

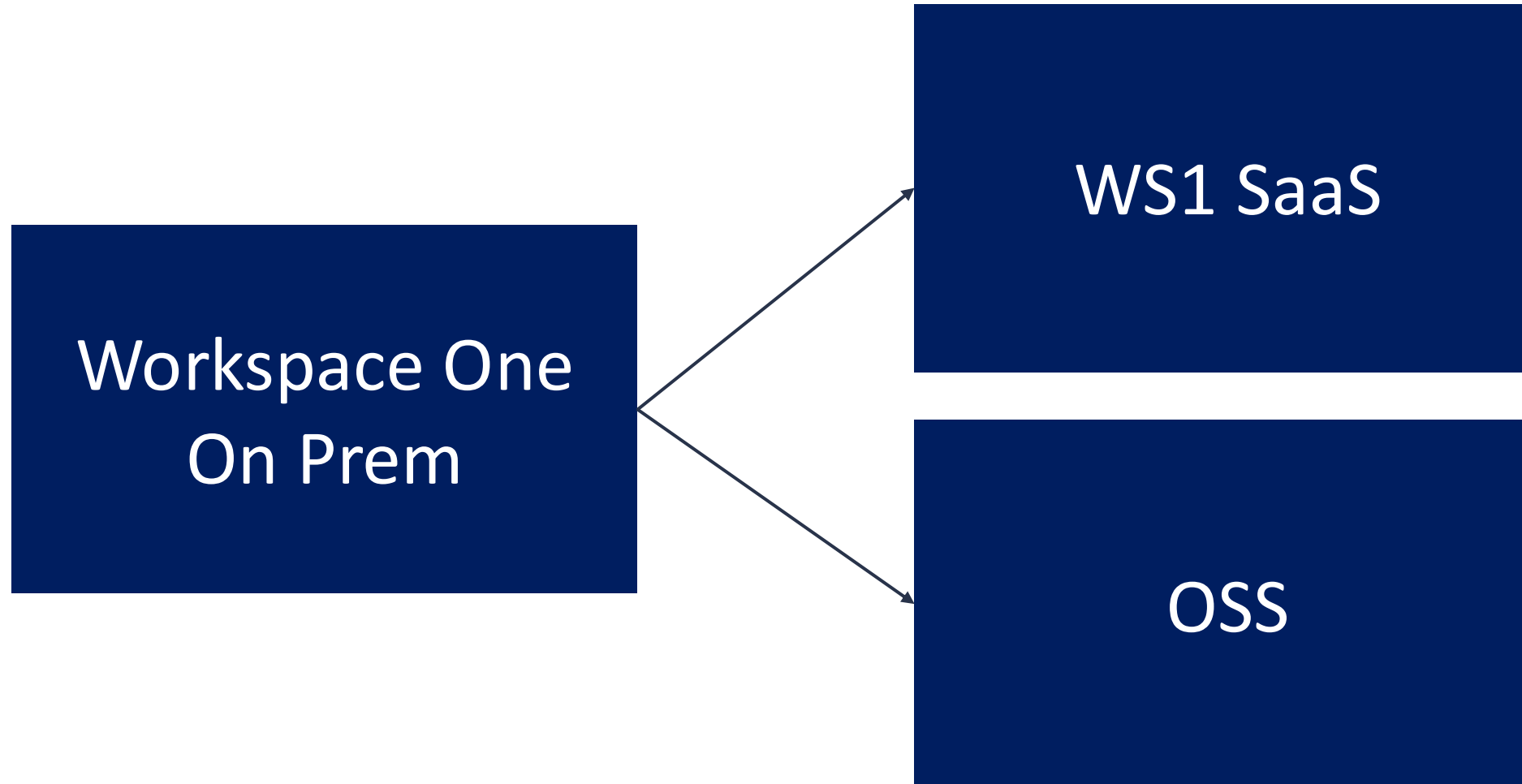


Omnissa Sovereign Solution

Dirk Daute

Director, Omnissa Partner Hosting Programs

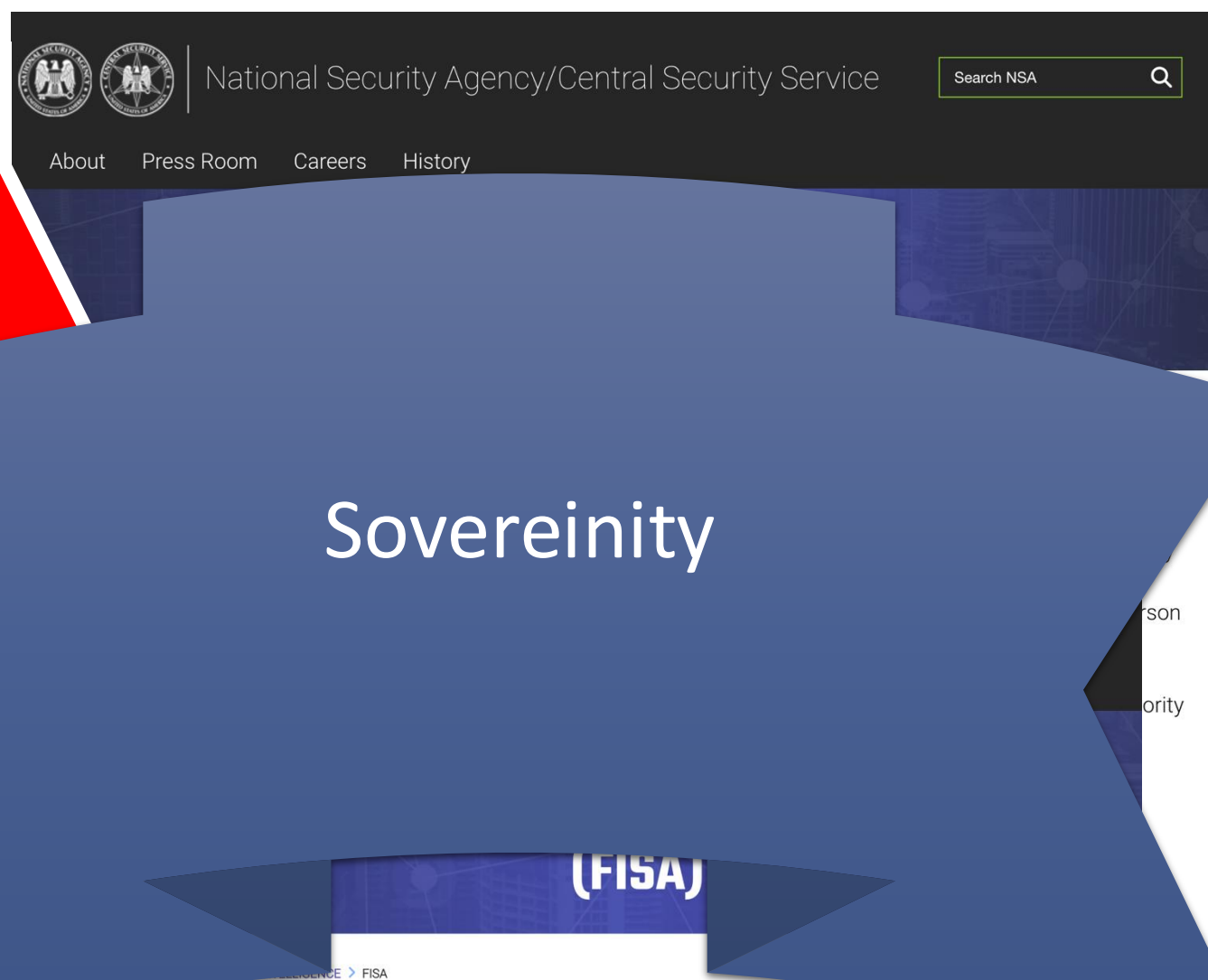
July 2026



The **Clarifying Lawful Overseas Use of Data Act** or **CLOUD Act (H.R. 4943)** is a United States [federal law](#) enacted in 2018 by the passing of the [Consolidated Appropriations Act, 2018](#), PL 115–141, Division V.

The CLOUD Act primarily allows federal law enforcement or subpoena to process data that is stored in the cloud.

STOP



The [Foreign Intelligence Surveillance Act of 1978 \(FISA\)](#) regulates certain types of foreign intelligence collection including certain collection that occurs with compelled assistance from U.S. telecommunications companies. Given the techniques that NSA must employ when conducting NSA's foreign intelligence mission, NSA quite properly relies on FISA authorizations to acquire significant foreign intelligence information and will work with the FBI and other agencies to connect the dots between foreign-based actors and their activities in the U.S. The FISA Court plays an important role in helping to ensure that signals intelligence collection governed by FISA is conducted in conformity with the requirements of the statute. All three branches of the U.S. Government have responsibilities for programs conducted under FISA, and a key role of the FISA Court is to ensure that activities conducted pursuant to FISA authorizations are consistent with the statute, as well as the U.S. Constitution, including the Fourth Amendment.

