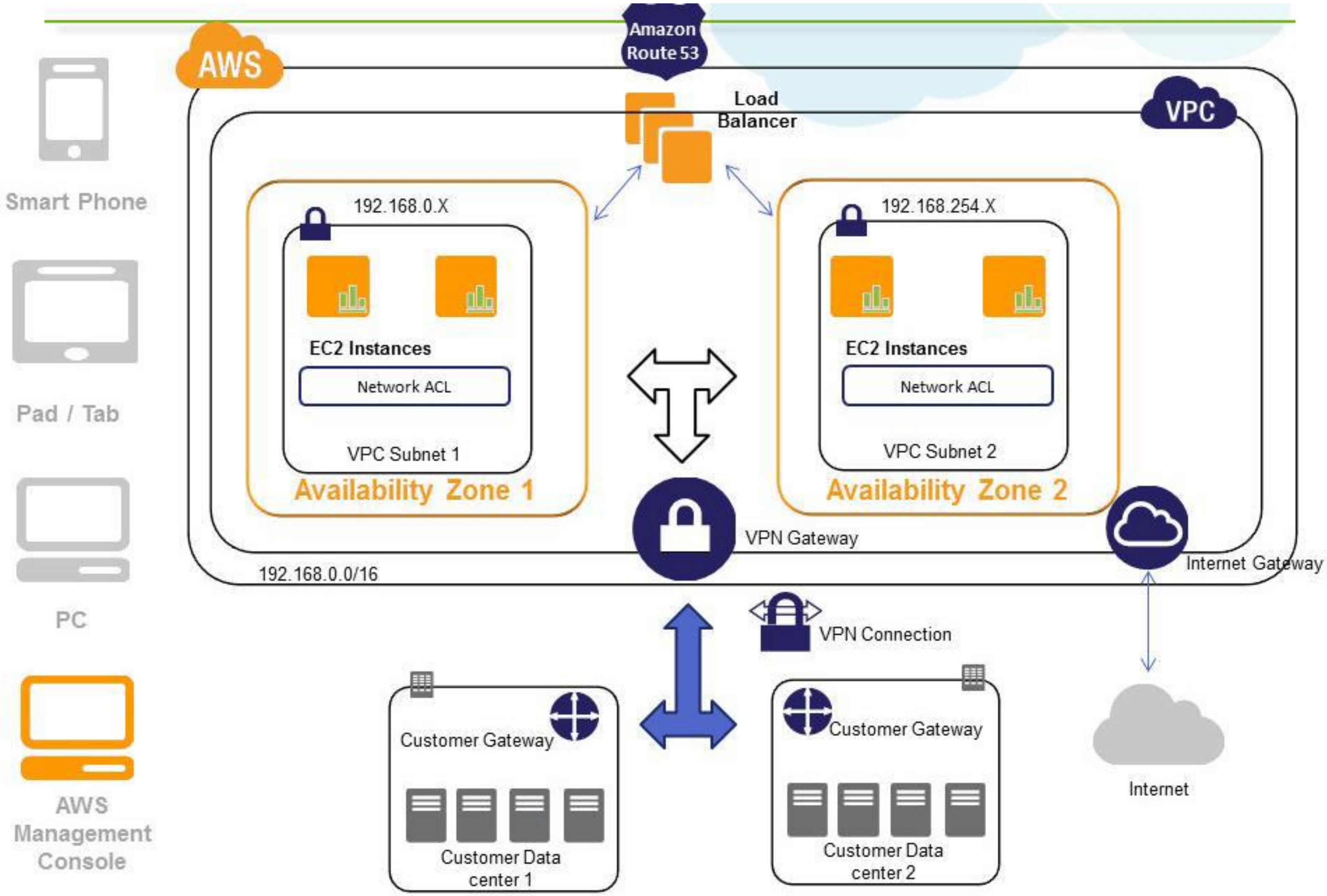
Management & Governance
AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
Trusted Advisor
Control Tower
AWS License Manager
AWS Well-Architected Tool
Personal Health Dashboard

Security, Identity, & Compliance
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
Key Management Service
CloudHSM
Directory Service
WAF & Shield
Artifact
Security Hub

