CYBER VATTAM

Cloud Security

Presented by
Venkatesh Jambulingam
Cloud Security Expert

02-Oct-2022

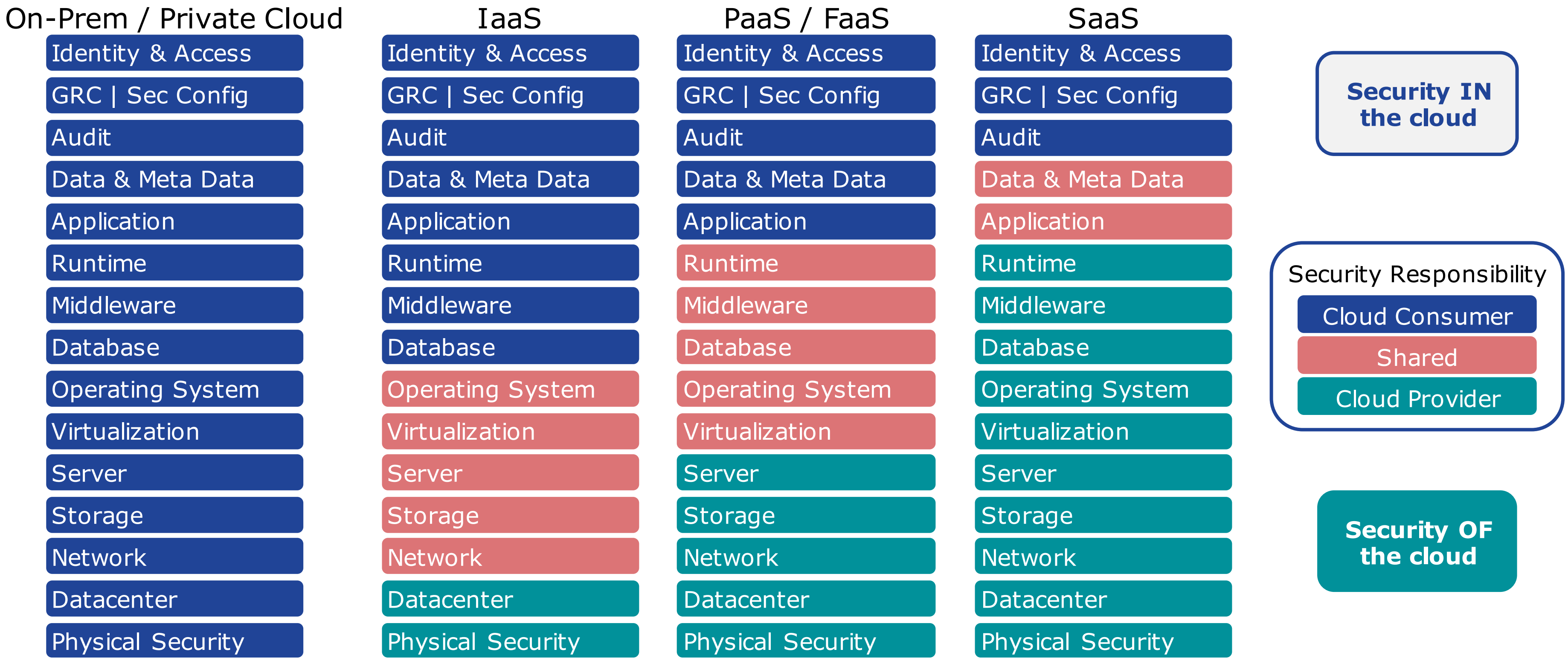
Contents

- Shared Security Responsibility Model

- Security of the cloud
  - Facilities Physical Security
  - Hardware Security
  - Abstraction/Virtualization Security
  - API/Management Plane Security
  - Core Connectivity Security
  - Business Continuity
  - Disaster Recovery

- Security in the cloud
  - Cloud Native Application Protection Platform (CNAPP)
    - Cloud Workload Protect Platform (CWPP)
    - Cloud Security Posture Management (CSPM)
    - SaaS Security Posture Management (SSPM)
  - Security Service Edge (SSE)
    - Secure Web Gateway (SWG)
    - Cloud Access Security Broker (CASB)
    - Zero Trust Network Access (ZTNA)
  - Cloud Identity
  - Cloud Identity and Entitlement Management (CIEM)
  - Cloud Data Security

Cloud Security Shared Responsibility Model



	On-Prem / Private Cloud	IaaS	PaaS / FaaS	SaaS
Identity & Access	🟦	🟦	🟦	🟦
GRC | Sec Config	🟦	🟦	🟦	🟦
Audit	🟦	🟦	🟦	🟦
Data & Meta Data	🟦	🟦	🟦	🟥
Application	🟦	🟦	🟦	🟥
Runtime	🟦	🟦	🟥	🟩
Middleware	🟦	🟦	🟥	🟩
Database	🟦	🟦	🟥	🟩
Operating System	🟦	🟥	🟥	🟩
Virtualization	🟦	🟥	🟥	🟩
Server	🟦	🟥	🟩	🟩
Storage	🟦	🟥	🟩	🟩
Network	🟦	🟥	🟩	🟩
Datacenter	🟦	🟩	🟩	🟩
Physical Security	🟦	🟩	🟩	🟩

Security IN the cloud

Security Responsibility

- 🟦 Cloud Consumer
- 🟥 Shared
- 🟩 Cloud Provider

Security OF the cloud

Security of the Cloud

Security of the cloud

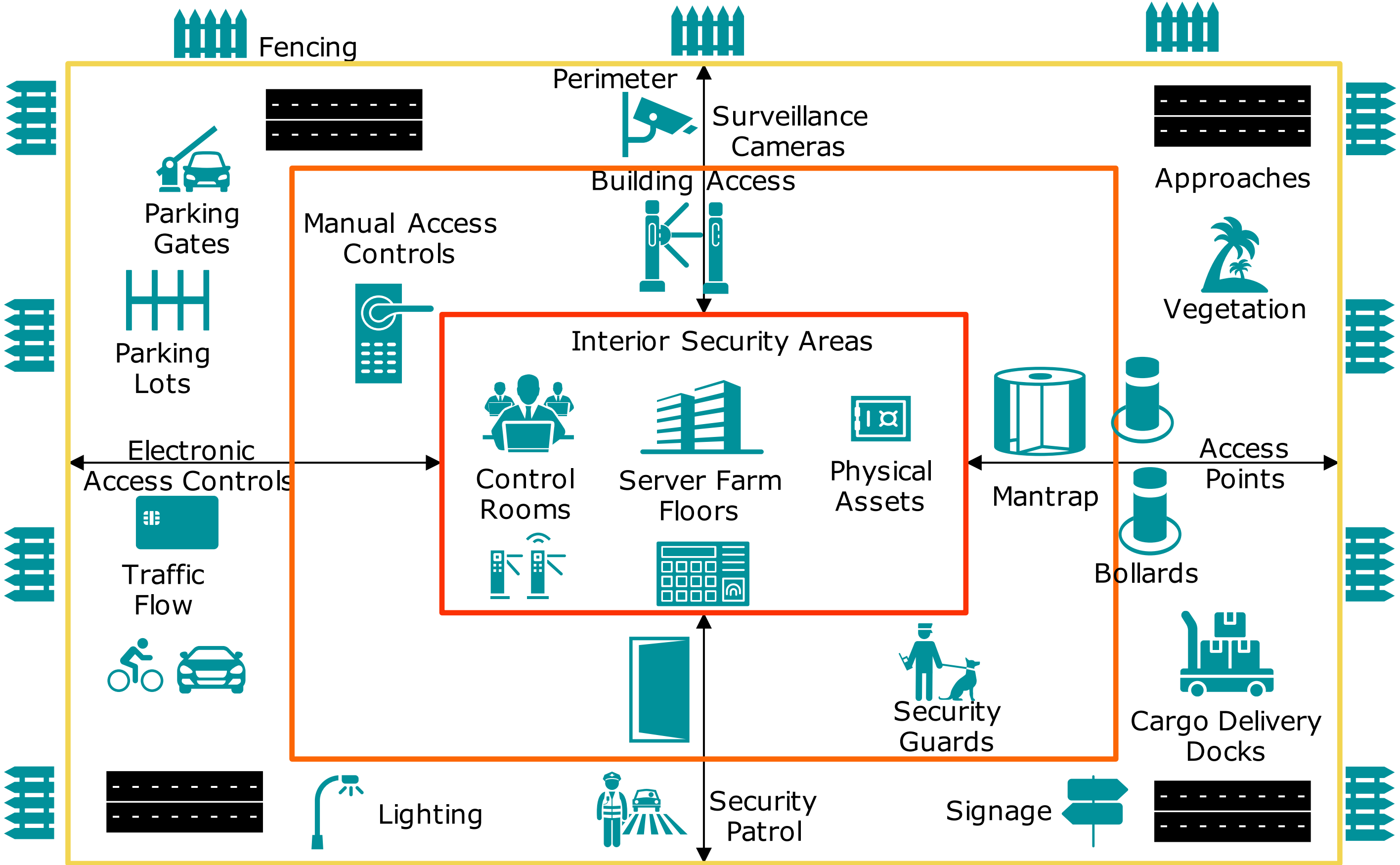
Platform Security

- Facilities & Physical Security
- Hardware Security
- Abstraction / Virtualization Security
- Core Connectivity Security
- APIs / Management Plane
- Business Continuity / Disaster Recovery

Facilities and Physical Security

Security Controls	Description
Location Security	The location of the data center itself should be safe from natural disaster, political unrest, availability of power, connectivity, ease of access, skilled people availability, Unmarked Buildings.
Physical Security	Landscaping, Fencing, Tire shredders, Cages, Bollards, Security Guards, Motion Sensor, Mantraps, Video Surveillance (CCTV), warning signs, Layered Perimeter Defense, Alarms, Safes, Badges, Smart Card & Biometrics
Environment Security	Redundant Power sources, Redundant ISP connectivity, UPS, Backup Generators with Fuel, HVAC, Lighting, Protective Barriers, Optimal Humidity Level, Fire Prevention, Detection, and Suppression
People Security	Good Hiring techniques, background verification, credit history, effective termination practices, Supervision of employees, tracking employee activity, Separation of duties, Rotation of duties

Facilities and Physical Security



Hardware Security

- The Physical hardware that is hosting the applications and data must be secured by cloud service provider.