Requirements for Omnissa Sovereign Solution

Code

- No visibility or control outside specified jurisdiction
- No concentration risk
- Data end to end encryption



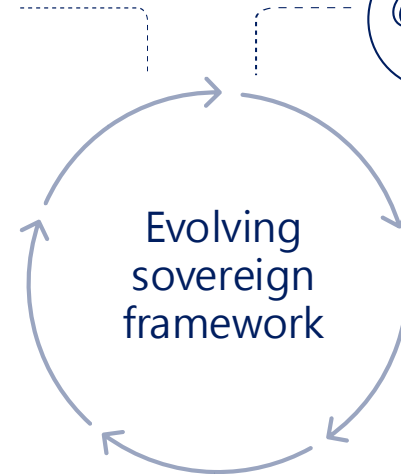
Location

- Data sovereignty & residency
- Controlled access (no internet)
- Know location (locally hosted)
- Compliant infrastructure



Access

- Strict access controls
- Certification of users
- Policy driven access & control



Management

- Managed within specified jurisdiction
- Certified partners & employees
- Audit & compliance
- Restricted value chain
- Authorized operations



What is Omnissa Sovereign Solution?

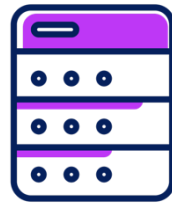
Why Omnissa Sovereign Solution ?

One deployment model doesn't work for all use cases



Sovereign (Gov/Public Sector)

Security, locality, risk, compliance, & control requirements are not addressed in a shared or cloud model



Need to host on-prem & not shared

Migration path from on-prem solutions performance, control, security or operational requirements



Location

Geographic imperative, Regulation or operational preferences may dictate where data & infrastructure are located and operated



Regulation

Regulatory compliance, security, & risk management may not be accommodated in the cloud

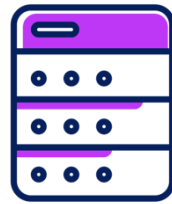
Why Omnissa Sovereign Solution Partners?

Omnissa is a software provider, not a service provider.



Sovereign (Gov/Public Sector)

Delivers Sovereign Cloud Use cases with access to Gov't procurement frameworks & regulation certification for public sectors bodies.



SaaS Cloud architecture Skills

Manages Migration path from on-prem to modern cloud service orientated architect



Location & Geographical Requirements

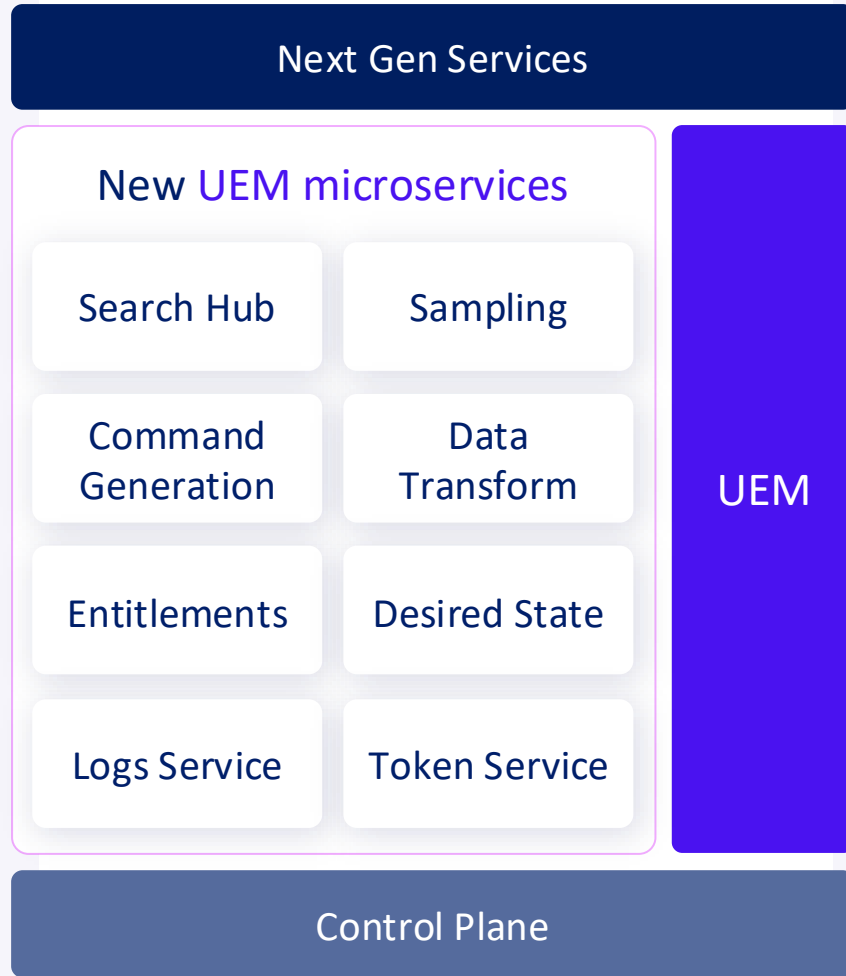
Extend Geo coverage in markets we don't have direct Omnissa capabilities in region



Regulation

Provides specific local regulatory compliance attestation, knowledge & Management

Do more with modern architecture



Speed and scale



Built for scalability



10x improved resource delivery



Support for complex workflows

For new capabilities

Apple DDM | Windows multi-user | AMAPI
Linux resource management | Windows updates
Freestyle – Mobile | Vulnerability Defense
Resource delivery and DLV improvements

Rolling out now

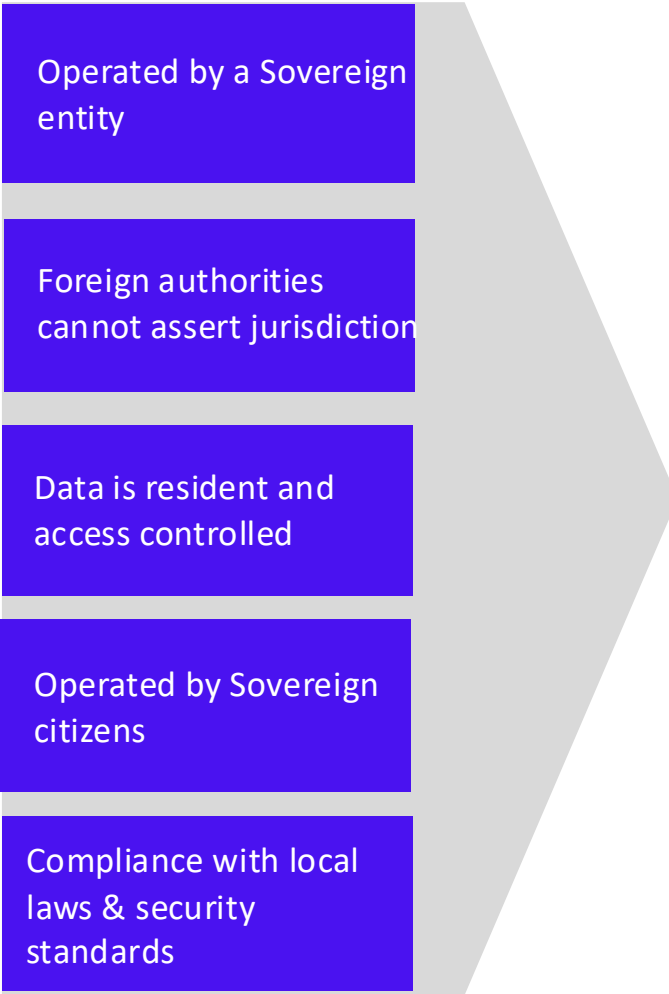
Select SaaS environments in production

Shared SaaS is enrolled now

Managed Hosted OSS environments available now

Operation Models for Omnissa Sovereign Solution

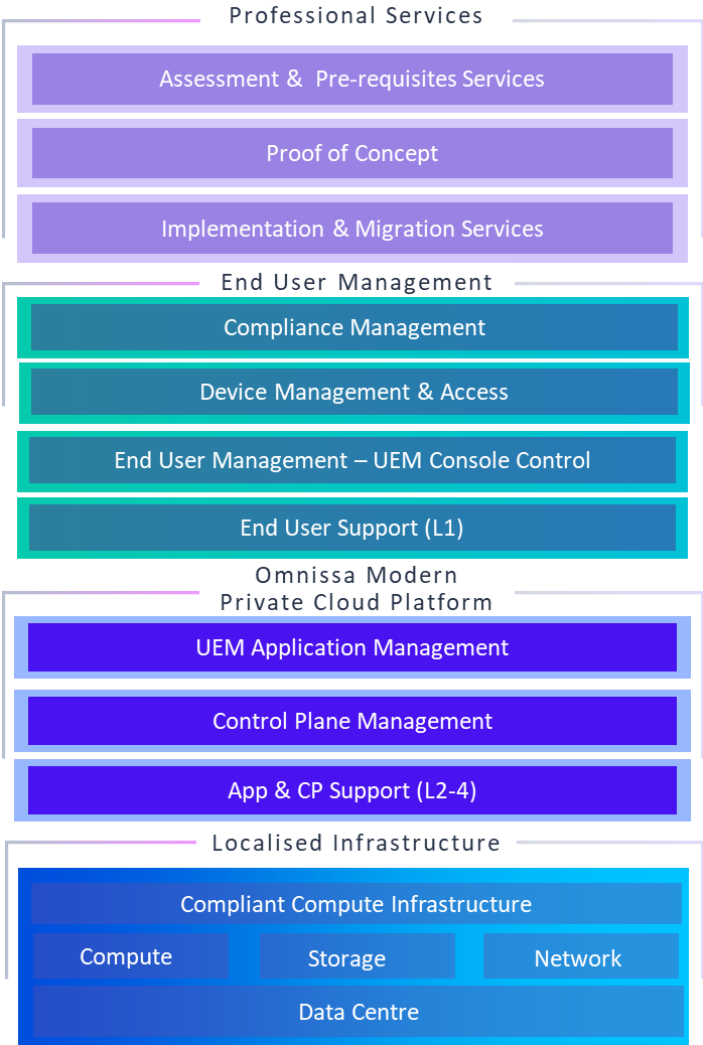
Sovereign or locally hosted UEM approach with Omnissa