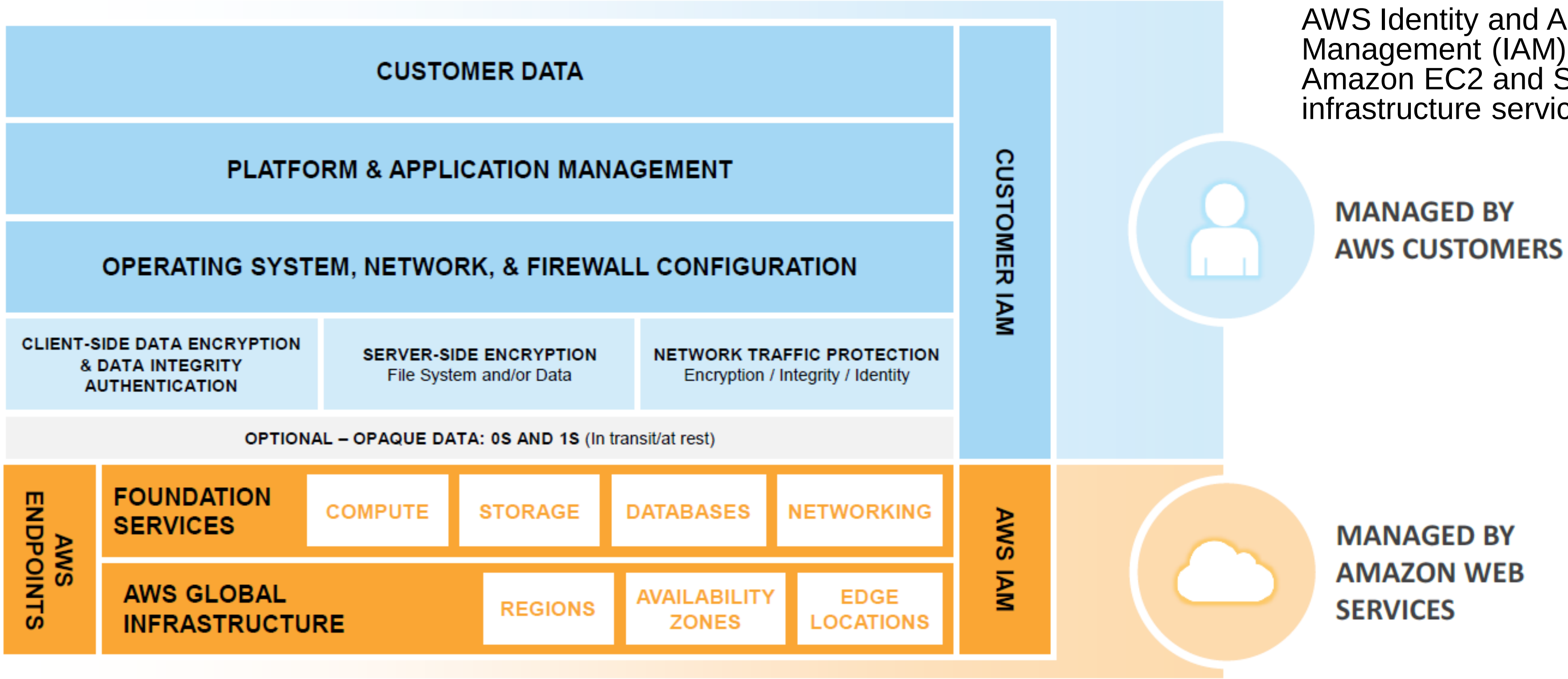
Mobile
AWS Amplify

close

AWS VPC Structure



Example: Security responsibility sharing in AWS IaaS infrastructure services

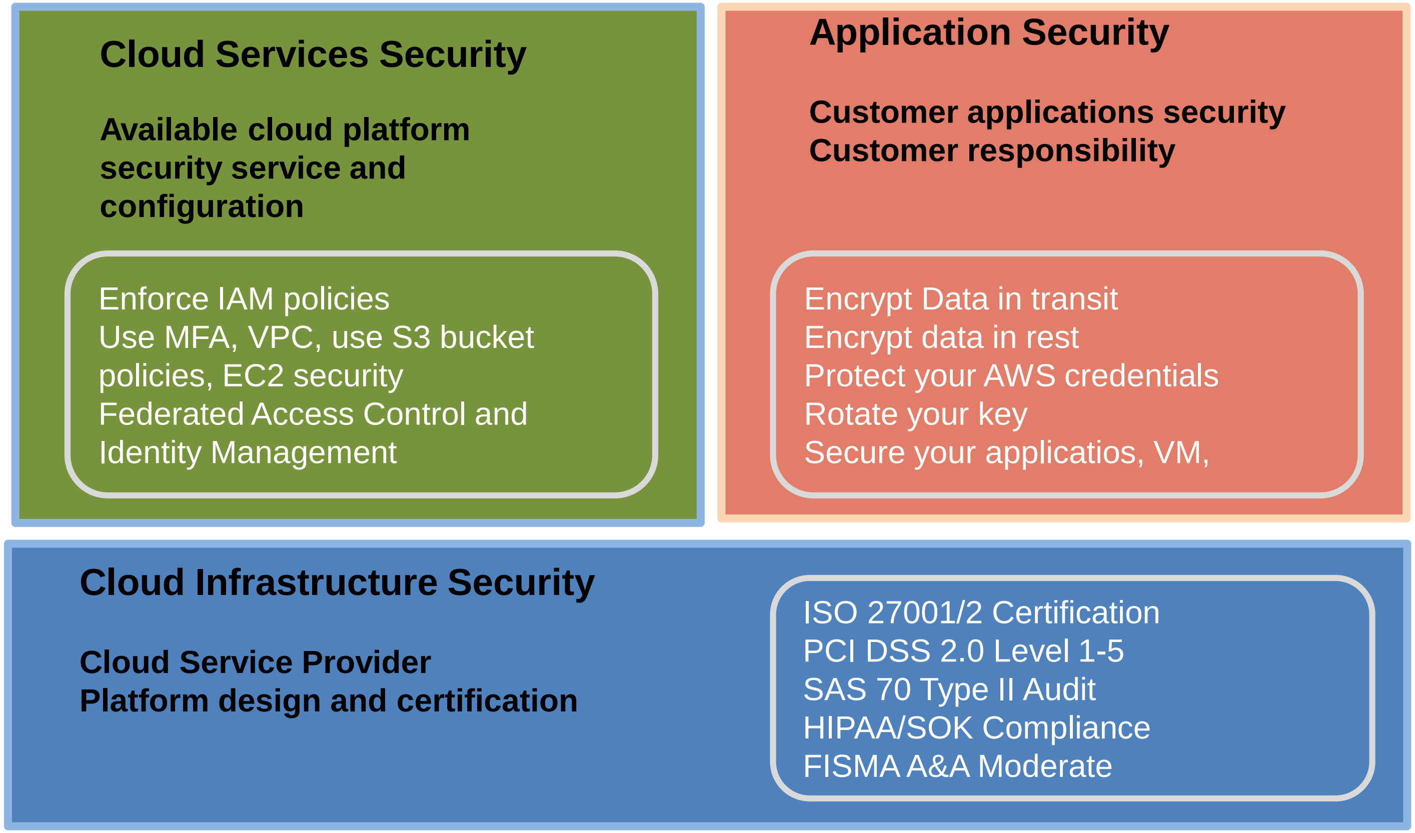

CUSTOMER DATA
PLATFORM & APPLICATION MANAGEMENT
OPERATING SYSTEM, NETWORK, & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION File System and/or Data
NETWORK TRAFFIC PROTECTION Encryption / Integrity / Identity
OPTIONAL – OPAQUE DATA: 0S AND 1S (In transit/at rest)
CUSTOMER IAM
MANAGED BY AWS CUSTOMERS
AWS ENDPOINTS
FOUNDATION SERVICES
COMPUTE
STORAGE
DATABASES
NETWORKING
AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS
AWS IAM
MANAGED BY AMAZON WEB SERVICES

AWS Identity and Access Management (IAM) over Amazon EC2 and S3 infrastructure services

- For other cloud service models PaaS and SaaS the responsibility of AWS goes up to OS, network and firewall for PaaS, and also includes the application platform and container for SaaS.
  - However, the responsibility for data remains with the customer.

[ref] Todorov, D. & Ozkan, Y. (November 2013) ‘AWS security best practices’, Amazon Web Services [Online]. Available from: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

Amazon Web Services Security Model



Cloud Services Security

Available cloud platform security service and configuration

Enforce IAM policies
Use MFA, VPC, use S3 bucket policies, EC2 security
Federated Access Control and Identity Management

Application Security

Customer applications security
Customer responsibility

Encrypt Data in transit
Encrypt data in rest
Protect your AWS credentials
Rotate your key
Secure your applicatios, VM,