- Door locks to wiring closets and access to main and intermediate distribution frame (MDF and IDF) areas
- No windows, or secured windows
- Protected wiring infrastructure and cable runs
- Security cameras and intrusion detection system (IDS)
- Hardened management stations
- Physical access should be strictly controlled, both at the perimeter and at room ingress points, by professional security staff using video surveillance, intrusion detection systems, and other electronic methods
- Authorized staff should pass two factor authentication a minimum of two times to access data center floors
- Biometric multifactor authentication (MFA) is highly recommended

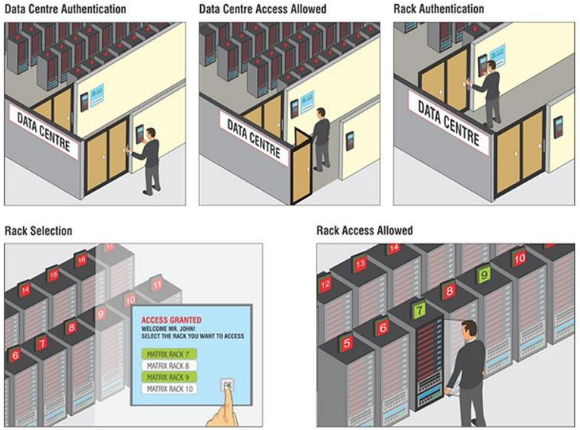


Image Credit: ISR Magazine

Image Credit: Brain Trust

Abstraction/Virtualization Security

Cloud Security providers virtualize the resource pool and slice it as needed and deploy multiple customer’s data on the single hardware resource

- Virtualization Protection
  - Hypervisor Hardening
    - Patching & Updating the Hypervisor itself
    - Logging & Monitoring the Hypervisor
    - Patching Host OS
  - Instance Isolation
    - Logical Isolation
    - Prevent data leaks & inter VM attack
    - Sandbox Testing
  - Host Isolation
    - Physical & logical isolation
    - Monitor for Guest Escape

- VM escape/Guest Escape: When a process running in the VM interacts directly with the host OS or Hypervisor

- VM escape protection techniques
  - Patch VMs and VM software regularly
  - Only install what you need on the host and the VMs
  - Install verified and trusted applications only
  - Use strong passwords
  - Control VM access

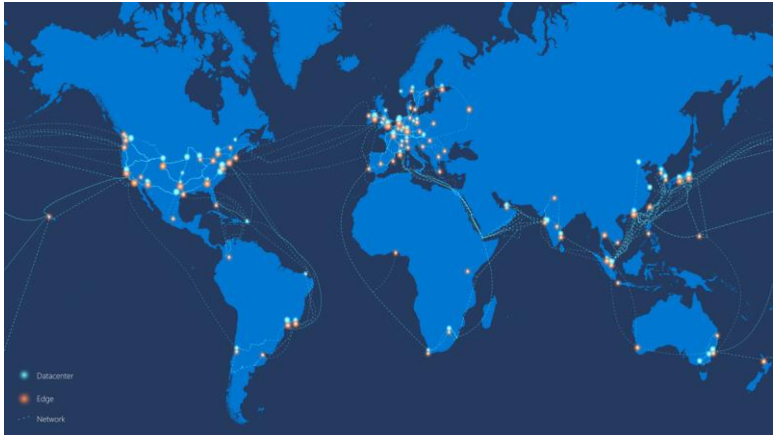
Core Connectivity Security

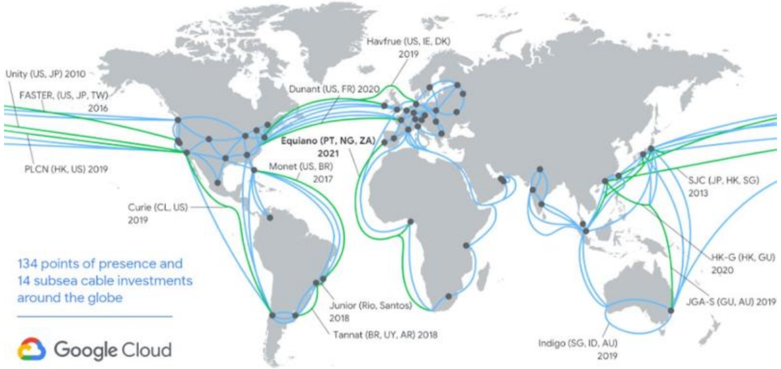
Cloud Service Providers have a vast private network & their own dedicated backbone connectivity and they do not use general internet for communication

- ▶Cloud provider should have proper network security controls
- ▶Protection Systems – Firewalls, Proxies, Gateways etc
- ▶Detection Systems – IDS/IPS, Honeypots, Deception Technologies
- ▶Communication Protection – VPN, Encryption, Authentication
- ▶Continuous Improvement – Vulnerability Assessments & Penetration testing

Cloud Service Provider should enable their customers to configure security networking by providing network security controls & supporting 3rd party network security controls

- ▶Virtual Local Area Network (VLAN)
- ▶Dynamic Host Control Protocol (DHCP)
- ▶Domain Name Service (DNS), its configuration & maintenance
- ▶Virtual Private Network for connectivity between cloud & on-prem networks



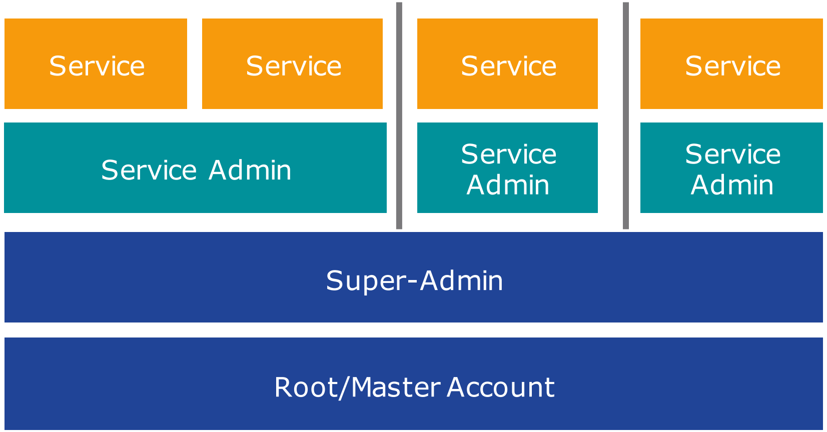


Management Plane/ API security

- Cloud APIs and web consoles are the way the management plane is delivered. API’s allow for programmatic management of the cloud. They are the glue that holds the cloud’s components together and enables their orchestration.

- Cloud providers and platforms will also often offer Software Development Kits (SDKs) and Command Line Interfaces (CLIs) to make integrating with their APIs easier.

- Perimeter security
- Customer authentication
- Internal authentication and credential passing
- Authorization and entitlements
- Logging, monitoring, and alerting



Business Continuity

- **Business Continuity Plan**: A playbook to address large scale failures. The goal is to get key people & processes up and running for business to resume within an acceptable amount of time.

- Business continuity within Cloud provider
  - Backup Cloud configurations & Infrastructure as Code
  - Adapt the architecture to leverage provider resiliency
  - Be considerate of cost to risk of outage (business impact analysis)
  - Data Replication across regions using provider mechanism
  - Cloud Storage back up & Snapshot Capabilities
  - Design applications to fail gracefully
  - Leverage DNS to redirect traffic to DR site
  - For extreme cases, think of different cloud provider as part of BCP
  - Chaos Engineering

Disaster Recovery

- **Disaster Recovery:** A tactical plan to restore technology systems that are critical to key people & process for a given business.