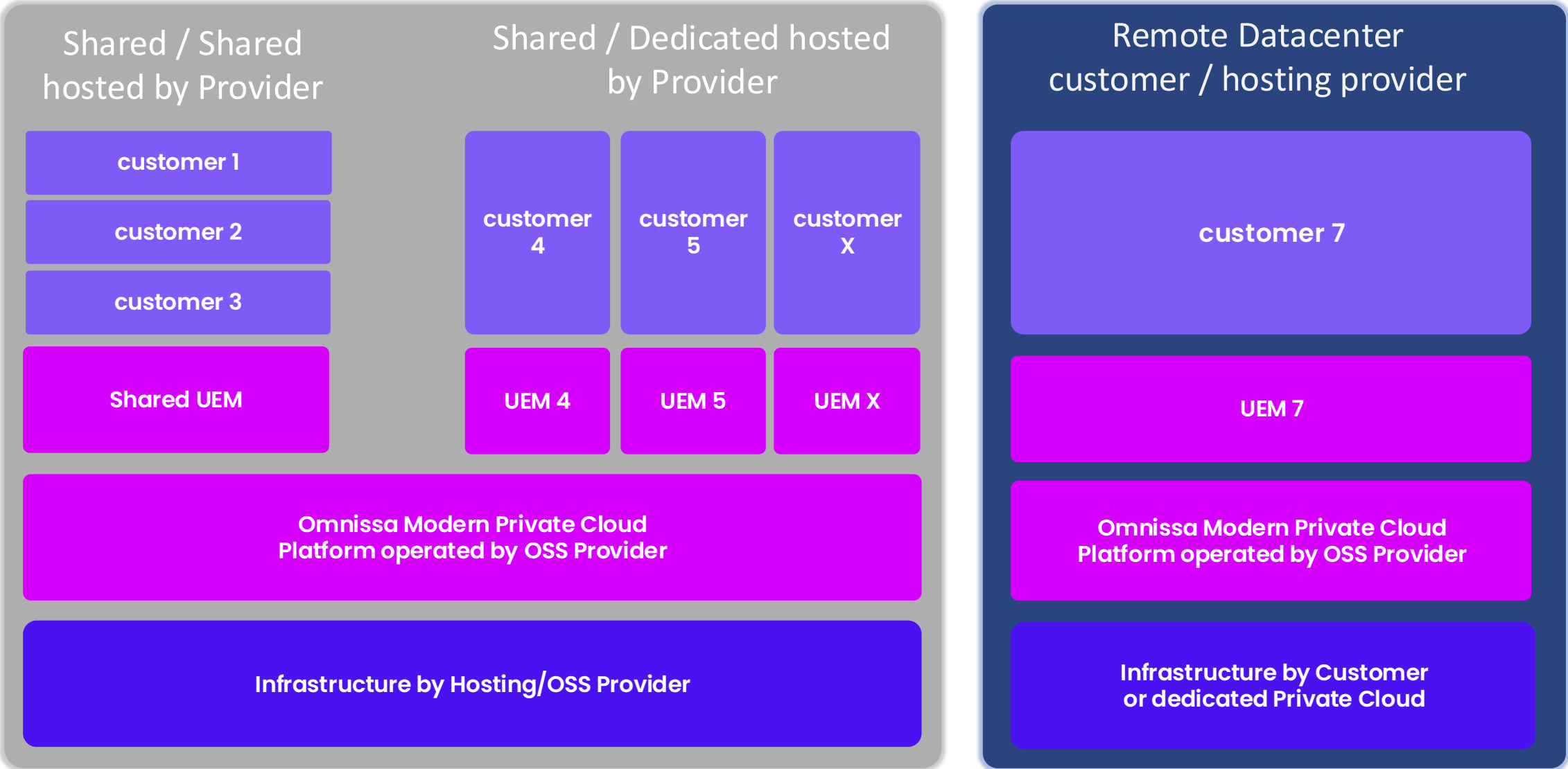
Sovereign Controls

- Data Sovereignty & Jurisdictional Controls Supported through local accredited Partners
- Data Access and Integrity delivered through WS1 Console & accredited Partner Services
- Data security & continuous compliance delivered through management of the Omnissa Platform by accredited service provider
- Compliant Infrastructure hosted locally

Omnissa Sovereign Solution



OSS Deployment Models



High level capability matrix between UEM environments

Technical availability, not licence or SKUs

Availability in Workspace ONE
UEM environment

Capability description	Product name	Legacy	SaaS	OSS
Mobile device management (MDM)	Workspace ONE UEM	Yes	Yes	Yes
Modern Desktop management (inc. Windows & Mac)	Workspace ONE UEM	Yes	Yes	Yes
Latest features: Apple DDM, AMAPI, Freestyle Orchestrator for mobile, Windows multi-user, expanded Linux mgmt., and more	Workspace ONE UEM (2406/10 & above)	No	Yes	Yes
Analytics, metrics, advanced reporting, telemetry, etc.	Omniassa Intelligence	No*	Yes	No*
Workflow & automations (UEM based only)	Omniassa Freestyle Orchestrator	No	Yes	Yes
Workflow & automations (Intelligence based only)	Omniassa Freestyle Orchestrator	No*	Yes	No*
Remote support (device control, session recording, troubleshooting)	Workspace ONE Assist	Yes	Yes	Yes
Mobile threat defense	Workspace ONE MTD	No*	Yes	No*
Secure tunnelling, secure email gateway, UAG	Workspace ONE Tunnel	Yes	Yes	Yes
Catalog application access, conditional access, self-service app store, identity federation, SSO	Omniassa Access	Yes (old)	Yes (new)	Yes (new)

* Can not be locally deployed on that platform but can be connected to SaaS instances of the product

Technical Insights for Omnissa Sovereign Solution

Main Components of OSS UEM



Control Plane Services

- Service Discovery
- Orchestration
- Secrets Mgmt
- SvctoSvc comms



Application Layer

- UEM Microservices
- Containers



Infrastructure Layer

- VM provisioning
- PhotonOS -> AlmaLinux
- Hypervisor (vSphere)



Core Services Layer

- PostgreSQL
- Kafka
- REDIS
- OpenSearch
- Observability

Modern SaaS Terms

CONTROL PLANE

the brain of a distributed system. It's the portion that directs, or "controls," how the rest of the system behaves.

OBSERVABILITY

ability to understand the internal state and behavior of the system based on the data it produces. This is crucial for ensuring performance, reliability, and rapid troubleshooting

MICROSERVICES

Microservices – Modern app services that consume the new features – they sit on the Control Plane

- Device State, Desired State, Entitlements, etc.
- Moving from UEM Windows services to containerized individual services.

CPS

Control Plane Services (Freestyle Orchestrator, Sensors, Scripts etc.)

CI/CD

Continuous Implementation / Continuous Delivery

- Frequently deliver code to customers by shrinking historic large update releases into continuous delivery pipelines complemented by additional validation gates and controls throughout the development process.