Cloud Infrastructure Security

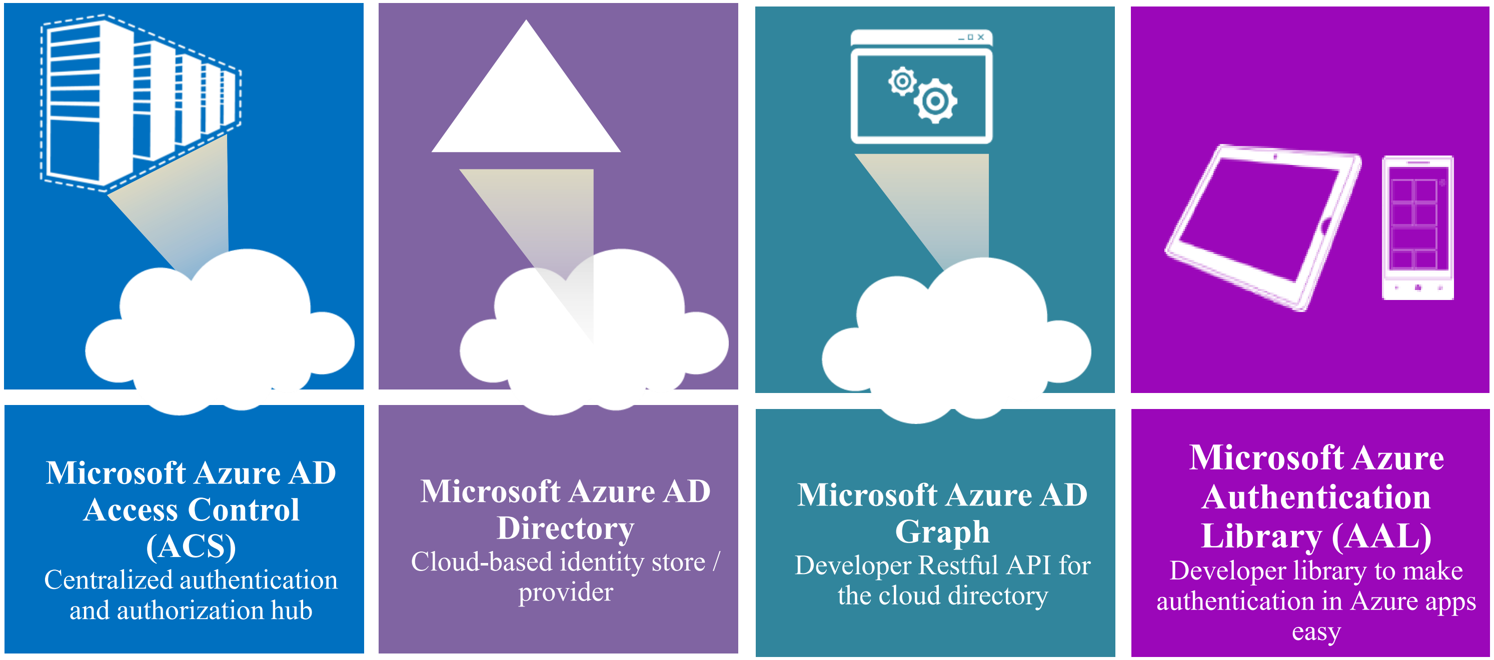
Cloud Service Provider
Platform design and certification

ISO 27001/2 Certification
PCI DSS 2.0 Level 1-5
SAS 70 Type II Audit
HIPAA/SOK Compliance
FISMA A&A Moderate

Security is declared as one of critical importance to AWS cloud that is targeted to protect customer information and data from integrity compromise, leakage, accidental or deliberate theft, and deletion.

- The AWS infrastructure is designed with the high availability and sufficient redundancy to ensure reliable services operation.

Microsoft Azure Active Directory (AAD)



Microsoft Azure AD Access Control (ACS)
Centralized authentication and authorization hub

Microsoft Azure AD Directory
Cloud-based identity store / provider

Microsoft Azure AD Graph
Developer Restful API for the cloud directory

Microsoft Azure Authentication Library (AAL)
Developer library to make authentication in Azure apps easy

Microsoft Azure Active Directory is a modern cloud service providing Identity Management and Access Control capabilities to cloud applications.

- Provides Identity and access management in the cloud
- Can be integrated with on-premises AD
- Supports Integration with cloud applications

Microsoft Azure Active Directory provides 4 basic services

- Microsoft Azure AD Access Control (ACS)
- Microsoft Azure AD Directory
- Microsoft Azure AD Graph
- Microsoft Azure Authentication Library (AAL)

Microsoft Azure AD Access Control

- A cloud federation service for your cloud applications and services
  - Federates on-premises and cloud identity services
- Prerequisites
  - Demands federated authentication
  - AD on-premises and AAD on cloud synchronisation
- Supports multiple identity providers
  - Facebook, Google, Microsoft, Windows Server AD FS, Yahoo!
- Supports multiple protocols
  - WS-Federation, WS-Trust, OAuth 2.0 (draft 13)
- Supports multiple tokens
  - JWT, SAML 1.1/2.0, SWT

Part 2. Cloud Compliance

- Compliance standards, Security Controls
- CSA GRC Stack: Governance, Risk Management and Compliance
- Compliance Assessment Initiative Questionnaire (CAIQ)

Security and Compliance

- Security and compliance are related and in some cases interchangeable
- **Security** is commonly defined as a set of technical, physical, and administrative controls in order to ensure normal operation of a system or application
  - Security is often associated with the CIA triad Confidentiality, Integrity, Availability
  - Appropriate level of security requires organizations to take measures and comply to the numerous security controls
- **Compliance** is a certification or confirmation that the system or an organization meets the requirements of specified standards, established legislation, regulatory guidelines or industry best practices that can be jointly defined as compliance framework
  - A compliance framework can includes business processes and internal controls the organization has in place to adhere to these standards and requirements
  - The framework should also map different requirements to internal controls and processes to eliminate redundancies
- Why it is important for cloud?
  - When moving to cloud, the organization moves from internal security and operational environment/context (that may not be formally defined) to external operational security that will become a part of SLA (or business requirement) with CSP
- Problem with achieving compliance for cloud based applications/solutions
  - Audit requirements are not designed for virtualised distributed environment
  - Lack of visibility in cloud: large CSP such as Amazon and Google are “walled/curtained gardens”
  - Requirements to allow CSP audit may involve Non-Disclosure Agreement (NDA) and risk of provider lock-in

Regulatory requirements to be considered for cloud compliance – Example General Standards

General standards and recommendations

- ISO/IEC 27001:2005 Certification on security infrastructure
  - Industry standard: the risk-based information security management program that follows a plan-do-check-act process
- NIST SP 800-53 Security Controls and ISO/IEC 15408 Evaluation Cirteria
- HIPAA/HITECH - The U.S. Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH)
  - Act created by the US federal government include provisions to protect patients' private information.
- NIST SP 800-144 Guidelines for Security and Privacy in Cloud Computing
- Cloud Security Alliance (CSA) Security Guidance for Critical Area of focus in Cloud Computing
- ENISA Cloud Computing Security Risk Assessment
- GDPR (General Data Protection Regulation)

Case study: Certification/Compliance by Amazon AWS Cloud

The AWS cloud infrastructure has been designed and managed in alignment with regulations, standards, and best-practices including:

- ISO/IEC 27001:2005
- SOC 1, SOC2, SOC3
- FIPS 140-2
- CSA
- PCI DSS Level 1
- HIPAA
- ITAR
- DIACAP and FISMA
- FedRAMP (SM)
- MPAA