- Key Factors to consider
  - Human Safety should be the priority
  - Should have Food Supplies & Water
  - DR Plan
  - Communication Equipment
  - Network Artifacts
  - Software Copies
  - Documentation

- Disaster Recovery Priorities:
  - Critical Asset Inventory
  - Event Declaration Criteria
  - Disaster Recovery Rules

Disaster Recovery Testing Methods

- Tabletop Test
  - Collate, Read documents & discuss the steps
- Dry Run
  - Some impact to daily operations where you do perform these steps. This will be a scheduled test
- Full Test
  - Full impact to daily operations. Usually done without informing in advance. This will be an unscheduled test

- Disaster Recovery Metrics:
  - Maximum Allowable Downtime (MAD)
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
  - Annual Loss Expectancy (ALE)

Security in the Cloud

CYBER
VATTAM

Security in the cloud

Service Security

- Hybrid/Multi-Cloud Security Challenges
- Cloud Security solution cornerstones
- Cloud Native Application Protection Platform (CNAPP)
  - Cloud Workload Protect Platform (CWPP)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SSPM)
- Security Service Edge (SSE)
  - Secure Web Gateway (SWG)
  - Cloud Access Security Broker (CASB)
  - Zero Trust Network Access (ZTNA)
- Cloud Identity
- Cloud Infrastructure Entitlement Management (CIEM)
- Cloud Data Security

Hybrid/Multi Cloud Security Challenges

Decentralized Administration & Lack of Visibility

- No CMDB, real-time asset inventory or network topology diagrams exist for public cloud
- Large number of privileged users with little governance
- Traditional security is focused on Infrastructure built in house

Complexity of Compliance Management in the Cloud

- Hundreds of unique cloud services, with more added daily
- Proving compliance to auditors challenging in dynamic environments
- People and companies move to a greater and greater use of Cloud they need to be more fluid and rapid to reduce risk

Inability to Rapidly Detect & Respond to Threats

- Data that is created natively in the cloud is invisible to traditional security measures
- Traditional SIEMs do not have cloud context, and are unable to adapt to large data volumes and speed of change in cloud
- Network security fails to protect data in the cloud and mobile era

Are my Apps & Data Secure?

Am I compliant?

Are my apps & data secure?

What do I have in the cloud?

What was historical behavior seen?

Are my hosts & containers secure?

What is happening?

Who is making changes & why?

Cloud Security Solution Cornerstones

Solution Cornerstone	Cloud Security Services	Technology Landscape
I want to secure my modern workplace but also leverage native controls	Security for Digital Workplace	Microsoft 365 Suite zoom
I want to have visibility and control of SaaS services both sanctioned and unsanctioned	Cloud Access Security Broker	Skyhigh Security **Microsoft Defender for Cloud Apps**
I want to secure my data center in the cloud without impacting the agility cloud brings	Cloud Workload Protection Platform	TREND MICRO CROWDSTRIKE PRISMA BY PALO ALTO NETWORKS aqua
I want to utilize the native security controls from my CSP and build a roadmap together	Native Cloud Security Services	amazon web services Azure Google Cloud
I want to retain control of who has access to my data, where it's located and be the only custodian to my keys	Cloud Data Security	THALES Building a future we can all trust aws ENTRUST
I want to retain control of who has access to my data, where it's located and be the only custodian to my keys	Cloud IAM & IEM	SailPoint SAVIYNT Microsoft Entra: Microsoft Azure Active Directory, Permissions Management, Verified ID orca security ermetic
I want to ensure my dev ops pipeline is secure	Cloud Application Security	AzureDevOps GitHub ATLASSIAN
What are my cloud risks today? Am I still compliant?	Cloud & SaaS Security Posture Management	PRISMA BY PALO ALTO NETWORKS CHECK POINT CloudGuard orca security

Cloud Workload Protection Platform

Introduction

- Cloud Workload Protection Platform (CWPP) is a workload-centric security product that protect server workloads in hybrid, multi-cloud and data center environments.
- Provide consistent visibility and control for physical machines, virtual machines (VMs), containers and serverless workloads, regardless of location.
- Protect workloads using a combination of system integrity protection, application control, behavioral monitoring, intrusion prevention and optional anti-malware protection at runtime.
- CWPP offerings should also include scanning for workload risk proactively in the development pipeline.

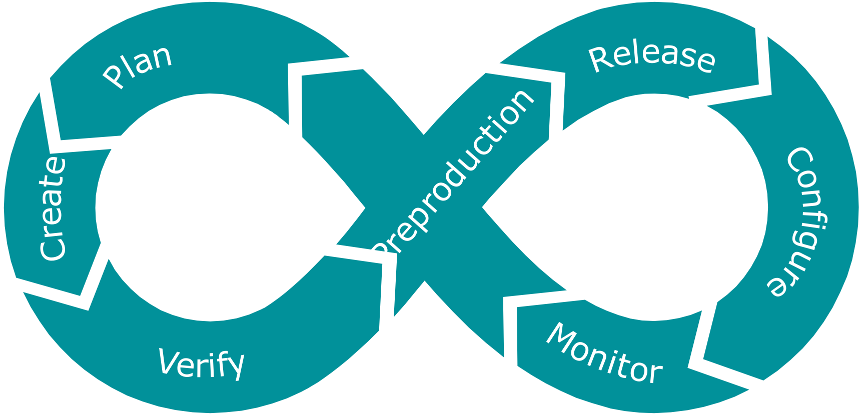
Evolution of Workloads

Workload	Physical Machines	Virtual Machines	Containers	Serverless
Virtualization	None/Monolithic	Hardware	Operating System	Application Runtime
Unit of Scale	Physical Servers	Virtual machines	Apps/Services	Resources
Life Span	Years	Months to Years	Minutes to Days	Seconds to Minutes

Cloud Workload Protection Platform

Features & Capabilities

Secure Build
Vulnerable Components
Cloud Configuration
Secrets
Malware
API discovery



Runtime Protection
Workload Vulnerability
Workload Configuration
Workload Segmentation
Integrity Monitoring
Application Control
Behavioural Monitoring
HIPS
Anti-malware

Container Registry Scanner

Containers
Serverless, PaaS/FaaS
Virtual Machine

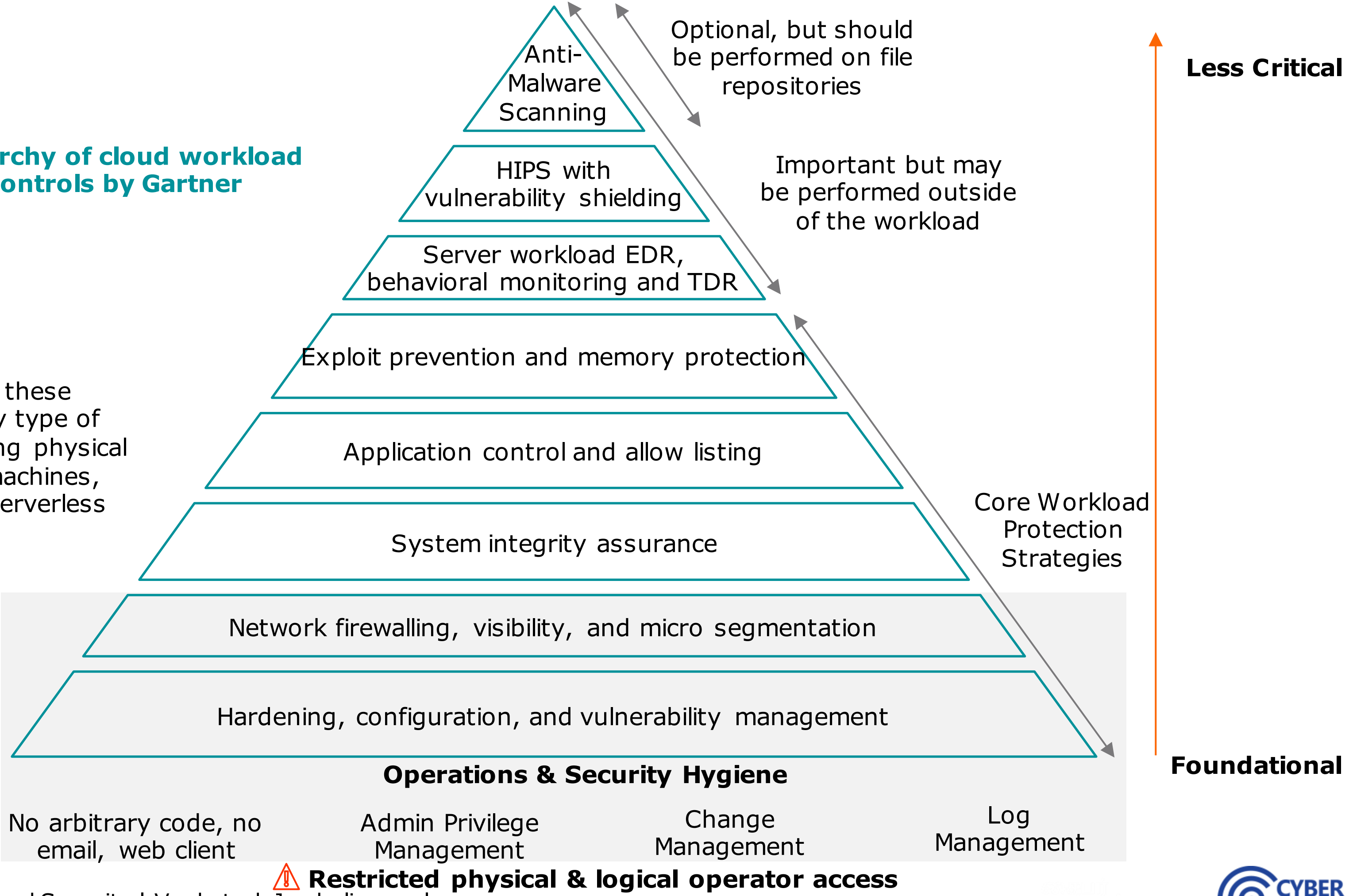
Public / Private Cloud

Virtual Server
Physical Server
Containers

Data Centre

Risk based hierarchy of cloud workload protection controls by Gartner

CWPPs can apply these capabilities in any type of workload, including physical servers, virtual machines, containers, and serverless functions.