DEPLOYMENT RING

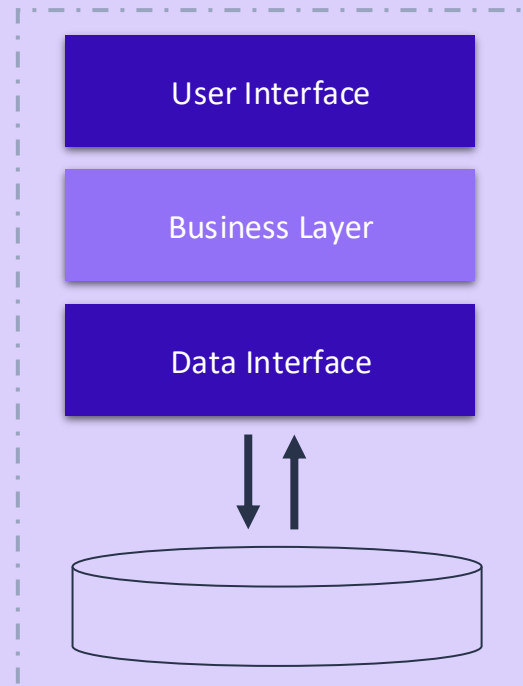
Deployment Ring – When a customer receives software updates through the CI/CD pipeline

OSS – the best of modern Software Architecture

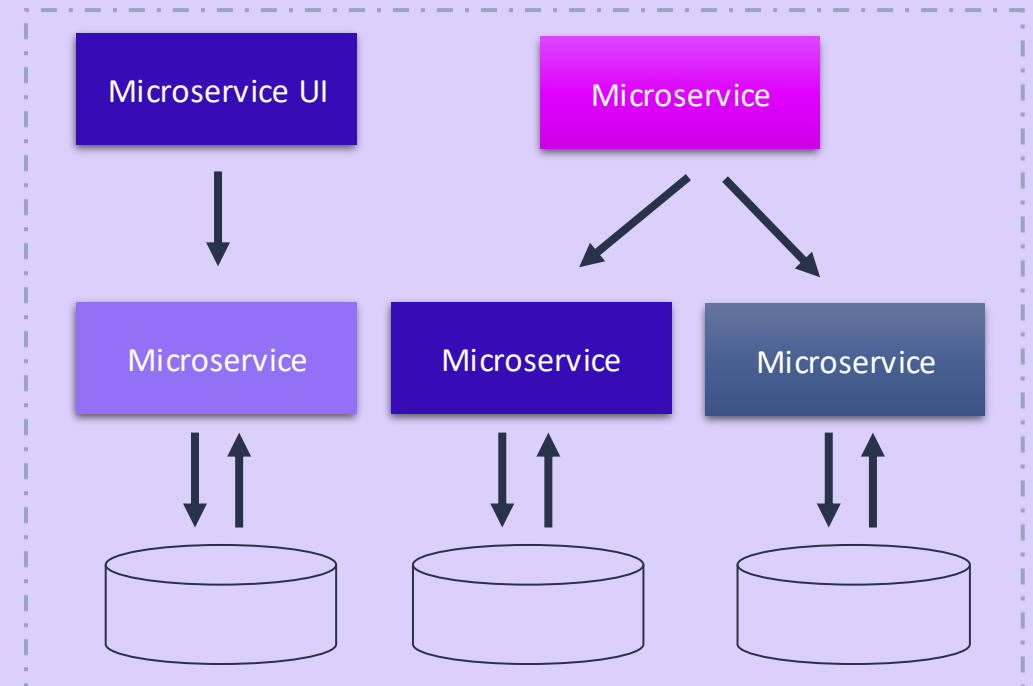
Legacy UEM vs Modern SaaS Architecture with OSS

- Monolith Architecture
 - Slower Dev Speed
 - Scalability Issues
 - Reliability
 - Lack of Flexibility
 - Deployment Issues
- Microservices Architecture
 - Agility
 - Flexible Scaling
 - Continuous Deployment
 - High Reliability
 - Independently Deployable

Monolithic Architecture
Legacy UEM



Microservices
Modern SaaS Architecture



Infrastructure & Hosting Services

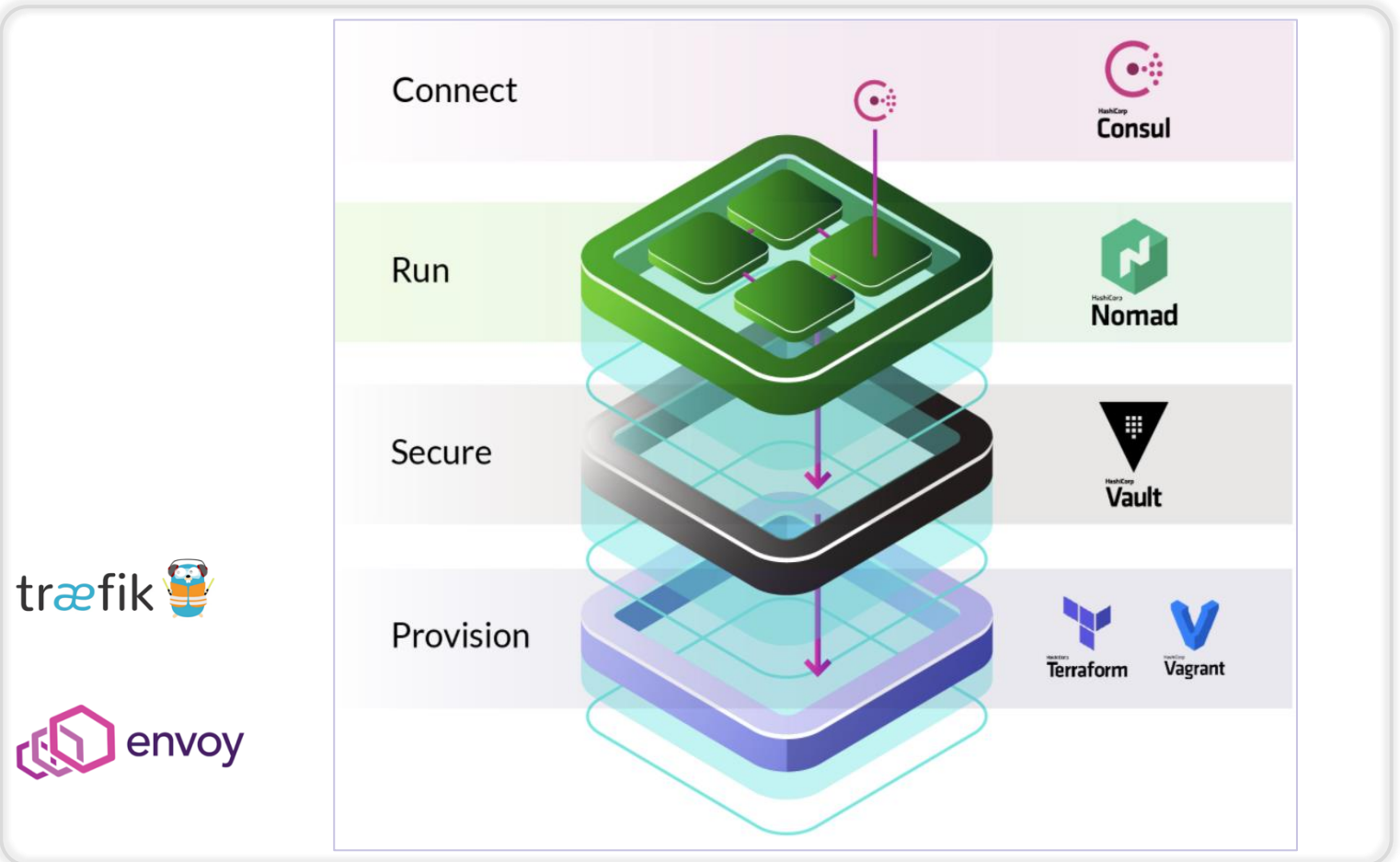
These services and infrastructure are required to operate both the modern and legacy stack. They are to be provided by the customer/MPC Partner, including the necessary licenses:

- vSphere Hypervisor
- NFS compatible FileServices (backup)
- CIFS Fileshare (Apps, Product Files)
- S3 Storage (native or MinIO)
- Database: MSSQL (UEM)
- Windows Server
- Compute on ESX: CPU, RAM, File-storage for VMs
- Firewall, DDoS
- Internet Connectivity
- Public Website Certificates
- Backup/Restore Capabilities



Control Plane: Tools & Technologies

- Using HashiCorp Native Stack
 - Consul
 - Service Discovery
 - Key: Value Storage
 - Service to Service Security
- Vault
 - Secrets Management
- Nomad
 - Orchestration
- Traefik
 - Client Side Load Balancing
- Envoy
 - Ingress Gateway (UEM -> Control Plane comms)



Core Services: Tools and Technologies

Licences will be provided as part of Omnissa and Offshoretech / GEMA costings

- Kafka
- REDIS
- OpenSearch
- Docker
- Alma Linux
- Kemp Load-balancer
- Observability based on Grafana
 - Log
 - Telemetry
- Database: Postgres





omnissa™

Thank you

BSI Updates & Roadmap

GEMA hosted (Germany or Austria)

- Data center and infrastructure operations

- Data center

- Tier 3+ data centers in Germany, Tier 3 data centers in Austria
- Certifications
 - EN 50600 (Building E, F/G, H)
 - ISO 9001
 - ISO 50001
 - ISO 27001 IT-GS (BSI)
 - ISAE 3402 Type II
 - PCI DSS
- 24/7 emergency service
- Redundant main and backup power systems
- Secured premises with multiple surveillance systems