Amazon Cloud is certified for hosting US Governmental services

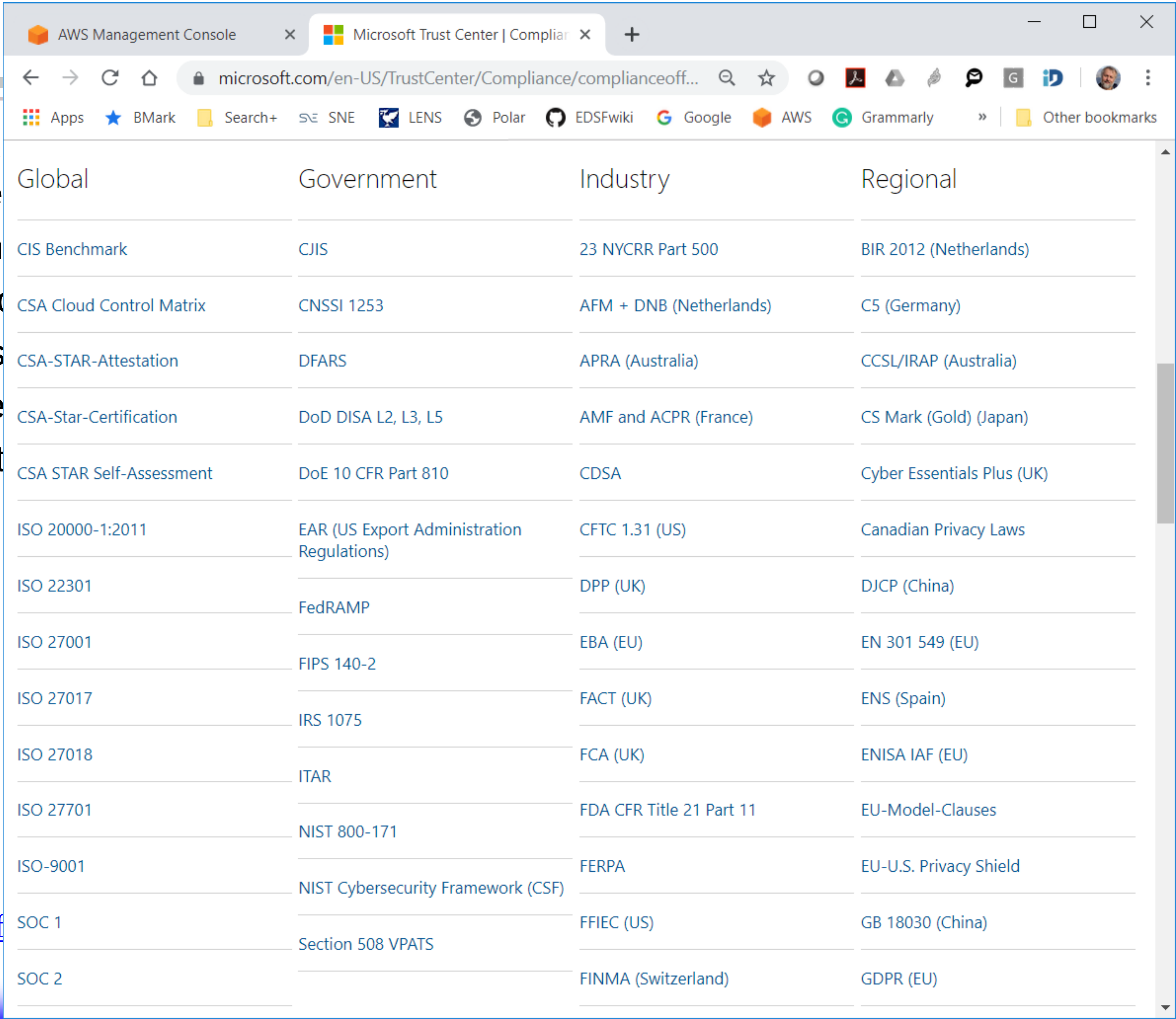
http://aws.amazon.com/compliance/

Case study: Compliance by Microsoft Azure

Microsoft servic
and compliance

- Current com
- Office 365 c
- Service Trus
- Microsoft Se
- Audit Report

https://www.microsof


AWS Management Console
Microsoft Trust Center | Complia
microsoft.com/en-US/TrustCenter/Compliance/complianceoff...
Apps
BMark
Search+
SNE
LENS
Polar
EDSFwiki
Google
AWS
Grammarly
Other bookmarks

Global	Government	Industry	Regional
CIS Benchmark	CJIS	23 NYCRR Part 500	BIR 2012 (Netherlands)
CSA Cloud Control Matrix	CNSSI 1253	AFM + DNB (Netherlands)	C5 (Germany)
CSA-STAR-Attestation	DFARS	APRA (Australia)	CCSL/IRAP (Australia)
CSA-Star-Certification	DoD DISA L2, L3, L5	AMF and ACPR (France)	CS Mark (Gold) (Japan)
CSA STAR Self-Assessment	DoE 10 CFR Part 810	CDSA	Cyber Essentials Plus (UK)
ISO 20000-1:2011	EAR (US Export Administration Regulations)	CFTC 1.31 (US)	Canadian Privacy Laws
ISO 22301	FedRAMP	DPP (UK)	DJCP (China)
ISO 27001	FIPS 140-2	EBA (EU)	EN 301 549 (EU)
ISO 27017	IRS 1075	FACT (UK)	ENS (Spain)
ISO 27018	ITAR	FCA (UK)	ENISA IAF (EU)
ISO 27701	NIST 800-171	FDA CFR Title 21 Part 11	EU-Model-Clauses
ISO-9001	NIST Cybersecurity Framework (CSF)	FERPA	EU-U.S. Privacy Shield
SOC 1	Section 508 VPATS	FFIEC (US)	GB 18030 (China)
SOC 2		FINMA (Switzerland)	GDPR (EU)

Cloud Security Alliance (CSA) GRC Stack: Governance, Risk Management and Compliance

The GRC Stack provides a toolkit for enterprises, cloud providers, security solution providers, IT auditors and other stakeholders to assess both private and public clouds against industry established best practices, standards and critical compliance requirements. https://cloudsecurityalliance.org/research/grc-stack/

- **Cloud Controls Matrix (CCM)** is designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider (https://cloudsecurityalliance.org/research/ccm/)
  - The CCM gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains
  - Defined in accordance to industry-accepted security standards, regulations, and controls frameworks such as the HITRUST CSF, ISO 27001/27002, ISACA COBIT, PCI, HIPAA and NIST.

- **Consensus Assessments Initiative Questionnaire (CAIQ)** provides an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS offerings, providing security control transparency (https://cloudsecurityalliance.org/research/cai/)
  - Provided in a form of questionnaire in the spreadsheet format, a set of questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.
  - ~ 200 yes/no questions that map directly to the CCM, and thus, in turn, to many industry standards.
  - **CAIQ answers by companies and certification are posted on the STAR website**
    - From self-assessment to certification and monitoring

CSA3.0 Security Guidance for Critical Area of Focus in Cloud Computing

The CSA3.0 defines 13 domains of the security concerns (controls) for Cloud Computing that are divided into two broad categories that define corresponding security controls.