Anti-Malware Scanning

HIPS with vulnerability shielding

Server workload EDR, behavioral monitoring and TDR

Exploit prevention and memory protection

Application control and allow listing

System integrity assurance

Network firewalling, visibility, and micro segmentation

Hardening, configuration, and vulnerability management

Operations & Security Hygiene

No arbitrary code, no email, web client

Admin Privilege Management

Change Management

Log Management

⚠ **Restricted physical & logical operator access**

Optional, but should be performed on file repositories

Important but may be performed outside of the workload

Core Workload Protection Strategies

Less Critical

Foundational

Cloud Security Posture Management

Introduction

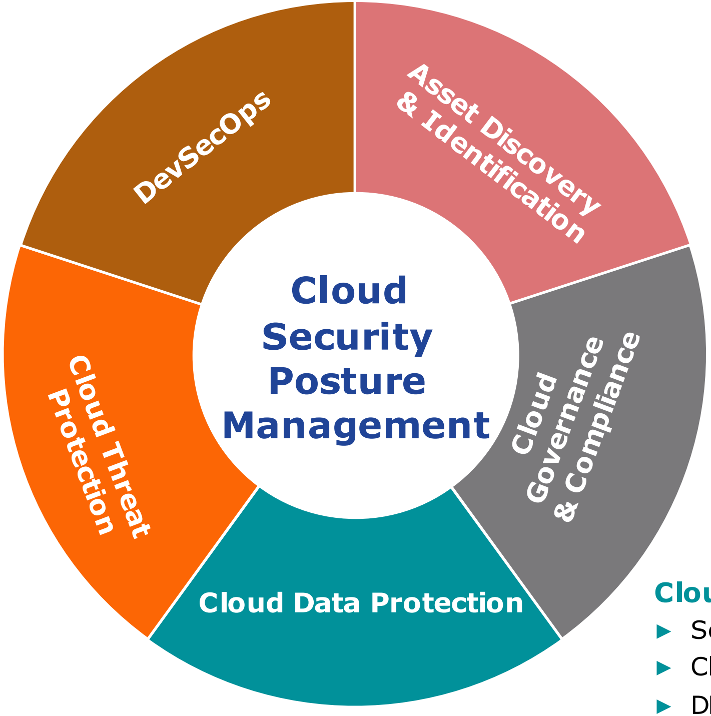
Security posture is a reference to the cybersecurity strength of an organization, which includes an assessment of its ability to detect and respond to security threats. Security posture encompasses readiness for both external and internal threats, as well as response and remediation capabilities.

DevSecOps

- Support for CI/CD integration by shifting security left
- API enablement
- Ensuring that IaC templates are vulnerability

Cloud Threat Protection

- Applying a single, unified policy across all public clouds
- Continuous behavior monitoring
- Implementing guardrails while maintaining the speed and flexibility of Cloud


Cloud Security Posture Management
DevSecOps
Asset Discovery & Identification
Cloud Governance & Compliance
Cloud Data Protection
Cloud Threat Protection

Asset Discovery & Identification

- Asset discovery
- Risk assessment, prioritization and remediation support
- Automatic remediation

Cloud Governance & Compliance

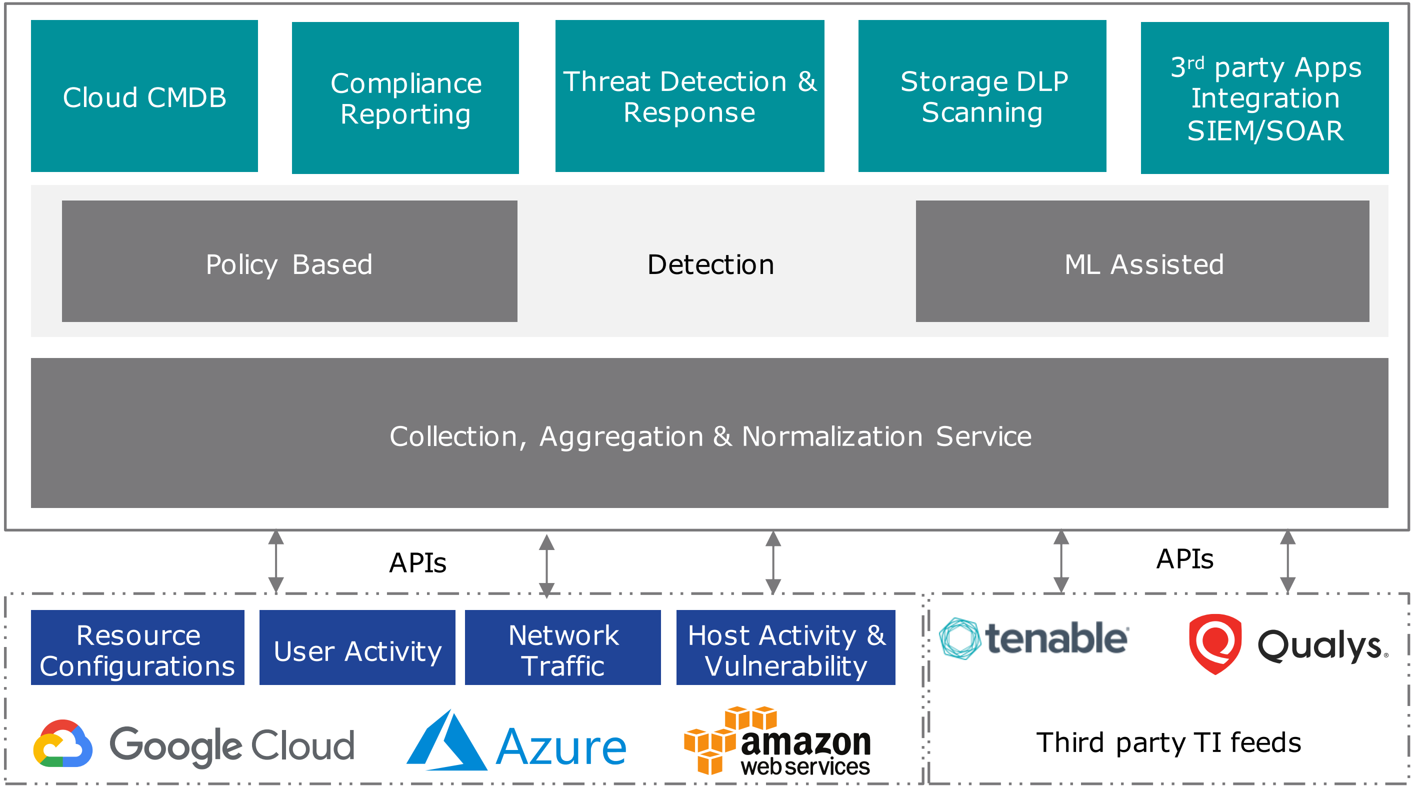
- Framework and regulatory compliance packs
- Automatic and scheduled reporting

Cloud Data Protection

- Security & Privacy by Design
- Cloud encryption
- DLP

Cloud Security Posture Management

Typical Components



SaaS Security Posture Management (SSPM)

Introduction, Features & Benefits

- SaaS Security Posture Management (SSPM) is an automated continuous monitoring process for cloud-based Software-As-A-Service (SaaS) applications to minimize risky configurations, prevent configuration drift, and help security and IT teams to ensure compliance.

Visibility

- Centralized visibility of all SaaS apps in use in the organization

Policies

- Detect risky settings & evaluate risk by comparing against best practices & industry standards

Alerts

- Receive security alerts for misconfiguration, policy drift as per the organization policy

Remediation

- Automated workflows and recommendations to fix the security risks & misconfiguration

SSPM Benefits

Simplifies compliance management

Prevents cloud misconfigurations

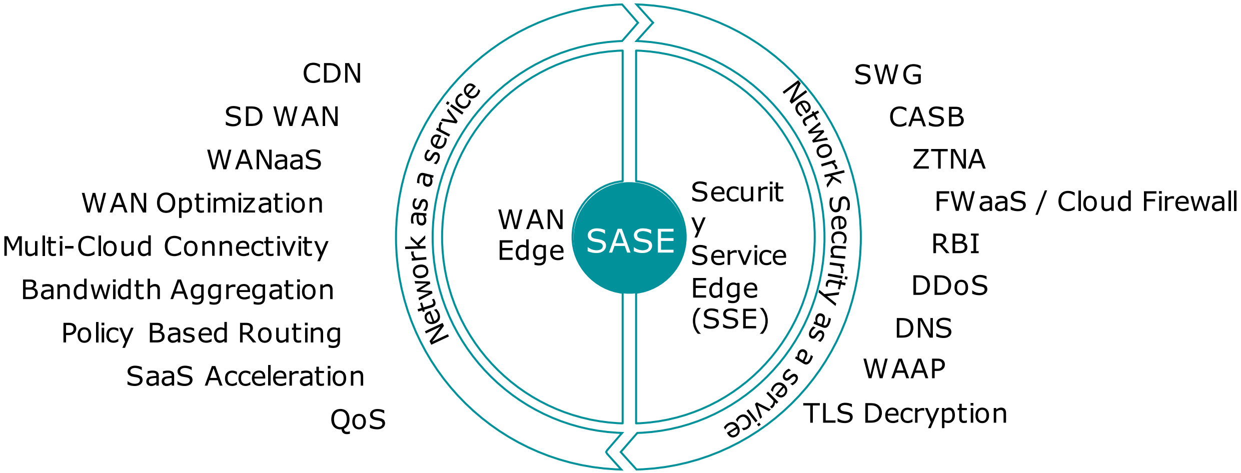
Detects excessive permissions

CSPM	SSPM
Scan IaaS & PaaS workloads	Analyse & Protect SaaS workloads
amazon web services	Microsoft 365 salesforce
Azure	zoom servicenow
Google Cloud	workday slack