- Operations

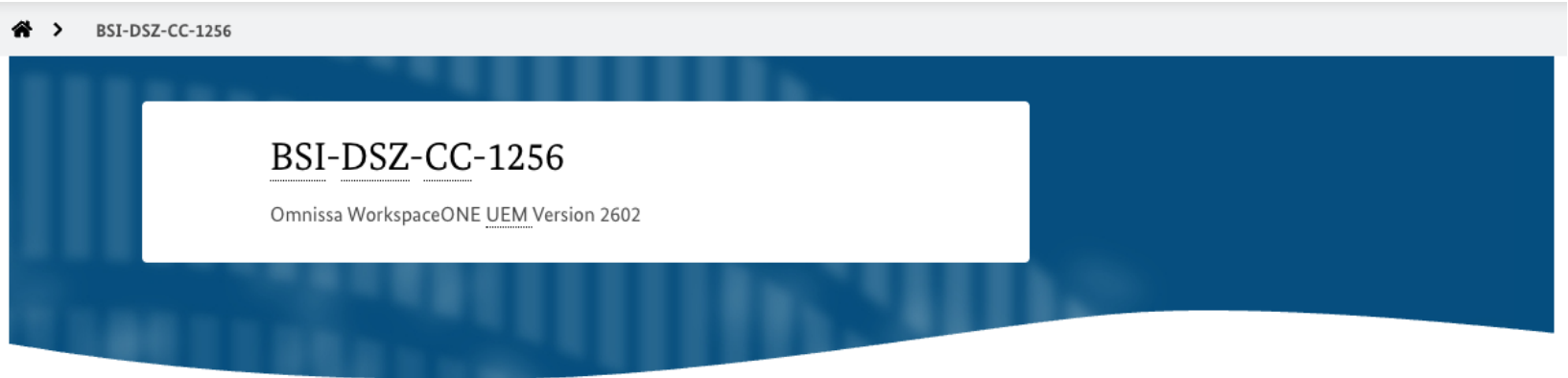
- German cloud operator
- Certifications
 - C5 (BSI)
 - ISO 27001
 - ISO 9001
- Encrypted data connections
- Immutable backup
 - SEC 17a-4(f)
 - CFTC Rule 1.31b
 - FDA 21 CFR Part 11
 - Sarbanes-Oxley Act
 - IRS 98025 and 97-22
 - ISO Standard 15489-1
 - MoReq2010



- Critical updates within 24hours
- Service Level Agreement 99,9% uptime
- Access rights management based on need-to-know principle, with dual control for critical systems
- Contractual agreements for secure data deletion after contract termination
- Regular security assessments
- Real-time environment monitoring

Status BSI EAL4+ Zertifizierung

Zertifizierung geplant bis zum 30.06.2026 abzuschließen, Änderungen vorbehalten



Antragsteller / Applicant	Omnissa LLC 590 E. Middlefield Road Mountain View, CA 94043 USA
Prüfstelle / Evaluation Facility	TÜV Informationstechnik GmbH
Prüftiefe / Assurance	EAL4, ALC_FLR.3

Zusatzinformation: Produkt befindet sich in Evaluierung / Additional information: Product in evaluation

[Link BSI Homepage](#)

Backup

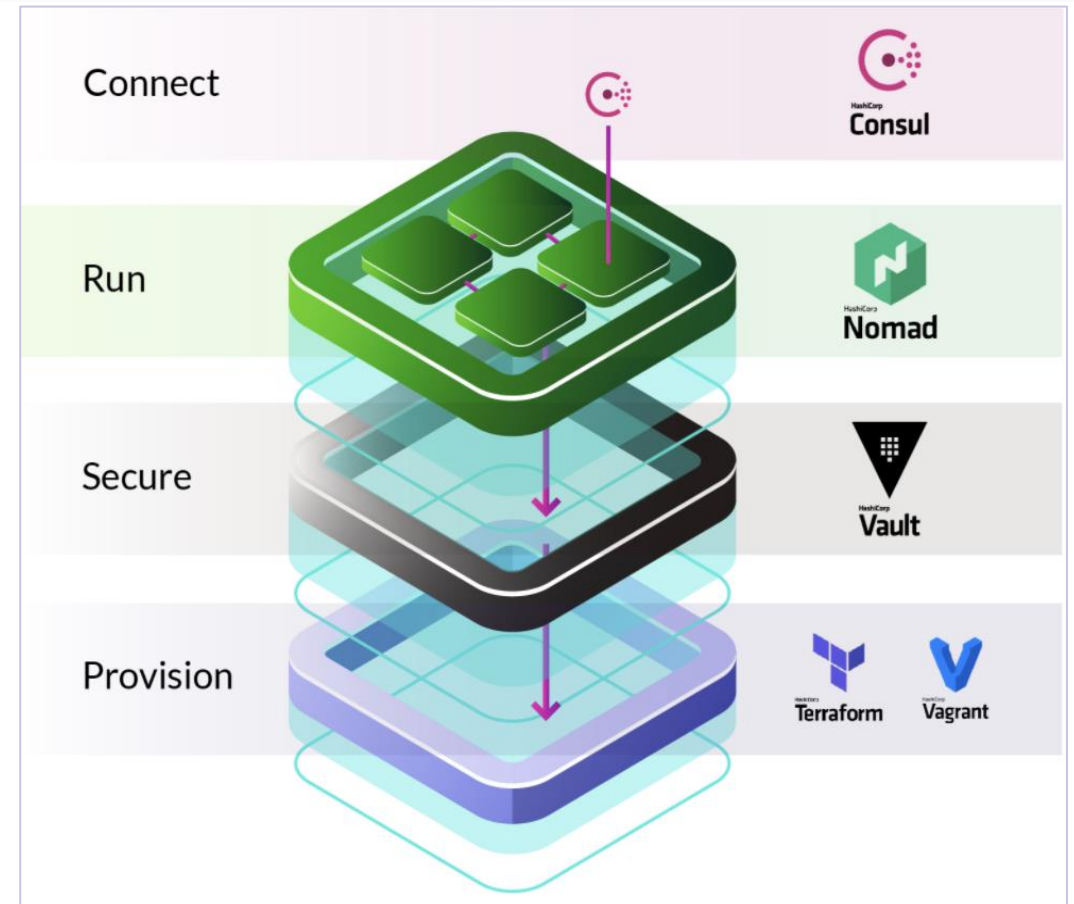
Omniassa Sovereign Solution RACI

Components of the service	Omniassa	Partner	Service Provider
Professional Services Consultancy, Implementation to end customer		✓	
Customer Support Configuration, Order Management, Monitoring, Incident, Problem & change Management		✓	
Workspace ONE License (Supply & Feature Development)	✓	✓	✓
Workspace ONE UEM Console for the Partner Environment and end customer OG set up		✓	
Application Services Software (UEM) Management & L3 Support			✓
Control Plane Software Management & L3 Support			✓
Security Services Information Security			✓
Network Security			✓
Security monitoring			✓
Patching & Vulnerability Management			✓
Partner & Service onboarding, Blueprint (Solution & Service) Knowledge transfer			✓
Platform Infrastructure Operating System, Database, ESX (software)		✓	✓
Local Physical Infrastructure Data centre, Network & Hardware		✓	✓

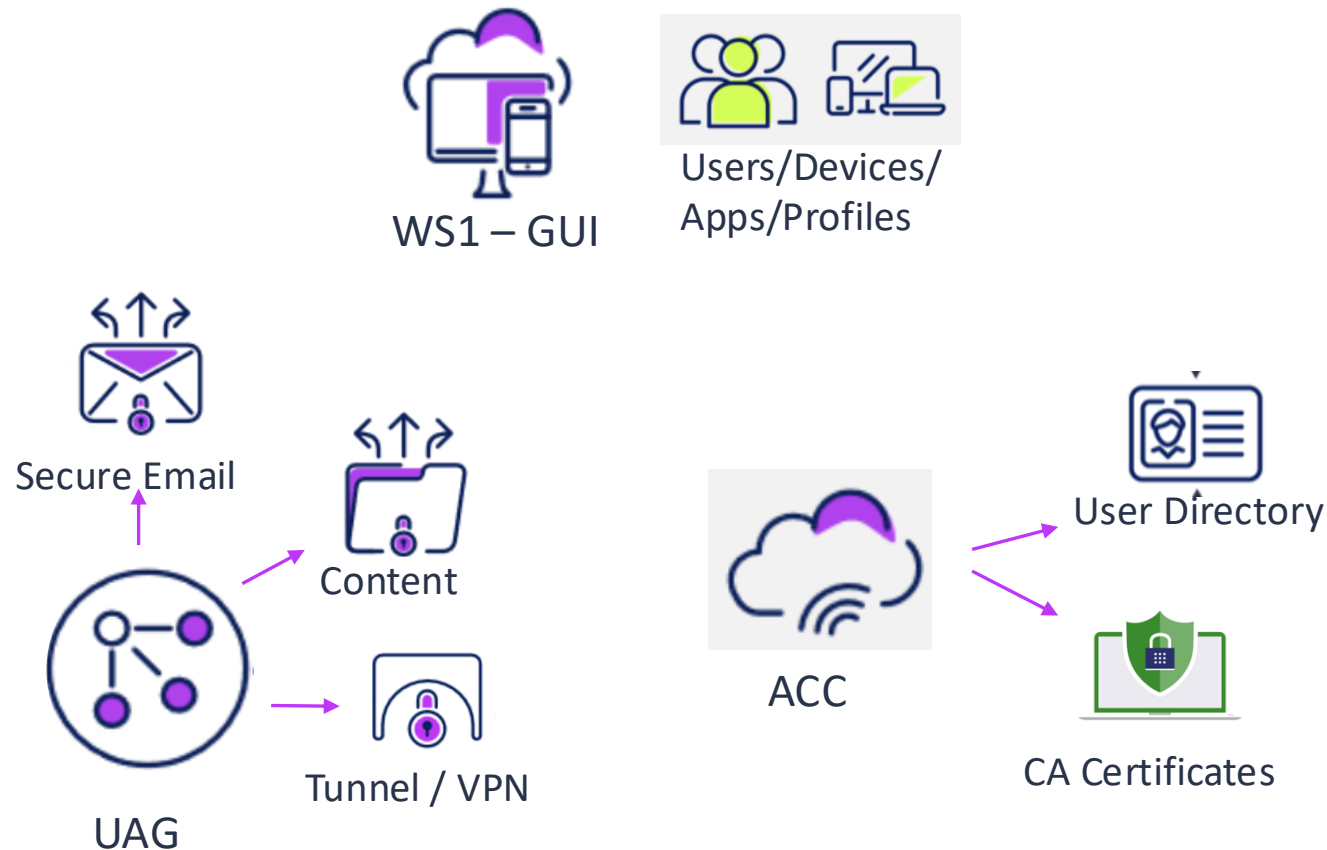
Control Plane: Tools & Technologies



- Using HashiCorp Native Stack
 - Consul
 - Service Discovery
 - Key: Value Storage
 - Service to Service Security
- Vault
 - Secrets Management
- Nomad
 - Orchestration
- Traefik
 - Client Side Load Balancing
- Envoy
 - Ingress Gateway (UEM -> Control Plane comms)