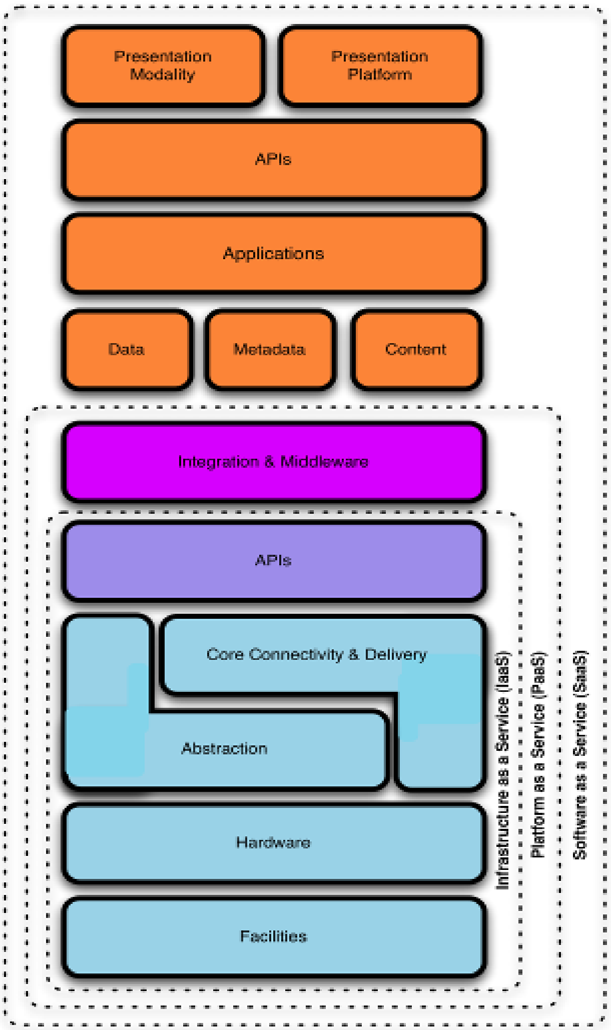
Governance domains

1. Governance and Enterprise Risk Management
2. Legal Issues: Contracts and Electronic Discovery
3. Compliance and Audit
4. Information Management and Data Security
5. Portability and Interoperability

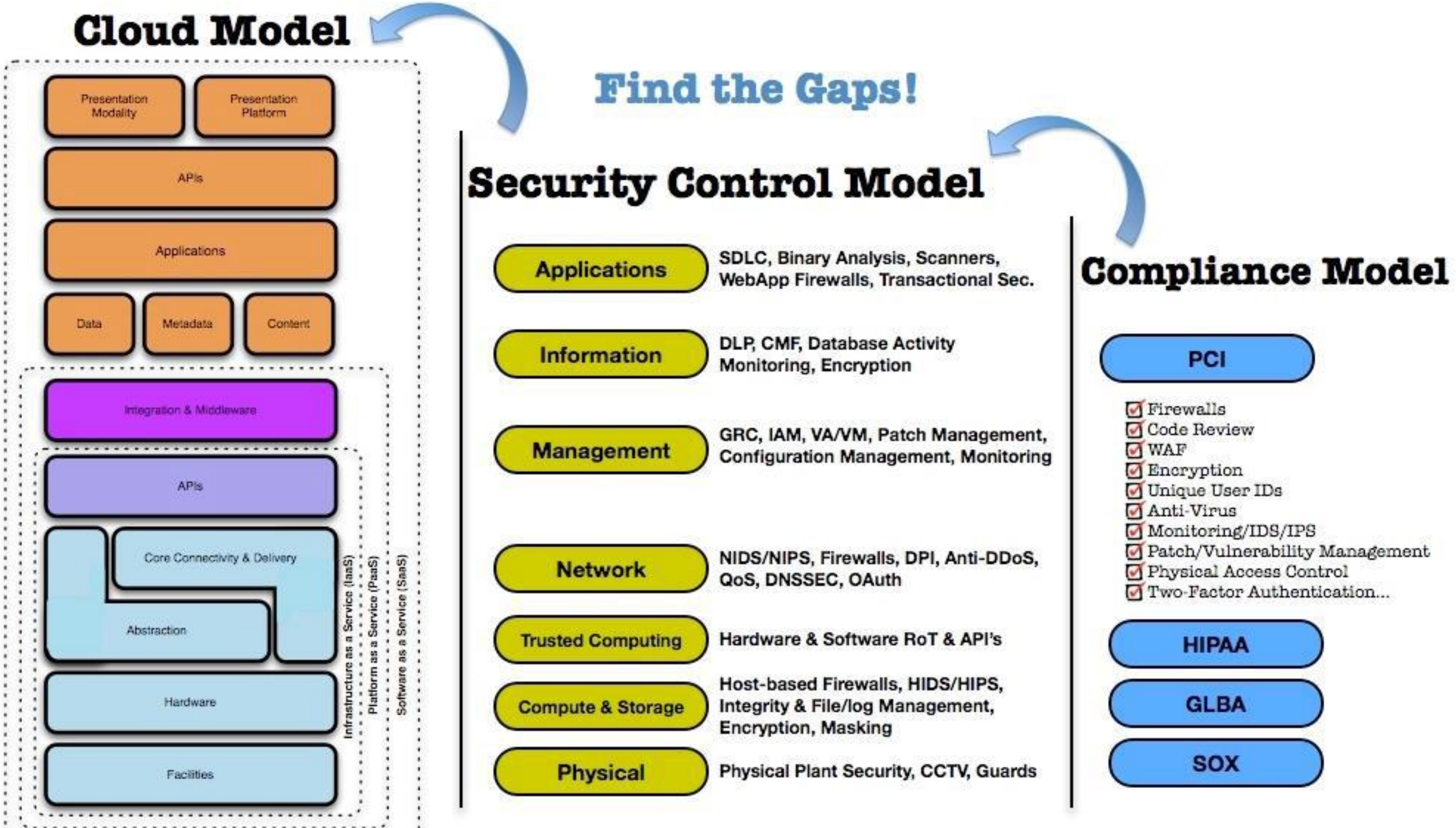
Operational Domains

6. Traditional Security, Business Continuity and Disaster Recovery
7. Data Center Operations
8. Incident Response, Notification and Remediation
9. Application Security
10. Encryption and Key Management
11. Identity and Access Management
12. Virtualization
13. Security as a Service

CSA3.0 Cloud Services Model



CSA3.0: Mapping the Cloud Model to the Security Control & Compliance



Security Control Model

- **Applications**: SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
- **Information**: DLP, CMF, Database Activity Monitoring, Encryption
- **Management**: GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
- **Network**: NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
- **Trusted Computing**: Hardware & Software RoT & API's
- **Compute & Storage**: Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
- **Physical**: Physical Plant Security, CCTV, Guards

Compliance Model

PCI

☑ Firewalls
☑ Code Review
☑ WAF
☑ Encryption
☑ Unique User IDs
☑ Anti-Virus
☑ Monitoring/IDS/IPS
☑ Patch/Vulnerability Management
☑ Physical Access Control
☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

SP500-292 (CCRA), CSA3.0

ISO/IEC 27002:2013 InfoSec Controls
(Historically originated from Common Criteria)

PCI DSS V3.0 (2013)

[ref] Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 (2013)
https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

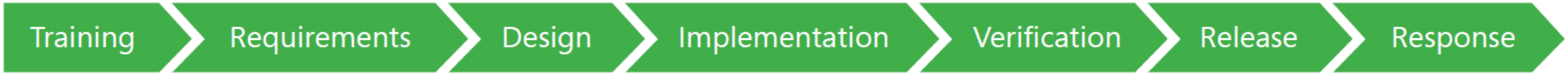
Recent CSA Publications

- **Top Threats to Cloud Computing: The Egregious 11 (2019)**
  - Contains stories about recent cloud breaches: all due to customer lame design and compromised credentials
- Top Threats to Cloud Computing: Deep Dive (2019)
  - A case study analysis for The Treacherous 12 Top Threats to Cloud Computing and relative industry breach analysis
- The Six Pillars of Security (2019)
  - Achieving Reflexive Security through integration of security < development and Operations
- Cloud Octagon Model (2019)
  - Model for Improving Accuracy and Completeness of cloud Computing risk assessment
-