Secure Access Service Edge (SASE)

Introduction

- Secure Access Service Edge (SASE) consists of two distinct components given below
  - Security Service Edge that provides network security as a service
  - WAN edge that provides network as a service



Secure Web Gateway

Introduction

- A secure web gateway (SWG) is a security solution that prevents unsecured internet traffic from entering an organization’s internal network. It is used by organizations globally to protect employees and users from accessing or being infected by malicious websites. It also helps to ensure regulatory compliance.

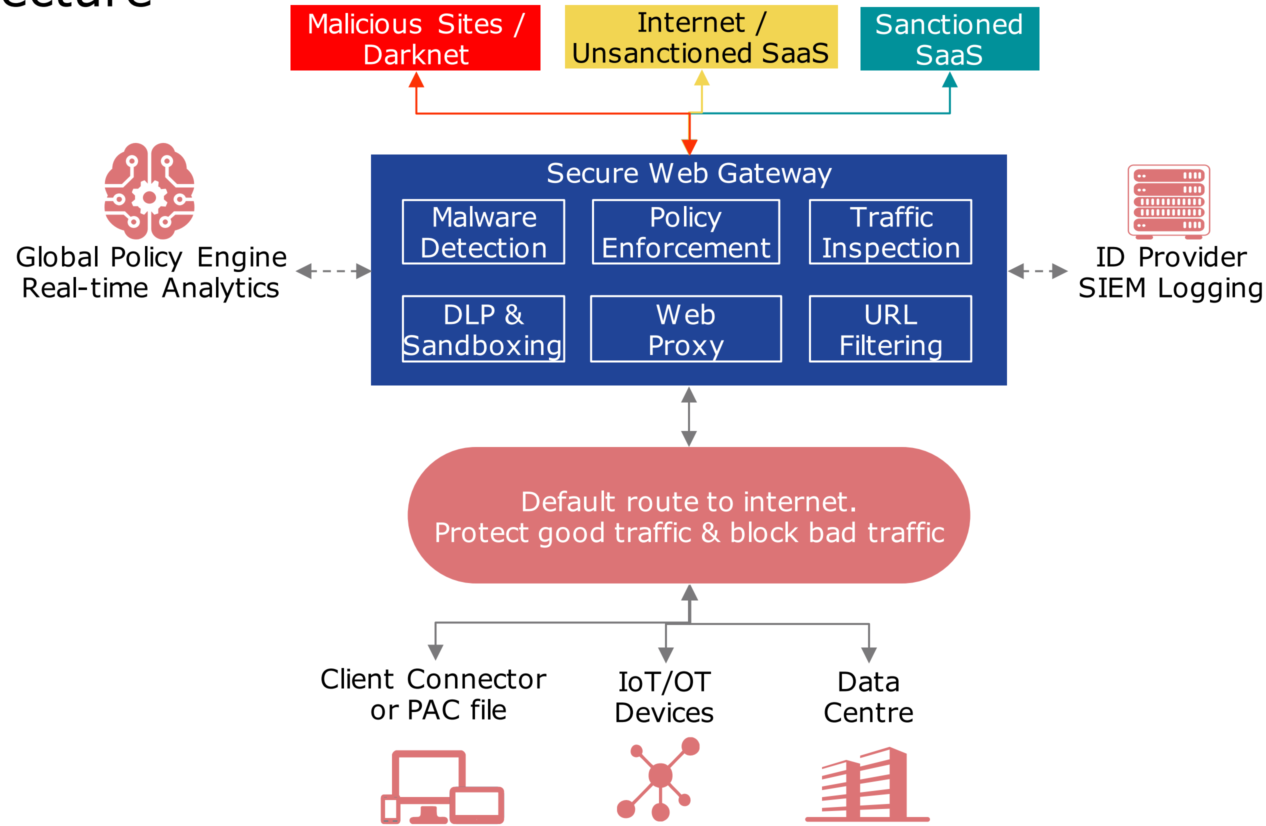
- According to Gartner, a secure web gateway must, at a minimum, include URL filtering, malicious code detection and filtering, and application controls for popular cloud applications such as Microsoft 365.

- An SWG is designed to block access to or from malicious websites and links. It enforces granular use policies and stops threats from accessing web applications by acting as a security gateway, and it does so by filtering web and internet traffic at the application level

SWG	Firewall	Proxy
SWGs operate at the application level, and they can block or allow connections or keywords according to an organization’s web use policy	Firewalls review the contents of incoming packets and compare their findings against a signature of known threats at the network level only	a proxy server filters which connections are allowed, while a gateway doesn't do any filtering A proxy server is like a wall that stops the inside of the network from being exposed to the internet

Secure Web Gateway

Architecture



Malicious Sites / Darknet

Internet / Unsanctioned SaaS

Sanctioned SaaS

Secure Web Gateway

Malware Detection

Policy Enforcement

Traffic Inspection

DLP & Sandboxing

Web Proxy

URL Filtering

Global Policy Engine
Real-time Analytics

ID Provider
SIEM Logging

Default route to internet.
Protect good traffic & block bad traffic

Client Connector or PAC file

IoT/OT Devices

Data Centre

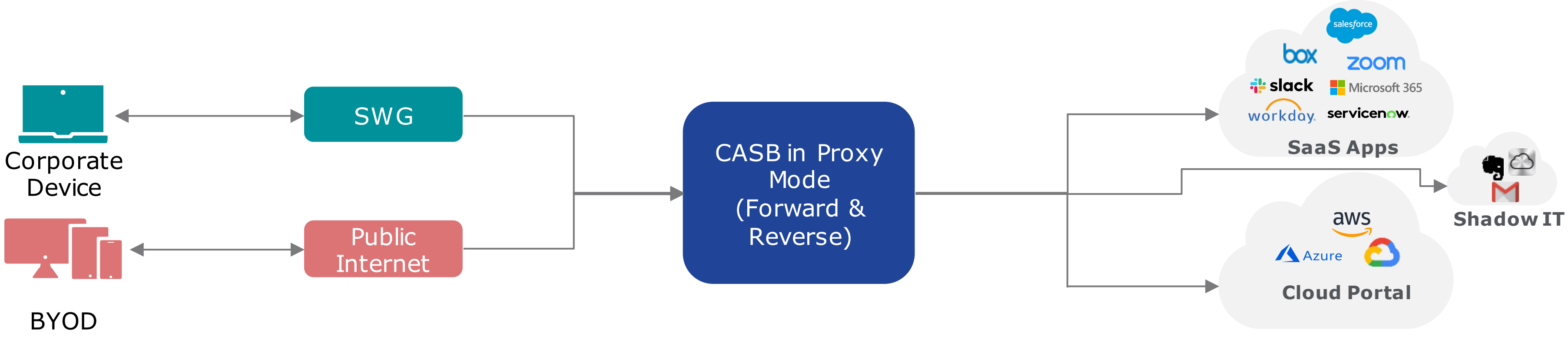
Cloud Access Security Broker

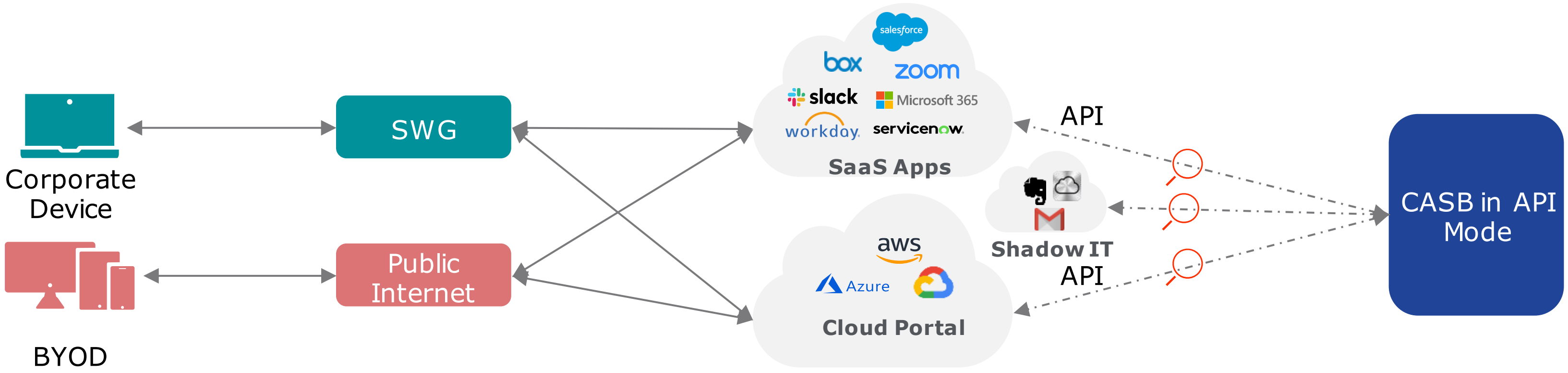
Introduction

- According to Gartner, **cloud access security brokers (CASBs)** are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed.
- CASBs consolidate multiple types of security policy enforcement. Example security policies include
  - Authentication
  - Single sign-on
  - Authorization
  - Credential mapping
  - Device profiling
  - Encryption
  - Tokenization
  - Logging & alerting
  - Malware detection/prevention
- Primarily aimed at protecting Software as a Service (SaaS) applications in the cloud
- Have limited capability to support PaaS & IaaS