UEM Components to be managed by customer or chosen partner



All UEM Components that can be managed from the WS1 GUI are being managed solely by the customer or its chosen partner:

- **WS1 GUI**
 - Users/Administrators/Distribution Groups
 - Apps
 - Products
 - Profiles
 - Compliance
 - Orchestration
 - Settings
- **ACC**
 - Directory Connection
 - User/Device Certificates
- **Unified Access Gateway (UAG)**
 - Content Gateway / File Access
 - Tunnel/VPN / Internal Web Site Access
 - Secure Email Gateway

SLAs

Reaction Times

GEMA provides an admin to admin helpdesk where tickets can be opened via email, 24/7 telephone hotline (calls may be answered in English – call back will be done by German based German speaking engineers) or system alarm.

Problem/Alarm	Priority	Reaction Time	Escalation Threshold
Service not available / System down (all Users and Features are affected and not functional)	1	Within 1 hour	2 hours
Significant degradation of Services (a large Group of Users, a full tenant and business critical Features are affected)	2	Within 4 hours	8 hours
Limited degradation of Services (a small number of Users or Features are affected and normal operations can commence)	3	Within 24 hours	48 hours
Minimal degradation of Services (normal operations are commencing as expected, single users are affected)	4	Within 48 hours	96 hours

Updates / Upgrades

Responsibilities and announcements

System	Priority	Information	Responsible	Execution Time
CP Layer - services	standard	7 days in advance	GEMA	Maintenance window
	critical	4 hours in advance	GEMA	Emergency Maintenance Window
CP layer – Alma Linux	standard	7 days in advance	GEMA	Maintenance window
	critical	4 hours in advance	GEMA	Emergency Maintenance Window
UEM Application Lay Servers including Windows Server Patches	standard	7 days in advance	GEMA	Maintenance window
	critical	4 hours in advance	GEMA	Emergency Maintenance Window
MS SQL Server including underlying Windows Server	standard	7 days in advance	Customer	Maintenance window
	critical	4 hours in advance	Customer	Emergency Maintenance Window
Observability Stack (no patches should require any downtime in CP layer)	standard	n.a. – will be agreed upon	GEMA	Standard operation hours
	critical	n.a. – will be agreed upon	GEMA	Standard operation hours
UEM load balancers	standard	7 days in advance	GEMA	Maintenance window
	critical	4 hours in advance	GEMA	Emergency Maintenance Window
ESX / vSphere / Networking / Storage	standard	7 days in advance	Customer	Maintenance window
	critical	4 hours in advance	Customer	Emergency Maintenance Window

DR – Design

Manual Service Restore

Service Repair First – same data center

Each Stack and service in itself is fully high available. Emergency measures to bring the service up again are:

1. **Increase Assignments:** Within CP layer there are pre-determined resource assignments, which under normal circumstances guarantee sufficient performance. In order to accommodate for short term performance issues, manual additional assignments can be created. This will provide time for a root cause analysis.
2. **Increase Cluster Sizing:** The current cluster configuration is based on the “xx-small” size layout allowing for up to 50.000 devices depending on usage scopes and device types. If that sizing is not appropriate anymore cluster sizing can be increased to “medium”.
3. **Scale UEM components:** Especially the Api service of the UEM Application servers is utilized heavily by the modern stack. Many degradations in service quality can be traced to API related bottlenecks. Scaling of the components until the root cause for the problem has been identified is recommended.
4. **Replacement of nodes:** If any node in the CP or UEM Application layer proves troublesome it can be removed and replaced within normal operations and without impacting the enrolled devices.

Restore to avoid reenrolment

The need to fully recreate the environment should not occur unless because of full data center outages or similar:

1. **Recreation from backup:** If backup of the MS SQL databases and the backup of the CP layer (NFS filesystem based) are accessible, the entire system can be brought up from scratch.

The restore time depends both on the size of the deployment and the type of backup available (especially UEM App Server backups - i.e. full machine restore vs. new installation and MS SQL DB restore).

In case of having to move the installation to a new data center the necessary backups need to be accessible:

1. **System installation:** Manually install the system from scratch.
2. **Replay of DB restores:** After both MS SQL and Postgres data has been restored, Opensearch Snapshots will be replayed.
3. **Global DNS shift (if change of data center is required):**
Access to new installation will be enabled

Responsibilities

	OSS Platform	
	GEMA	Customer
Task/Work Stream/Role	Owner	Owner
Installation, Base configuration of vSphere environment		X
vSphere environment patching	Inform	X
Firewall + Network		X
Troubleshooting of Infrastructure or vSphere environment	Inform	X
Installation and base configuration of OSS platform components	X	
Monitoring and Update of OSS platform components	X	Inform
Certificates for OSS components	Inform	X
Featureset and Feature changes of OSS	X	Inform
OSS Performance Monitoring	X	Inform*
OSS Troubleshooting	X	Assist**
Inbound Problems from customers/tenants	Assist	X
Changes to OSS Infrastructure	X	Approve
Licenses – Workspace One (Per Device)		X
Licenses – Microsoft Windows, Firewall, MS SQL		X
Licenses – Alma Linux Extended Security Patches, Grafana, Kemp Load balancer, Redhat	X	
Standard maintenance tasks OSS layer	X	Inform
Standard maintenance tasks Infrastructure layer + MS SQL Servers	Inform	X
OSS Service Reporting - monthly	X	
OSS Service Improvement Meetings – yearly	X	Assist
End-User Helpdesk		X
Admin to Admin support for platform related issues (Lvl2, Lvl3)	X	Inform
Escalation to Omnissa + root cause analysis support	X	Inform
Providing and Granting remote Access to GEMA		X
Extended management of OSS virtual machines (creation, changes, boot, ...)	X	Inform

* Where necessary

** Where backend infrastructure services are involved

*** FI will be provided a frontend for tenant creation

PoC Success

Exit Criteria

- Devices can be registered
- Orchestration is working
- Security / Compliance settings become active
- Apps are being installed and secured
- Certificate distribution and revocation to devices works seamlessly
- WiFi access based on UEM distributed certificates has been achieved
- Administrative separation (RBAC) works as determined in workshop
- Secure Access to Web Sites is available
- iOS Updates can be forced
- Patchmanagement for Clients by GEMA
- Apple DDM profiles can be applied
- Maintenance Access works as designed
- Backup/Restore have been verified
- Grafana shows metrics and logs
- System Update has been successfully performed remotely (CP, UAG, OS)
- Secure Access to File Shares is available

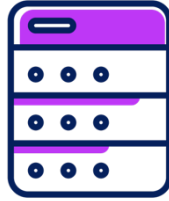
PoC Tech Preview

Phases



Discovery

- Detailed Requirements Document
- Workshop
 - System Design
 - Support Design
 - Entry & Exit Criteria Definition
 - Brownfield Migration
 - Remote Access
- Initial Documentation



Implementation

- Inspection of provided Infrastructure
- Creation of Repositories, Templates and VMs
- Observability Stack
- UEM System Setup
- CP Layer Installation
- UEM + CP Layer connection + ModStack
- Feature Enablement
- Backup/Restore preparation



Initial Setup

- Setup of UEM Functions (by customer)
- Feature Verification
- Enablement of UEM addons (UAG, ACC – by customer)
- Directory Connection Enablement (by customer)
- Content Locker Enablement (by customer)



Testing

- Device functionality verification (by customer)
- Support (Lvl2, Lvl3, Lvl4 – with Omnisssa)
- Updates/Upgrades
 - Zero Downtime
 - Full Update
 - UEM Update
 - OS Update
- Restore Test
- Verification of Exit Criteria

