Zero Trust at the Tactical Edge

Maintaining policy enforcement and mission continuity in Denied, Degraded, Intermittent, and Limited (DDIL) environments.

Chris Betz

Federal Chief Technology Officer
Omnissa Federal

June 2026

The Omnissa Story

Formally the EUC Division of VMware

- On November 22, 2023, Broadcom Inc. completed its acquisition of VMware, Inc., and on December 7, 2023, Broadcom CEO Hock Tan announced his intention to divest the End-User Computing Division (EUC).
- Global investment firm KKR announced on February 26, 2024, that it has signed a definitive agreement with Broadcom to acquire the EUC Division.
- July 1, 2024 Omnissa Divests and Goes Private
- July 1, 2025 Sustained business
- Present - Growing the business

What KKR and EUC Announced

Visit media.kkr.com to read the press release

KKR, a global investment firm, has signed a definitive agreement to acquire Broadcom's EUC Division.

EUC will become a standalone company with a new name and brand when the transaction closes.

We expect the deal to close later this year, subject to customary closing conditions and regulatory approvals.

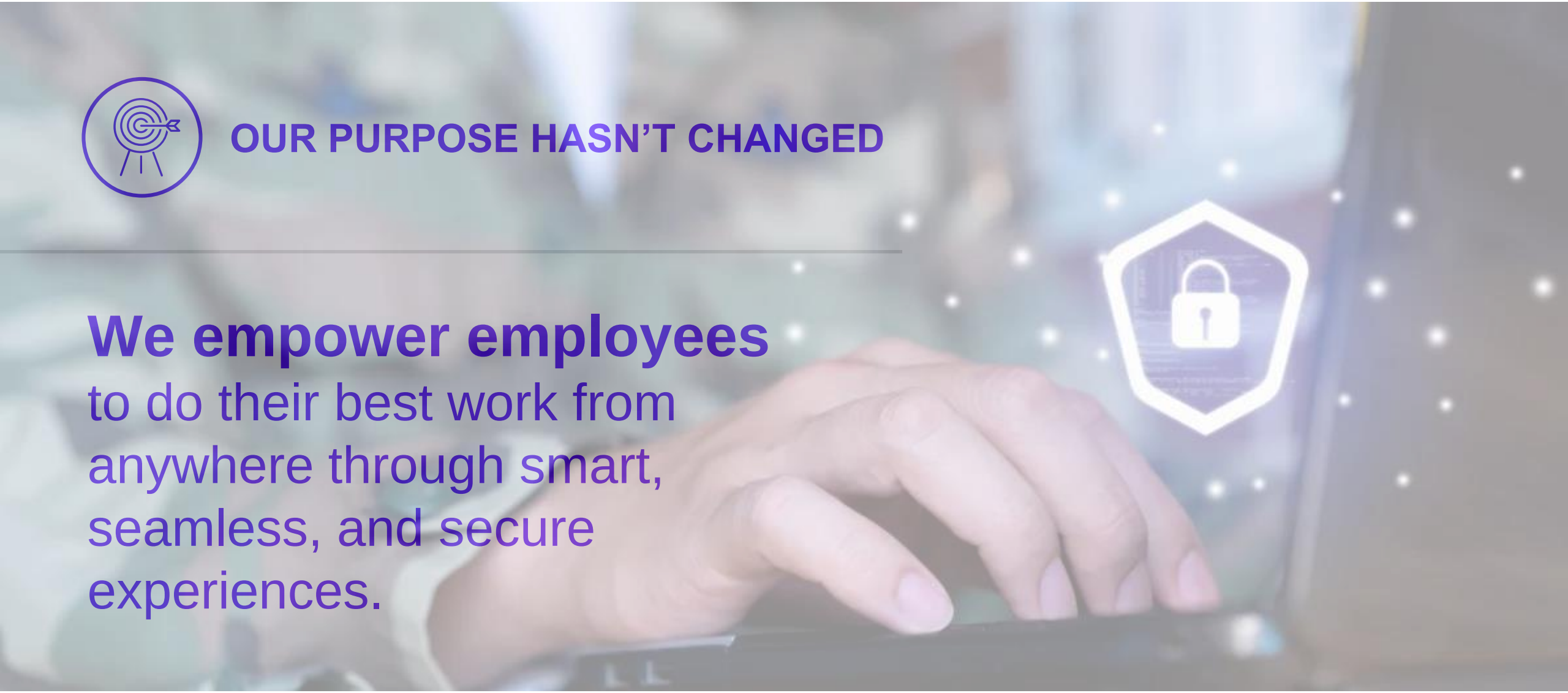
IN THE NEWS

"We see great potential to grow the EUC Division by empowering this talented team and **investing in product innovation, delivering excellence for customers and building strategic partnerships**

– Bradley Brown, KKR Managing Director
Feb 26, 2024 Press Release

...this is the **best possible outcome for employees, customers and partners**. This is good news for VMware EUC solution providers.