Cloud Access Security Broker

Deployment Modes

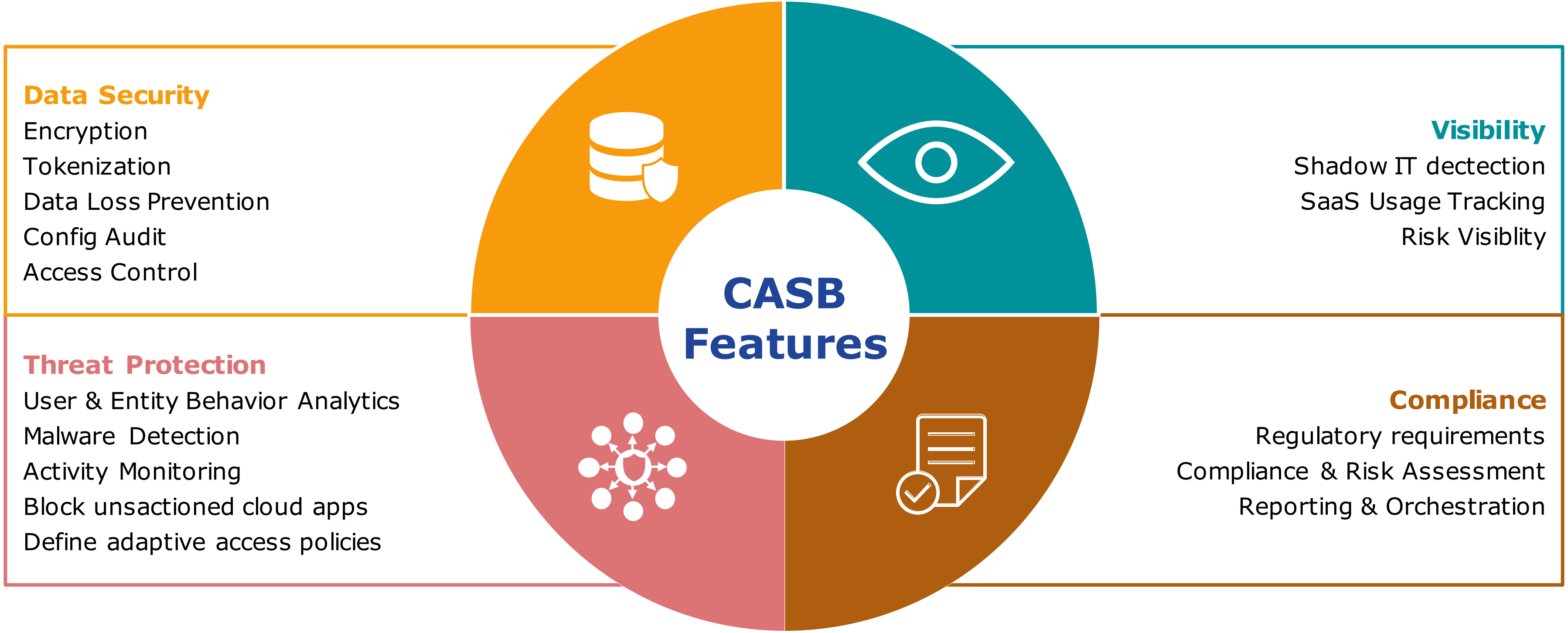




CYBER VATTAM

Cloud Access Security Broker

Features



CASB Features

Data Security
Encryption
Tokenization
Data Loss Prevention
Config Audit
Access Control

Visibility
Shadow IT dectection
SaaS Usage Tracking
Risk Visiblity

Threat Protection
User & Entity Behavior Analytics
Malware Detection
Activity Monitoring
Block unsactioned cloud apps
Define adaptive access policies

Compliance
Regulatory requirements
Compliance & Risk Assessment
Reporting & Orchestration

Cloud Access Security Broker

Use Cases

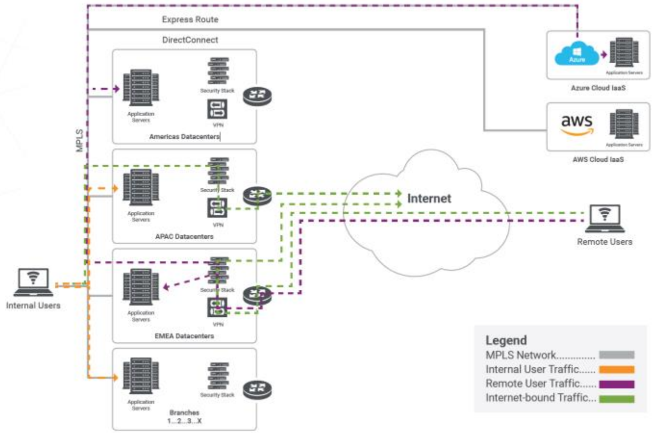
Shadow IT use Cases	
Discover cloud services in use	Regular report such as TOP 10 risky services in use
Assess cloud service risk	Continuous tuning to mark reliable services
Detect data exfiltration and proxy leakage	Detection of malware operating on the enterprise network
Applying Cloud governance policies	Automatically block selected Shadow IT cloud based on agreed criteria

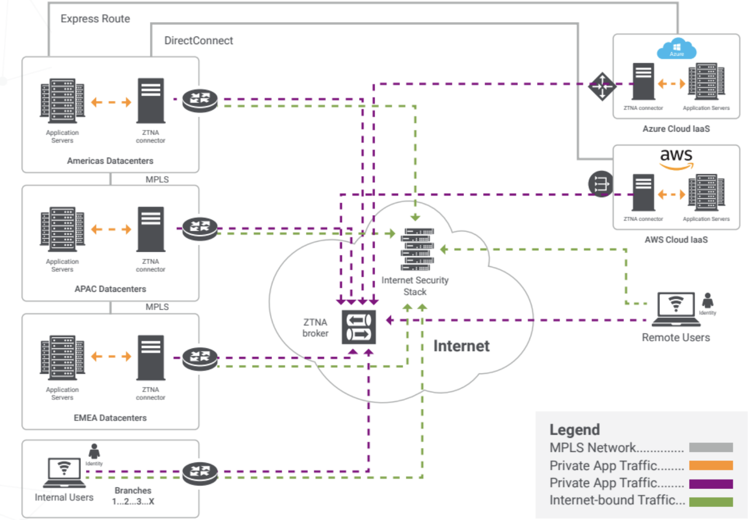
Sanctioned cloud use cases	
Forensic Investigation	Capture an audit trail of user activity
Detect threats	Compromised accounts, insiders and privileged users
Enforce collaboration policies	Data shared from cloud services
Set up the same security policies	Enforce on-premises DLP solution policies
Prevent cloud data misusage	Detect and remediate malware
Higher security for supported apps	Encrypt data stored in the cloud

Zero Trust Network Access

Introduction

- Zero trust network access (ZTNA), also known as the software-defined perimeter (SDP), is a set of technologies and functionalities that enable secure access to internal applications for remote users.
- It operates on an adaptive trust model, where trust is never implicit, and access is granted on a need-to-know, least-privileged basis defined by granular policies.
- ZTNA gives remote users seamless, secure connectivity to private applications without ever placing them on the network or exposing apps to the internet.