PoC Tech Preview Parameters / Limitations

Price Indication

Basic Parameters	Limitation	Time Frame	Pricing
• Very small environment for tech and service verification • Brownfield Pre Verification Only • Admin Lvl2, Lvl3 + Lvl4 Support 10/5 • 1 full week onsite for implementation • Repositories, Automation and Templates can be kept for production environment • Bi-Weekly Updates • 1 Full Upgrade • Enhanced Support during PoC	• Up to 100 devices • No High Availability • Grafana Free Edition -> limited Alarms • NO Feature limitations • Devices need to be enrolled into new OSS environment (no migration)	• Workshop Preparation, Execution, Result Summary -> 1 week • Implementation • 2-3 week preparation by PTLs • 1 full week of on site implementation • Documentation • 8 weeks of PoC Execution (testing by PTLs) • PoC Exit Meeting on site	• Paid PoC with GEMA • Plus travel expenses

Device state management

The next phase of the evolution of device management



UEM

Unified Endpoint Management

Mobile and desktop management, security, analytics, automation, orchestration, and more

MDM

Mobile Device Management



Basic mobile device management and some app controls

EMM

Enterprise Mobility Management



MDM + granular app control, advanced security policies, and access controls

DSM

Desired State Management

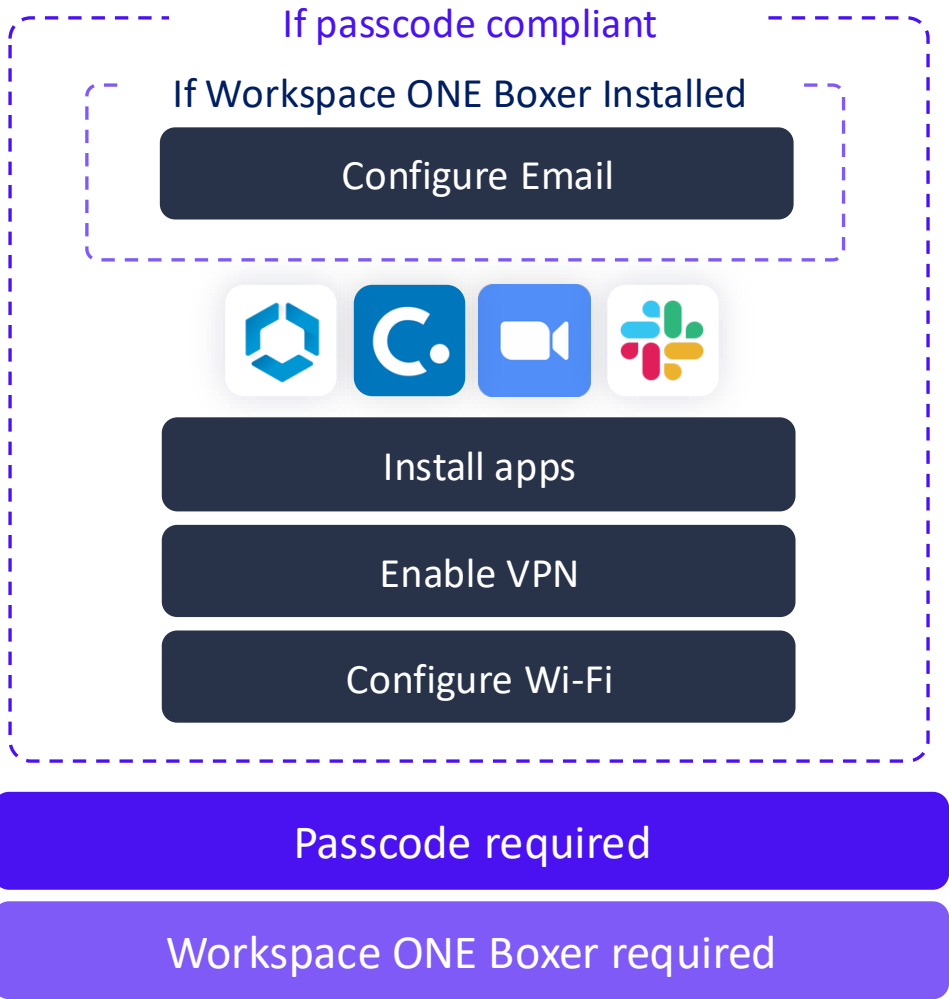


Tie specific policies to specific attributes, making devices more autonomous during their lifecycle

Apple declarative device management for iOS & macOS



Modern architecture’s **self-healing** capabilities work alongside Apple protocol to ensure desired state of the device, **including software update enforcement**.



Features Enabled With The WS1 OSS Architecture

Apple

Declarative Device Management



Resource Delivery & Device List View Improvements



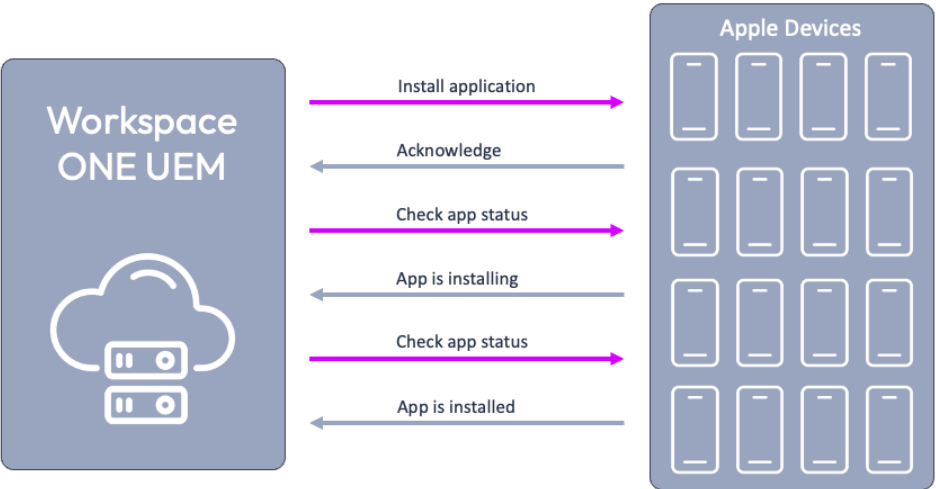
Eins der neuen Apple DDM Features

Software Update Enforcement	iOS, iPadOS, macOS	Forces a device to update to a specified OS version at a specific date & time.
-----------------------------	--------------------	--

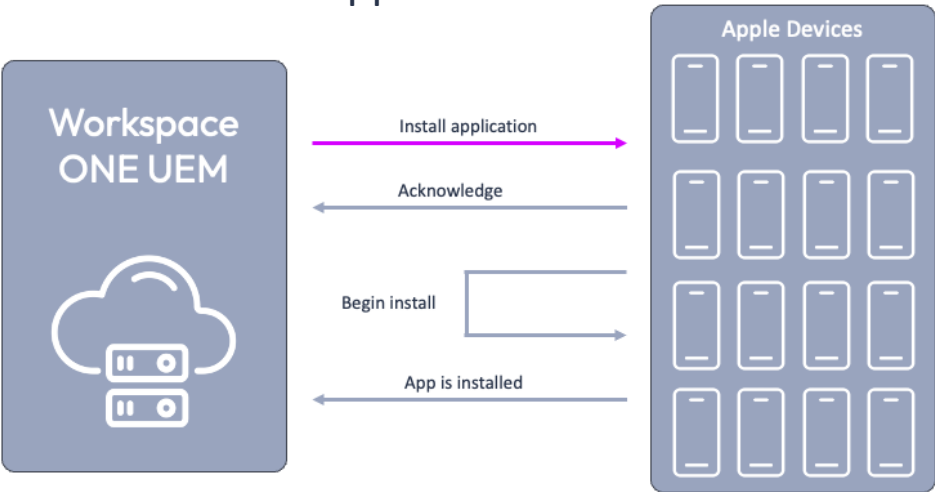
Freestyle - Mobile



Ohne Apple DDM



Mit Apple DDM



Android Management API (AMAPI)

A new approach to Android Enterprise for desired state management



Native

Part of the Android DNA – updated and maintained by Google

Simple

Workspace ONE writes policies and AMAPI applies them

Powerful

Industry-standard common stack with built-in best practices

AMAPI roadmap across Android management modes

Work Profile

GA

COPE

GA

Fully Managed

Roadmap

Features Enabled With The WS1 OSS Architecture

Resource Delivery &
Device List View
Improvements



Freestyle - Mobile



Apple

Declarative Device
Management



Current on prem Architecture
centralized push to devices



- Sequential queue based operations
- Multiple attempts cause queues to blow up
- Multiple changes result in multiple places in the queue

New OSS Architecture
Devices pull and get full to do list



- Every time device checks in -> diff to required is being calculated and action list transferred to device -> latest after four hours every device picks up new payload
- Instant push still available