DevSecOps and SSDL

- SSDL – Security Services Development Lifecycle
  - Developed by Microsoft in 2000s and widely accepted by industry

SSDL = Security and Privacy by Design



Training → Requirements → Design → Implementation → Verification → Release → Response

- Security design principles by big software vendors Amazon, Apple, Google

- DevOps meets Security -> DevSecOps
- DevSecOps as alternative to Waterfall model where security is treated as non-functional requirement and is addressed at later stages of development

DevSecOps: Building a Secure Continuous Delivery Pipeline

- DevSecOps is extension of DevOps with inclusion of Security
- Traditional InfoSec crisis: Lost identity
  - 100 developers:10 operations:1 security -- problem
- Continuous delivery pipeline and DevSecOps toolchain: 5 stages
  - Develop: version, sprint, unit test
  - Inherit: libraries and dependencies
  - Build: acceptance testing, audit
  - Deploy (moving artefact from built machine to production)
  - Operate: user and attacker faced

Security Testing: Misconfiguration and secrets

- Creds leakage, e.g.
  - Creds in source code on github
  - AWS access key in a version control history
- Use **git-secrets** https://github.com/awslabs/git-secrets
  - Prevents from committing passwords and other sensitive information to a git repository
  - git-secrets scans commits, commit messages, and --no-ff merges to prevent adding secrets into your git repositories.
  - If a commit, commit message, or any commit in a --no-ff merge history matches one of your configured prohibited regular expression patterns, then the commit is rejected.
  - Installation for Linux, Mac, Windows
- Use: git secrets –scan[-history]

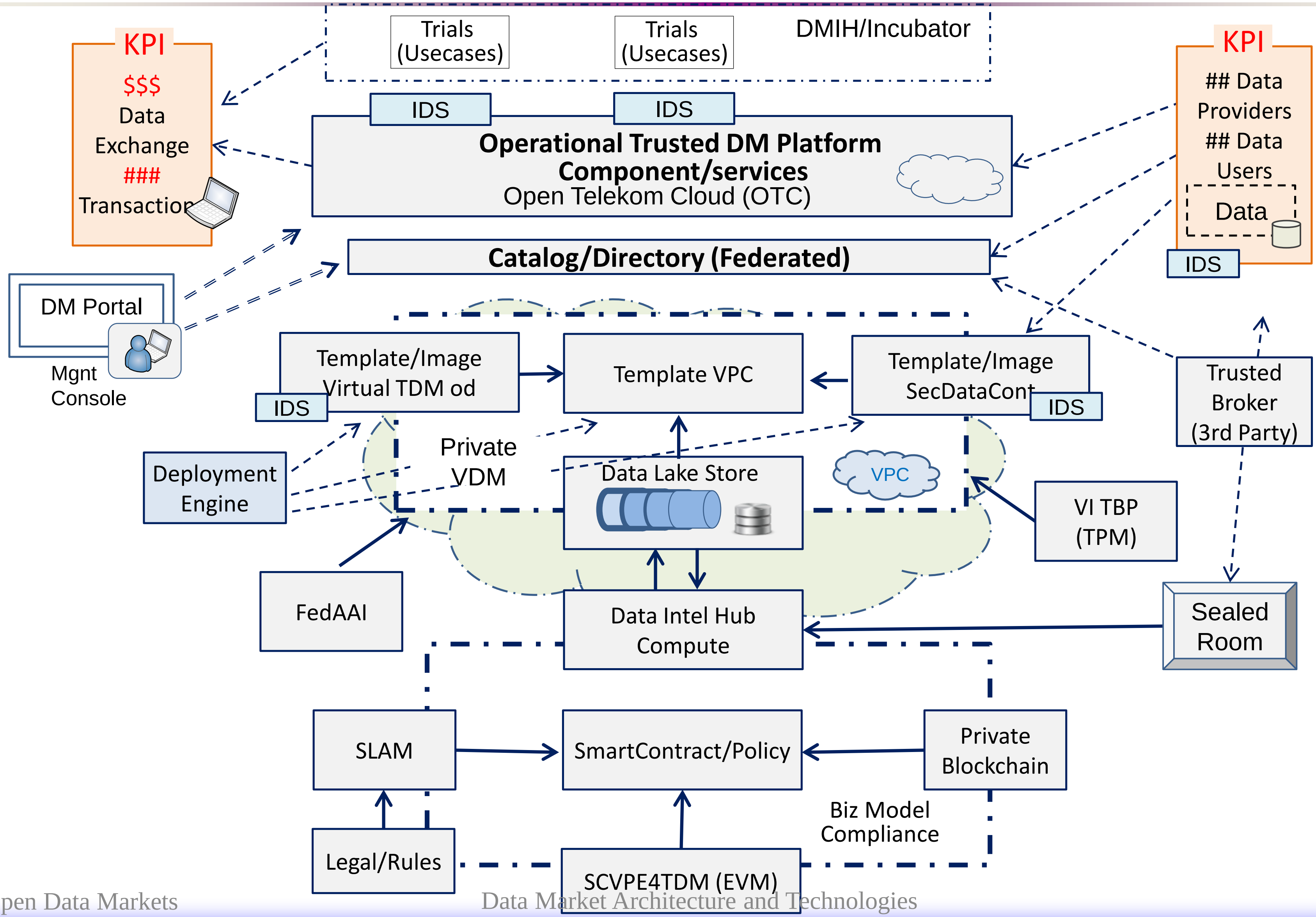
Security Development Practices and OSS

- Security of Open Source Software (OSS) is slightly agitated
  - Security problems require security expertise and not all developers are security experts.
    - More advanced topics like cryptography, for example, further narrow the field for those who can review code for such security flaws.
  - There's also no standard way of documenting security on open source projects. In the top 400,000 public repositories on GitHub, only 2.4% had security documentation in place.
  - Dependencies in open source projects allow some vulnerabilities to fly under the radar..
- According to the latest Veracode report, only 28% of organizations do any kind of regular analysis to find out what components are built into their applications.
  - **94% commercial software have dependencies on OSS libraries**
  - As the use of open source code grows, this risk surface expands.
- According to the Snyk survey (https://snyk.io/):
  - 88 % of open source code maintainers add security-related announcements to the release notes
  - 34 % say that they deprecate the older, insecure version.
  - 25% that they make no effort at all to notify users of vulnerabilities
  - only 10% file a CVE reports

Cloud Security Config Monitoring

- AWS Tools
  - AWS Config – Monitor configuration changes
  - AWS CloudTrail - Create a trail to retain a record of events
  - Amazon Inspector - analyzes the behavior of AWS resources and helps identify potential security issues
  - Amazon GuardDuty – Activity monitoring & Intelligent threat detection
- Third party tools
  - https://www.threatstack.com
  - https://www.alienvault.com
  - https://evident.io – multicloud solution
- InSpec is compliance as code service https://www.inspec.io
  - Turns compliance, security, and other policy requirements into automated tests
  - Includes compliance requirements into code