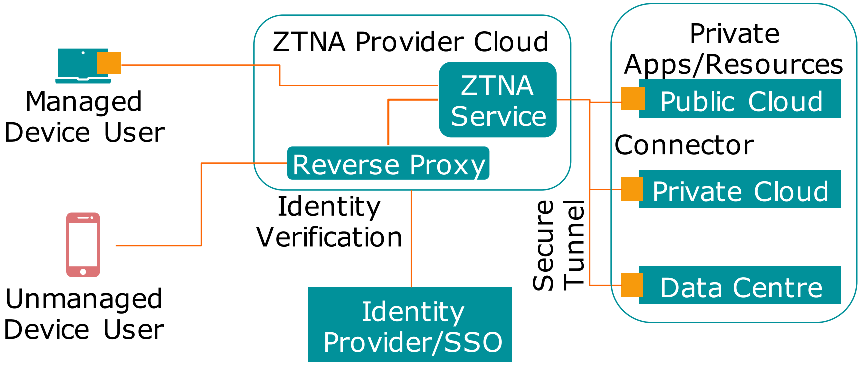


Zero trust network access

Deployment Architecture

- ZTNA completely isolates the act of providing application access from network access
  - Reduces risks to the network, such as infection by compromised devices
  - Grants access to only specific applications for authorized users who have been authenticated.
- ZTNA makes outbound-only connections
  - Ensuring both network and application infrastructure are made invisible to unauthorized users.
  - IPs are never exposed to the internet, creating a “obscured net” that makes the network impossible to find.
- ZTNA’s native app segmentation ensures that once users are authorized, application access is granted on a one-to-one basis
  - Authorized users have access only to specific applications rather than full access to the network.
  - Segmentation prevents overly permissive access as well as the risk of lateral movement of malware and other threats.
- ZTNA takes a user-to-application approach rather than a traditional network security approach.
  - The network becomes less important, and the internet becomes the new corporate network
  - Leverages end-to-end encrypted TLS micro-tunnels instead of MPLS.

ZTNA Architecture



ZTNA Use Cases

- VPN alternative
- Secure multi cloud access
- Reduce third-party risk
- Accelerate M&A integration

Cloud Identity

Introduction

What is a Cloud Identity?

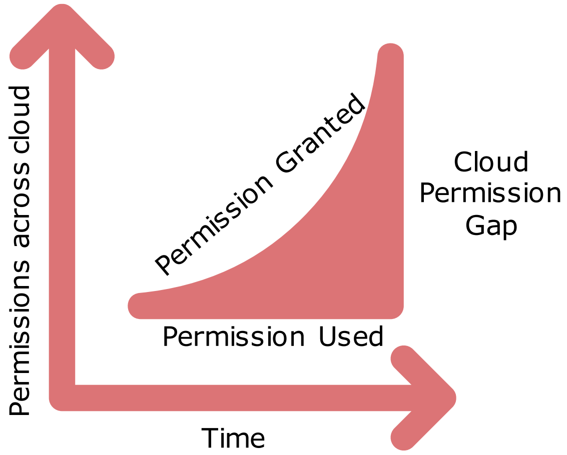
- A cloud identity is any entity with access to cloud services/cloud resources. There are two types of cloud identities:
  - Human identity - Any person accessing the cloud, e.g., users, admins, developers.
  - Non-human (service) identity - Any non-human entity that accesses the cloud on behalf of a human, e.g., connected devices, IT admin, software-defined infrastructure (SDI), artificial intelligence (AI).
- An organization can grant both cloud identity types with cloud entitlements.

- What is a Cloud Entitlement?
  - Cloud entitlements determine which tasks an identity can perform and which resources it can access across an organization’s cloud infrastructure. The main types of entitlements are cloud resources and cloud services.
    - Cloud resources, e.g., files, Virtual Machines (VMs) and servers, serverless containers.
    - Cloud services, e.g., databases, buckets and storage, applications, networking services.

Cloud Identity

Challenges

- Lack of Visibility
  - The ever-growing nature of cloud environments complicates the ability to monitor and manage identities and their access privileges effectively as security teams lose visibility of all identities on the network.
- Inconsistent Security Mechanisms
  - Organizations likely use many different cloud services to perform various business operations. Each cloud provider has unique security policies and IAM capabilities, creating security inconsistencies across the cloud environment.
  - Identifying and remediating each platform's security gaps and vulnerabilities drains significant time and resources from security teams.
- Permissions Gap
  - Organizations often assign excessive permissions to users rather than using the principle of least privilege, creating a cloud permissions gap and expose organizations to unnecessary cyber risks
  - Another common reason to the permissions gap is the presence of inactive identities (users with access to cloud resources and services they don't use)



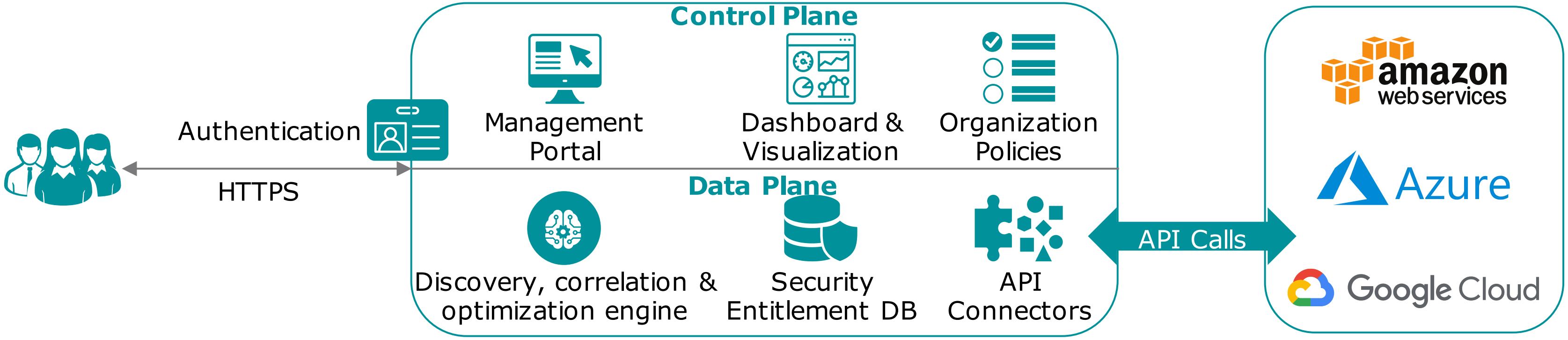
Cloud Infrastructure Entitlement Management

Introduction

- Cloud Infrastructure Entitlement Management (CIEM) is a cloud security solution used to manage identities and cloud permissions through the principle of least privilege (POLP).

- CIEM uses machine learning and analytics to detect anomalies in account permissions within multi-cloud environments. This visibility enables organizations to apply consistent identity access management (IAM) across their cloud services to mitigate cyber threats, such as data breaches and data exfiltration

- CIEM solutions are delivered through a software-as-a-service (SaaS) model, alongside other cloud security solutions, such as Cloud Security Posture Management (CSPM) and Cloud Access Service Brokers (CASBs).



Cloud Infrastructure Entitlement Management

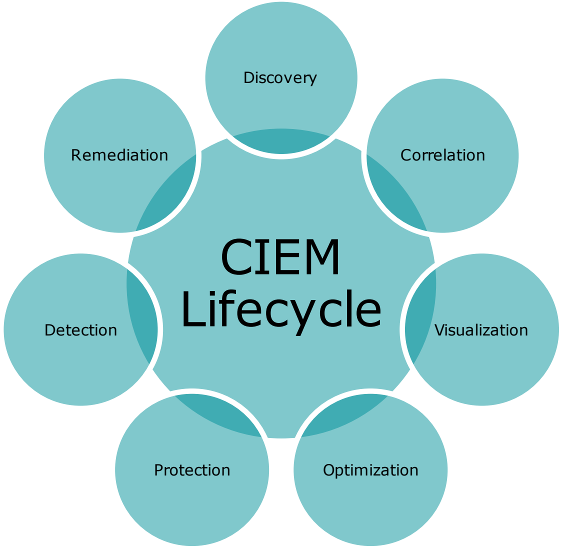
Lifecyle

- **Discovery**: Provide granular visibility of cloud identities and their entitlements, in line with cloud-based activity on a continuous basis
  - Non Human /workloads Identity (services, compute instances, data stores, secrets)
  - Cloud policies (IAM policies, resource policies, permissions boundaries, ACLs)
  - Native and federated identities (On-Prem AD, Okta, Ping)

- **Correlation**: As cloud providers uses different mechanisms and terminology to address permissions, CIEM should have ability to correlate entitlements across CSPs

- **Visualization:** Provide ability to visualize and understand the access available to a given identity in tabular or visual format, to filter and search, and to view metrics and scores that help quantify the risk
  - visualize all identities that have access to a confidential resource/data
  - all permissions assigned to a given role

- **Entitlement Optimization:** Provide ability to continuously remove excessive permissions and reduce the attack surface of cloud environment.
  - Enforces strict access control via principle of least privileges.
  - Uses advanced analytics to understand which permissions are being used, and to assess the risk level of unused permissions and ensures identities have just enough entitlements to do their job and nothing more



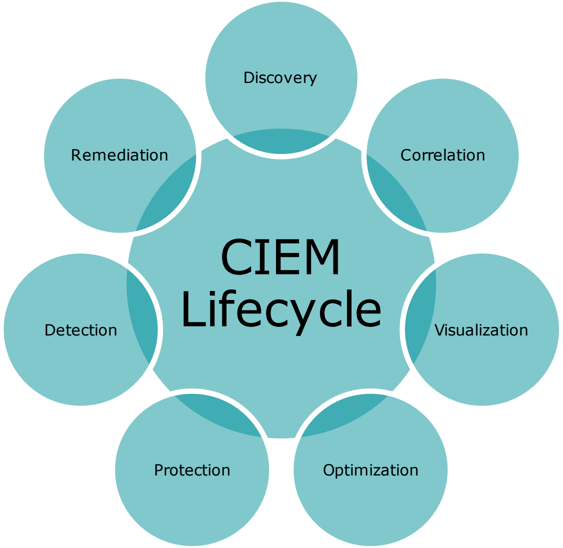
Cloud Infrastructure Entitlement Management

Lifecyle

- **Protection:** Detect when privileges are changed and alert the changes
  - Changes to entitlement/privilege could indicate a threat (e.g. privilege escalation).
  - Provide configurable rulesets that enable you to define the entitlement guardrails to be enforced.
  - Ensures IAM compliance with CIS, GDPR, SOC2, NIST, PCI DSS, ISO

- **Detection:** Provide continuous monitoring of resources and policies to detect suspicious activity
  - Indicates an external threat or an internal human error.
  - Configure rules to stream data to a SIEM or UEBA platform as per organization policy

- **Remediation:** CIEM solutions support multiple means of remediation. Organizations have different processes for managing entitlements
  - A new remediation policy can be sent directly to the cloud provider via API, or to a ticketing system or IGA system for fulfillment.
  - For DevOps teams, remediation can be handled as part of the pipeline using IaC platforms.