Features Enabled With The WS1 OSS Architecture

Freestyle - Mobile

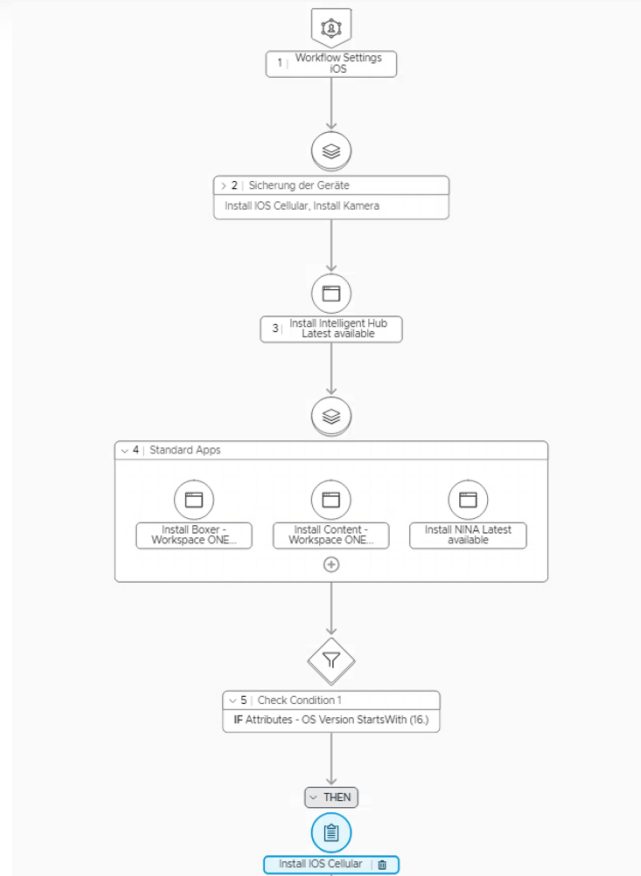


Resource Delivery &
Device List View
Improvements

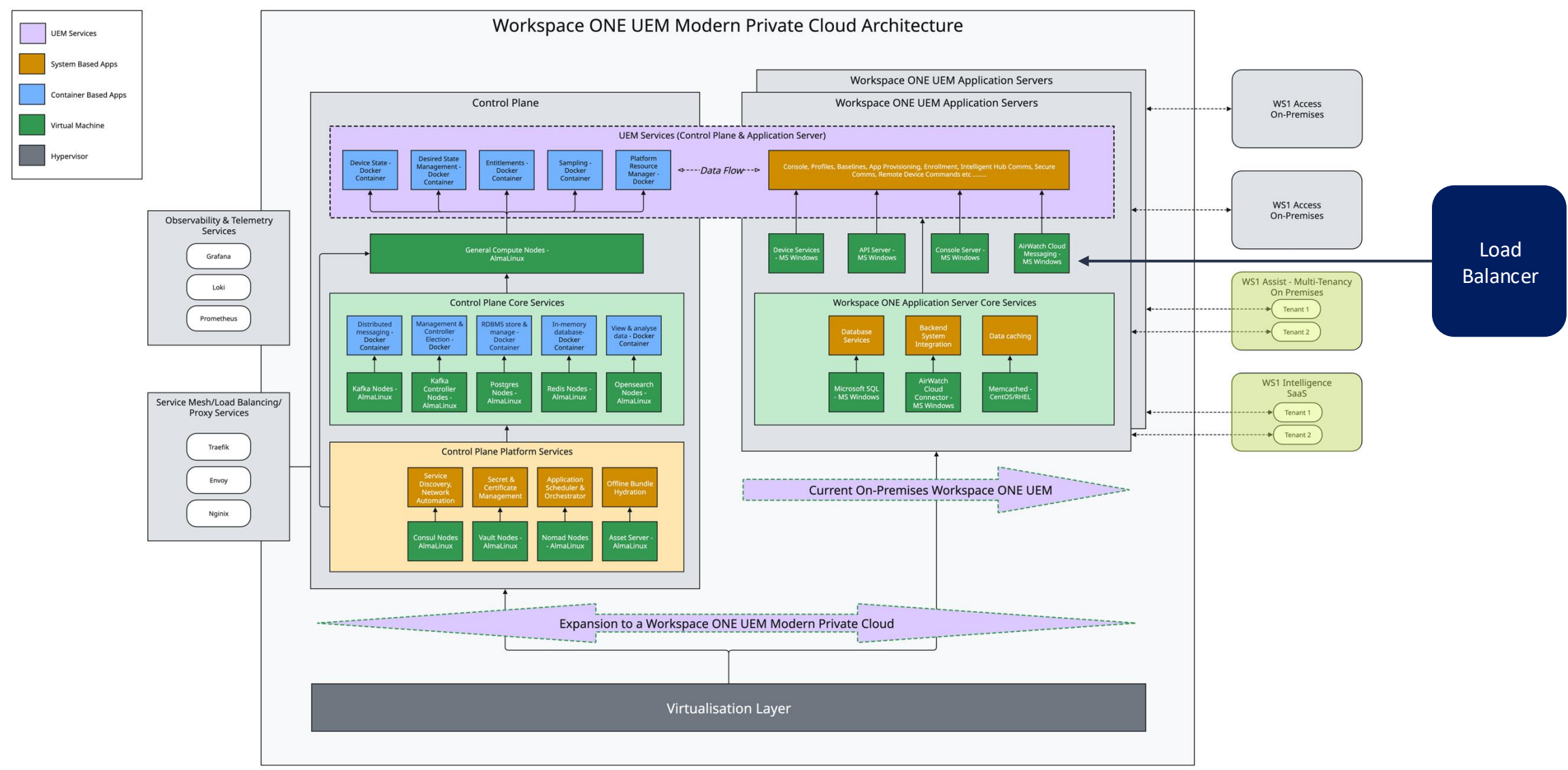


Apple

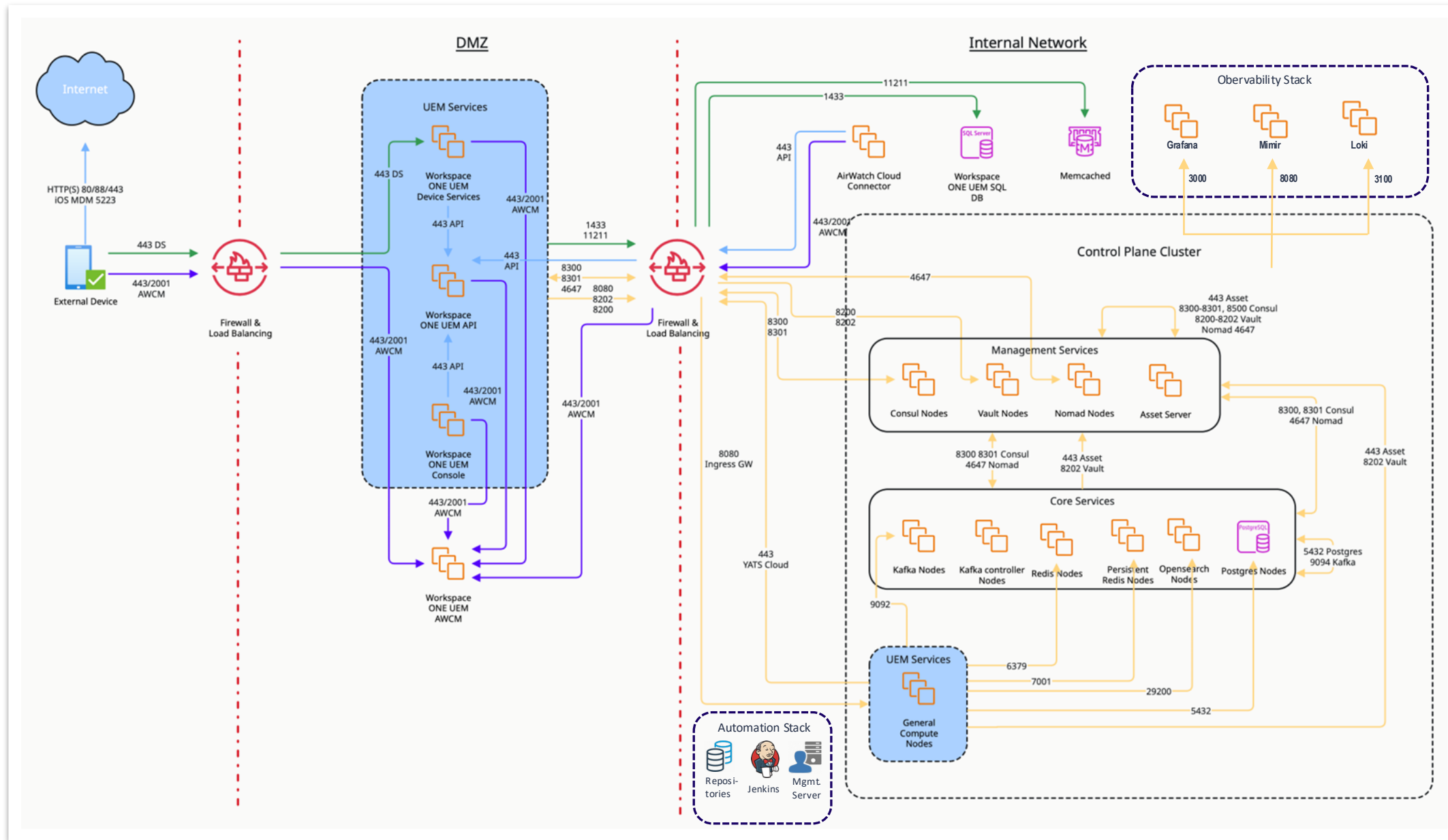
Declarative Device
Management



Workspace ONE OSS Architecture Overview



WS1 OSS Network Diagram



Questions