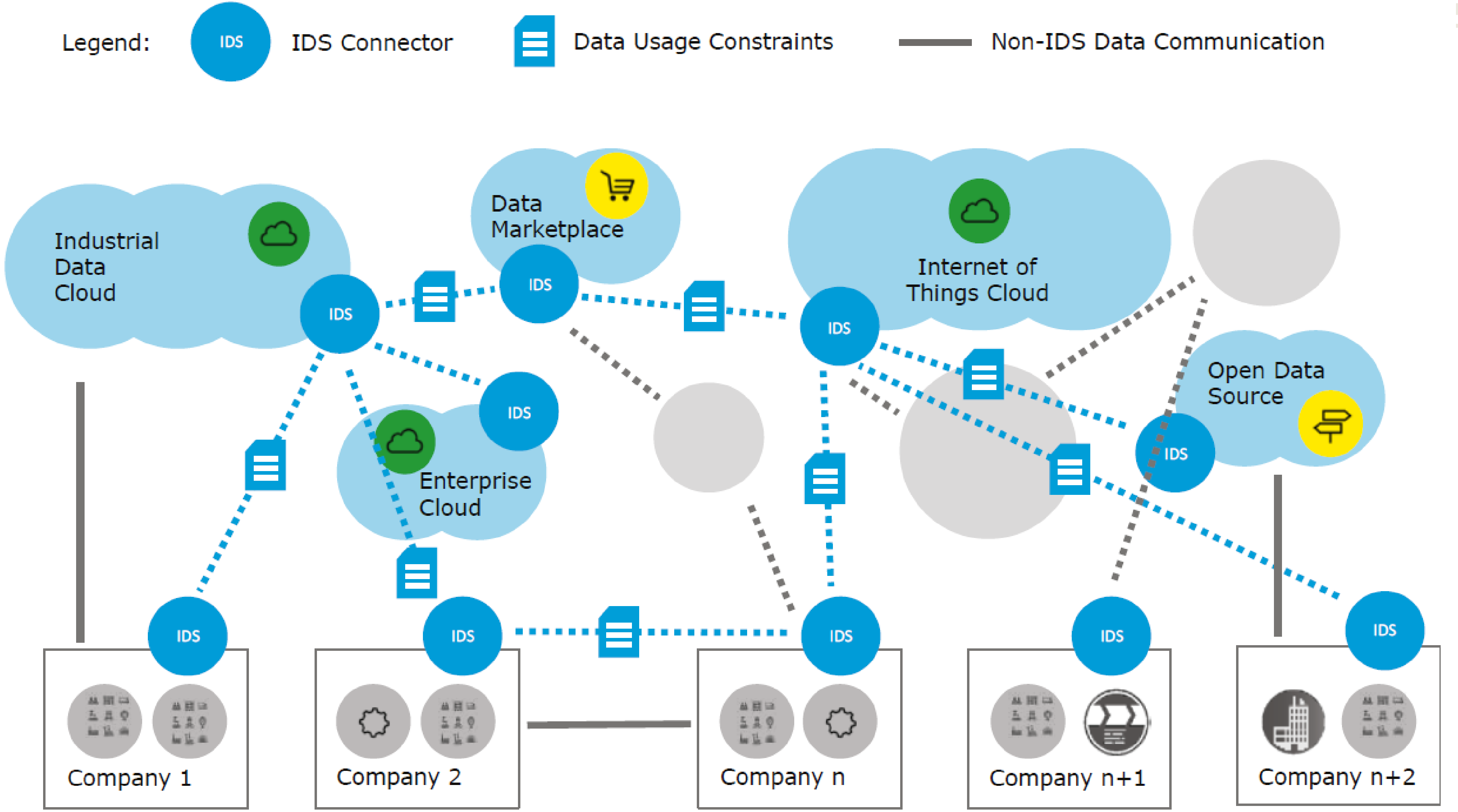
Case Study: Trusted Data Market Infrastructure and composable components



TDM Infrastructure Templates and DevOps tools

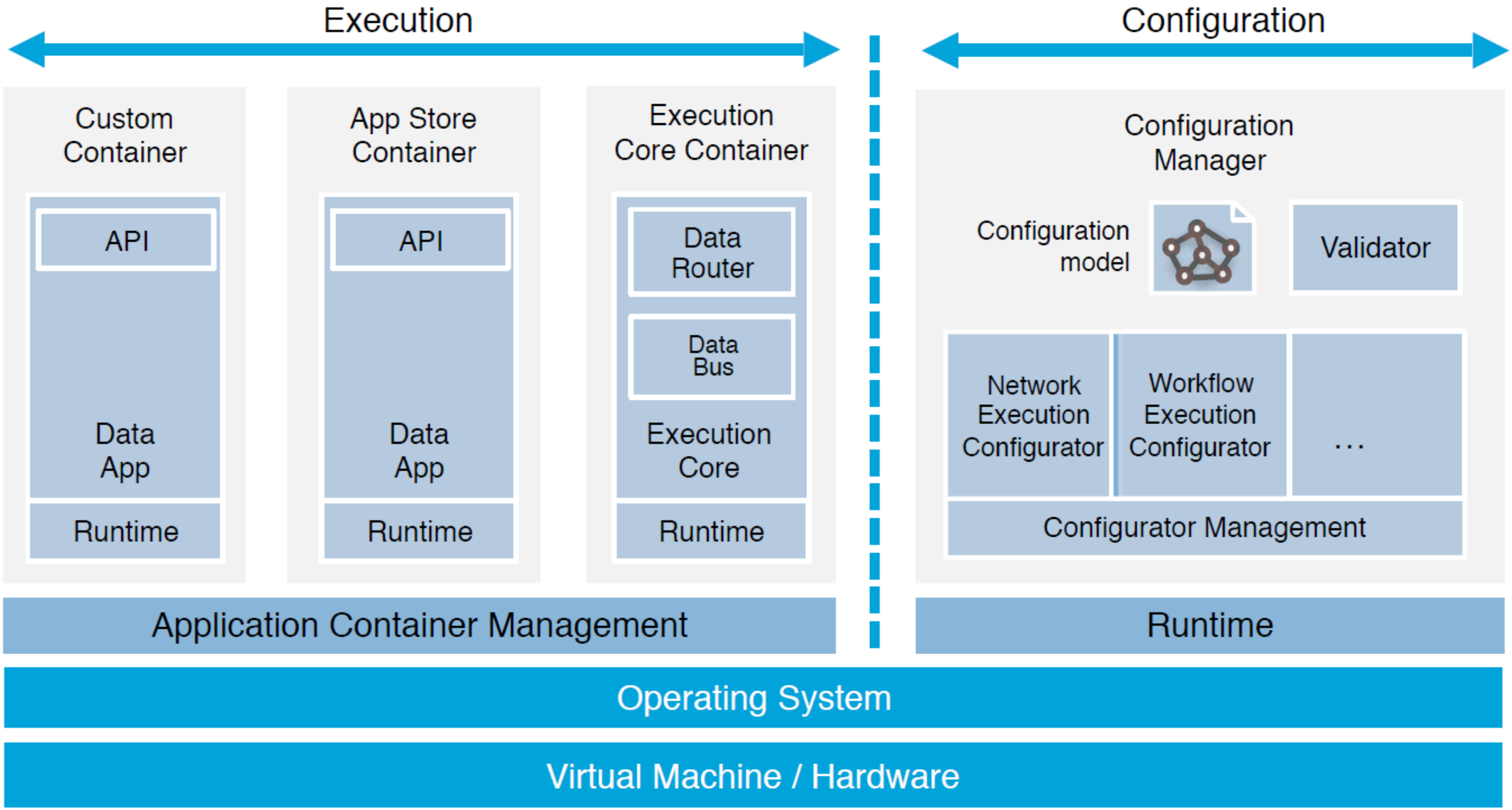
- DM infrastructure is provisioned on demand for each cooperating groups of partners
  - Digitally Enforceable Policy/Contract is embedded into infrastructure
- DM infrastructure template is composed of basic infrastructure patterns described
  - For platform dependent patterns in the formats of cloud platform
    - AWS: CloudFormation
    - Azure: Azure Resource Manager (ARM)
  - For general infrastructure descriptions/templates
    - Ansible – YAML based, combines computational and network resources
    - Others: Chef (directly supported by AWS), Puppet, Terraform (directly supported by Azure)
  - Blockchain enabled Virtual Private execution Engine (SCVPE)