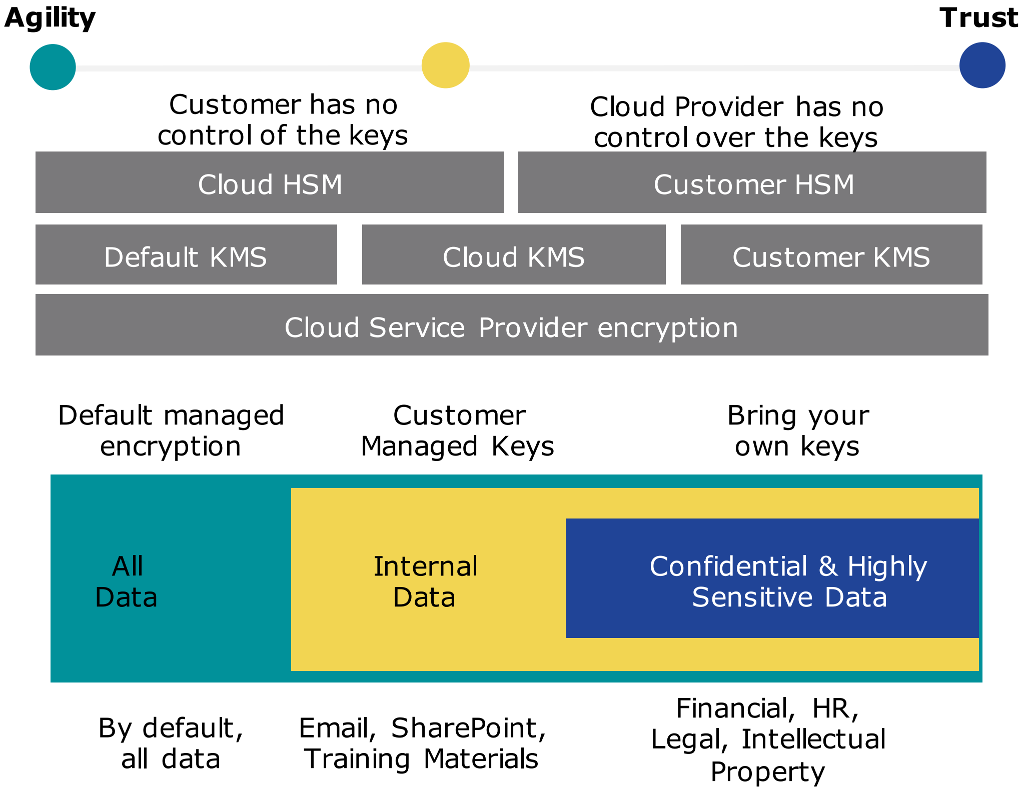
Cloud Infrastructure Entitlement Management

Benefits

- Granular Cross Cloud Visibility of cloud entitlements from a Single Dashboard
- Stronger Overall Security Posture
- Enforce principle of least privilege
- Uncover the unused permission risk
- Monitor, detect & remediate anomalies
- Empower your DevOps team with the needed speed & agility

Cloud Data Security

Encryption for Data Sovereignty in the cloud



Agility

Trust

Customer has no control of the keys

Cloud Provider has no control over the keys

Cloud HSM

Customer HSM

Default KMS

Cloud KMS

Customer KMS

Cloud Service Provider encryption

Default managed encryption

Customer Managed Keys

Bring your own keys

All Data

Internal Data

Confidential & Highly Sensitive Data

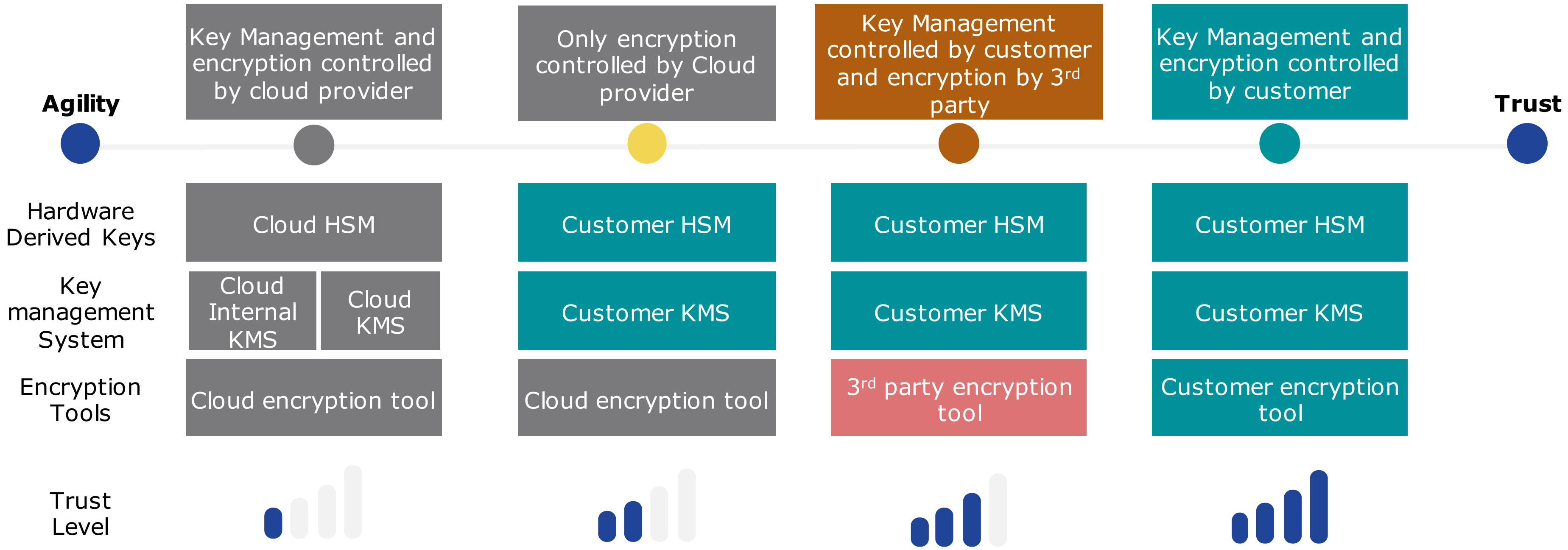
By default, all data

Email, SharePoint, Training Materials

Financial, HR, Legal, Intellectual Property

Cloud Data Security

Encryption for Data Sovereignty in the cloud



Agility → **Trust**

	Key Management and encryption controlled by cloud provider	Only encryption controlled by Cloud provider	Key Management controlled by customer and encryption by 3rd party	Key Management and encryption controlled by customer
Hardware Derived Keys	Cloud HSM	Customer HSM	Customer HSM	Customer HSM
Key management System	Cloud Internal KMS Cloud KMS	Customer KMS	Customer KMS	Customer KMS
Encryption Tools	Cloud encryption tool	Cloud encryption tool	3rd party encryption tool	Customer encryption tool
Trust Level	▮▯▯▯	▮▮▯▯	▮▮▮▯	▮▮▮▮

Public Cloud Service Providers

Native Security Controls

amazon web services

- AWS IAM & SSO
- AWS Cognito
- AWS Security Hub
- AWS Guard Duty
- AWS Inspector
- AWS Config
- AWS Cloud Trail
- AWS Cloud Watch
- AWS Macie
- AWS KMS & HSM
- AWS Firewall, WAF
- AWS Shield
- AWS Certificate Manager
- AWS Secret Manager

Azure

- Azure Active Directory
- Azure Application Gateway
- Azure Defender
- Azure DDoS Protection
- Azure HSM & Key Vault
- Azure Front Door
- Azure Information Protection
- Azure Sentinel
- Azure Security Center
- Azure VPN Gateway
- Azure WAF
- Azure Attestation
- Azure Log Analytics

Google Cloud

- Assured Workload
- Binary Authorization
- Cloud Asset Inventory
- Cloud Data Loss Prevention
- Cloud Key Management
- Confidential Computing
- Firewalls & WAF
- Secrets Manager
- Security Command Center
- Cloud Identity
- Cloud Armor
- Identity Aware Proxy
- Titan Security Key
- reCAPTCHA Enterprise

Thank you

CYBER
VATTAM

About me

Venkatesh Jambulingam
Cloud Security Expert

Email:
cybervattam@gmail.com
cybervattam@outlook.com

Follow me on