Leveraging IDS Architecture and Connector with Cloud



- IDS Connector is the main functional component
- No specifically defined infrastructure

Reference Architecture Data Connector

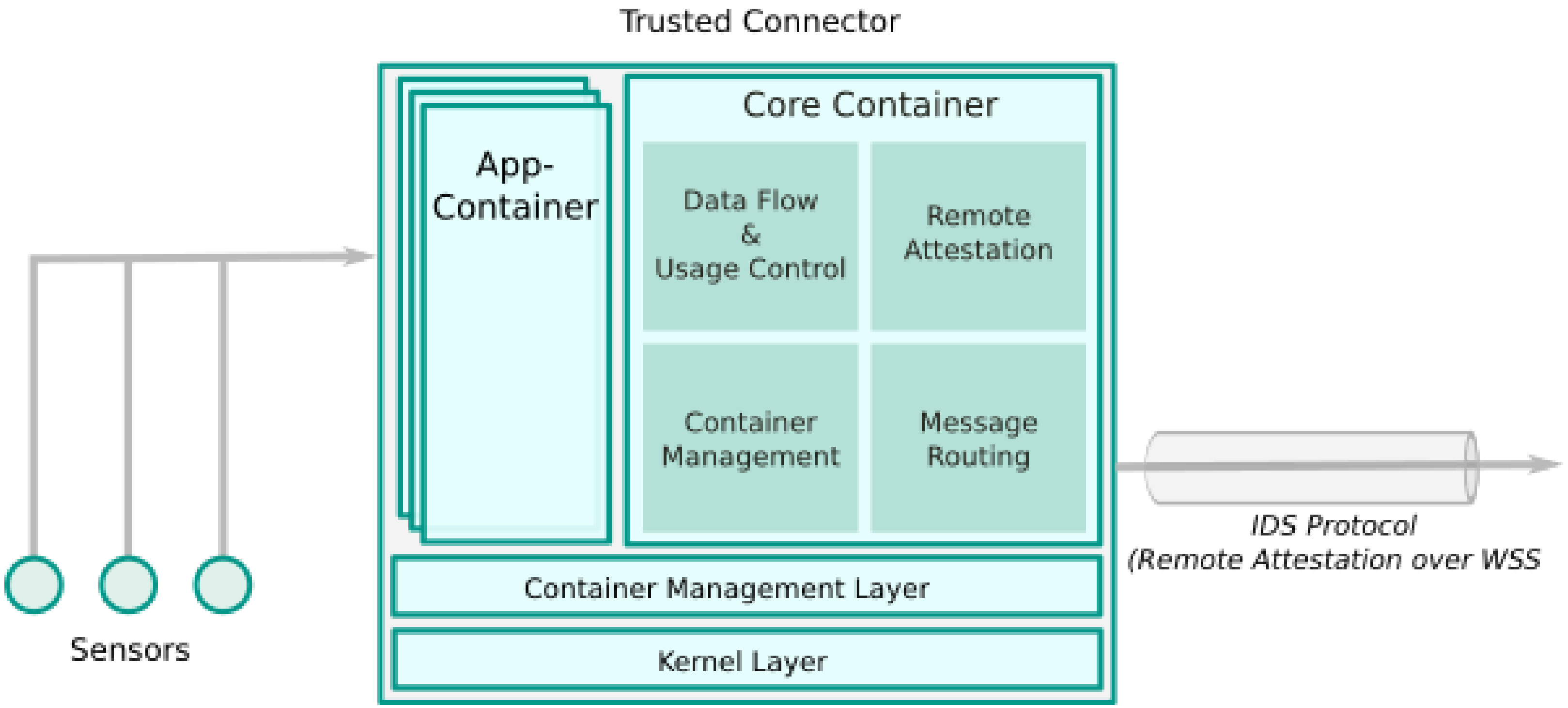


- Execution and configuration
- Application container

- Undergoing DIN Standardisation

LUCON: Trusted Connector Implementation

https://industrial-data-space.github.io/trusted-connector-documentation/



- The Trusted Connector features the secure container management layer *trust|me* as an alternative to Docker.
- trust|me basic mechanisms are similar to Docker (namespaces, cgroups and chroot)
- trust|me was developed as a security architecture including secure boot, platform integrity measurements, and a hardened kernel.

Research topics in Cloud Security

- Federated Identity Management and Access Control in hybrid enterprise-CSP infrastructure + Identity provisioning

- Cloud Access and Security Brokers: Security with Trusted Third Party
- VPC infrastructure security model and analysis

- Bootstrapping cloud based VPC and enterprise or applications trust domains
  - Leveraging Zero Trust model in networking security
  - Leveraging TPM and Trusted Computing Platform Architecture

- Data protection in clouds at all stages of data processing (Data Lifecycle)
  - Data Sovereignty and Data Ownership attribute/property
  - Computationally Enforceable Policies and data provenance
  - Data Management Infrastructure for AI and Digital Twins
  - Blockchain enabled data provenance in multi-platform multi-cloud environment

- Personal information protection in cloud based multitenant multi-tier applications

- Cloud infrastructure to enable GDPR + FAIR data principles

Summary and take away

- Cloud Security impose new security challenges
- Cloud Security is based on the core security principles and models
- Shared responsibility is the basic model cloud security
- Cloud compliance provides a basis for wider cloud services adoption and inter-cloud integration.
- Compliance is supported by numerous standards, legislation, regulatory guidelines and industry best practices that jointly define a compliance framework
  - Knowing major cloud compliance standards is necessary for correct cloud services design, deployment and operation
- IDSA architecture and Trusted Data Market as example of critically trusted environment in cloud

Discussion and Questions