– CRN, Feb 24, 2024



OUR PURPOSE HASN'T CHANGED

We empower employees to do their best work from anywhere through smart, seamless, and secure experiences.

Autonomous Workspace

Consolidation without compromise

- **Onboard** any persona
- **Manage** any endpoint
- **Deliver** all apps
- **Secure** all touchpoints
- **Optimize** all experiences

Horizon®

Workspace ONE®

Open ecosystem

- Device
- Apps
- Cloud
- Security
- AI

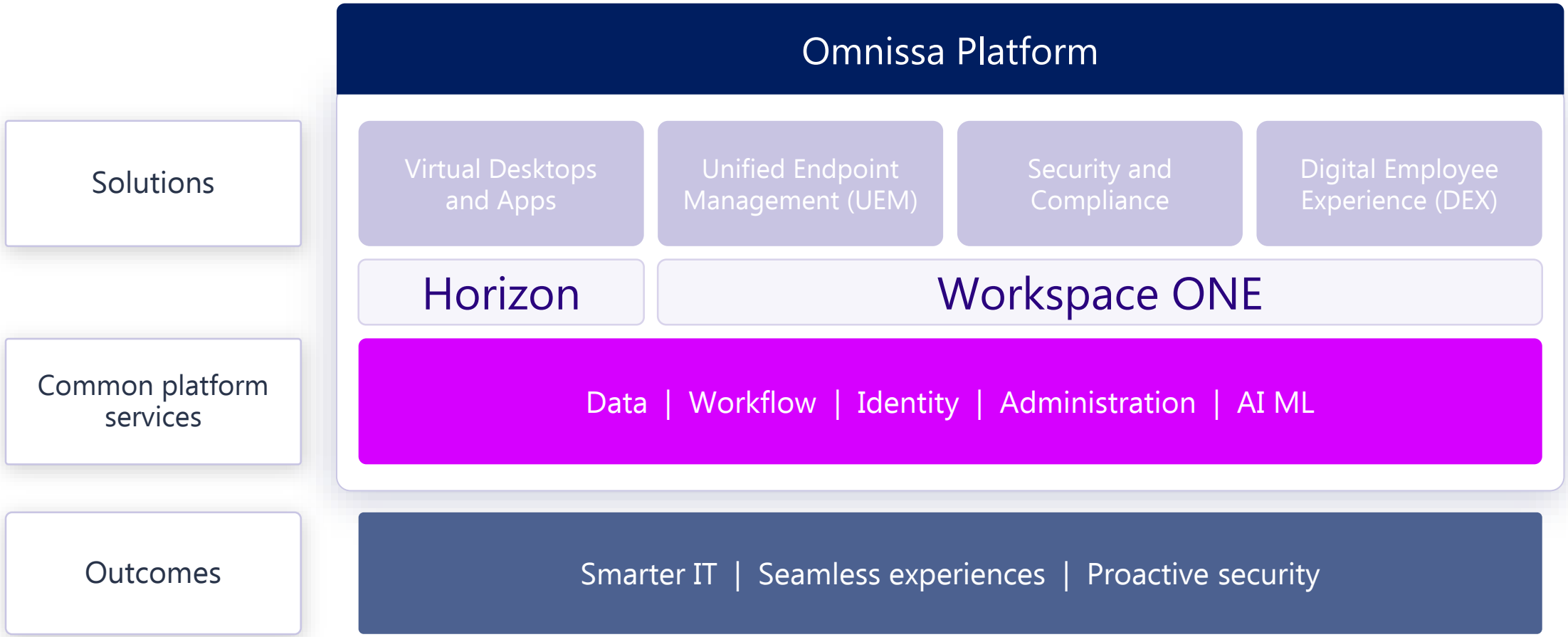
AI-driven core capabilities

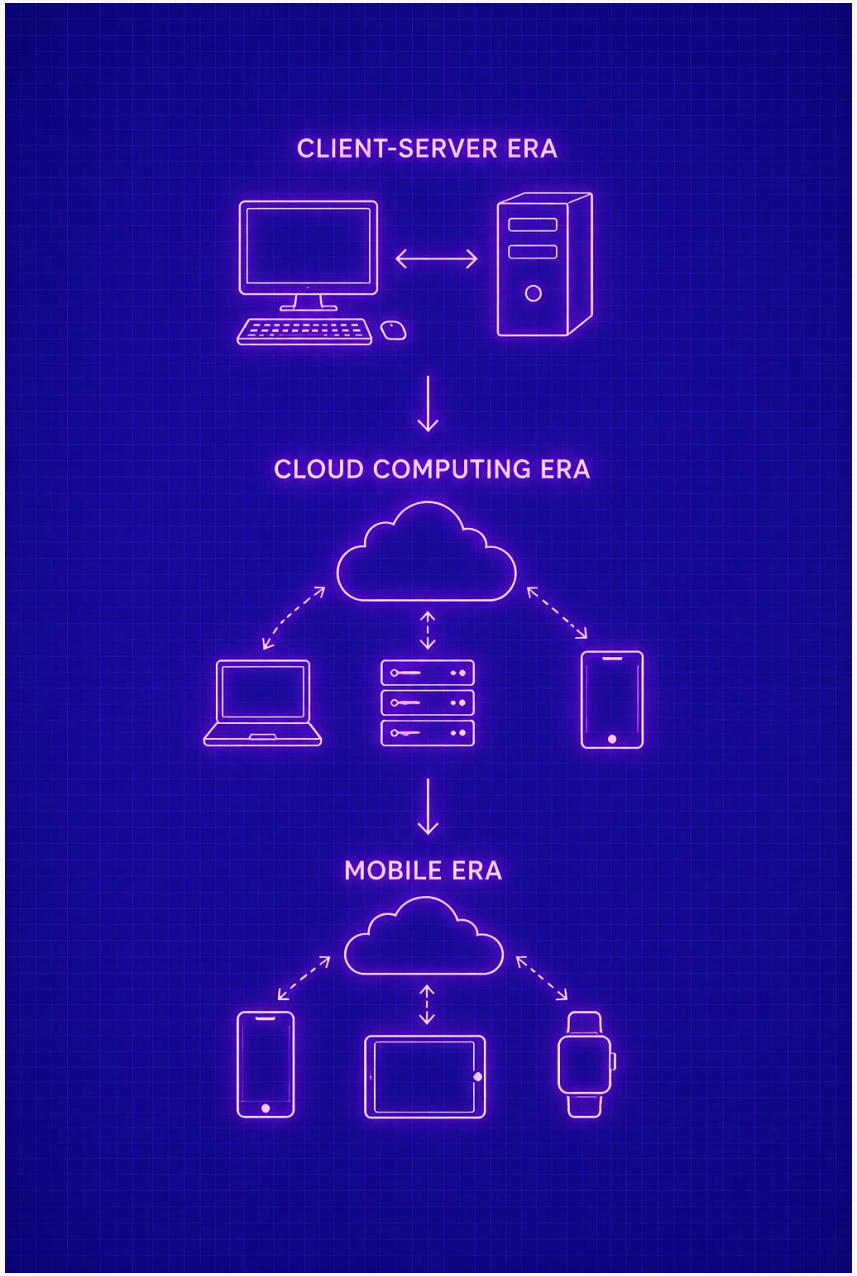
- Unified architecture
- Adaptive security
- Hyper-automation

- Self-configuring
- Self-healing
- Self-securing

Introducing Omnissa Platform
The former VMware End-User Computing Business

For smart, seamless, and secure experiences anywhere





Primary Reason for Change

The IT landscape is shifting rapidly — from traditional Client/Server infrastructures to agile, Mobile Cloud environments that deliver apps and data across any device, anywhere.

Client/Server

Legacy on-premise infrastructure with fixed access points

Cloud Platform

Apps and data hosted in scalable, centralized cloud environments

Mobile Access

Seamless delivery to any device — tablet, Android, or iOS

Three Major Trends Shaping Federal Work

New device platforms, mission apps, and user expectations are redefining secure work — and how Omnissa keeps teams mission-ready.

Mission Device Platforms

- Work extends beyond desktops and office networks
- Windows, macOS, iOS, Android, ChromeOS, and rugged endpoints
- New perimeters across bases, field sites, and partner networks
- Legacy VPN and management tools no longer scale

Mission Apps

- SaaS and mobile-first mission applications dominate
- M365, OneDrive, Teams, DEOS, and Cloud Identities
- App volume and compliance complexity are rapidly increasing
- Desktop is now a collection of mission services — fluid, not static

User Expectations

- Seamless collaboration with mission partners and contractors
- Faster, secure access drives readiness and productivity
- Mobile First, BYOD, and Self-Service as the new standard
- Users won’t accept slow digital experiences

Zero Trust at the Tactical Edge

Maintaining policy enforcement and mission continuity in Denied, Degraded, Intermittent, and Limited (DDIL) environments.

Chris Betz

Federal Chief Technology Officer
Omnissa Federal

June 2026

The Zero Trust Assumption Gap

Zero Trust architectures are often designed with the assumption of consistent connectivity, which can create a significant gap when applied to missions operating in environments with limited or no network access.

Common Assumption:

- Continuous reliance on centralized policy, cloud control planes, and real-time data.

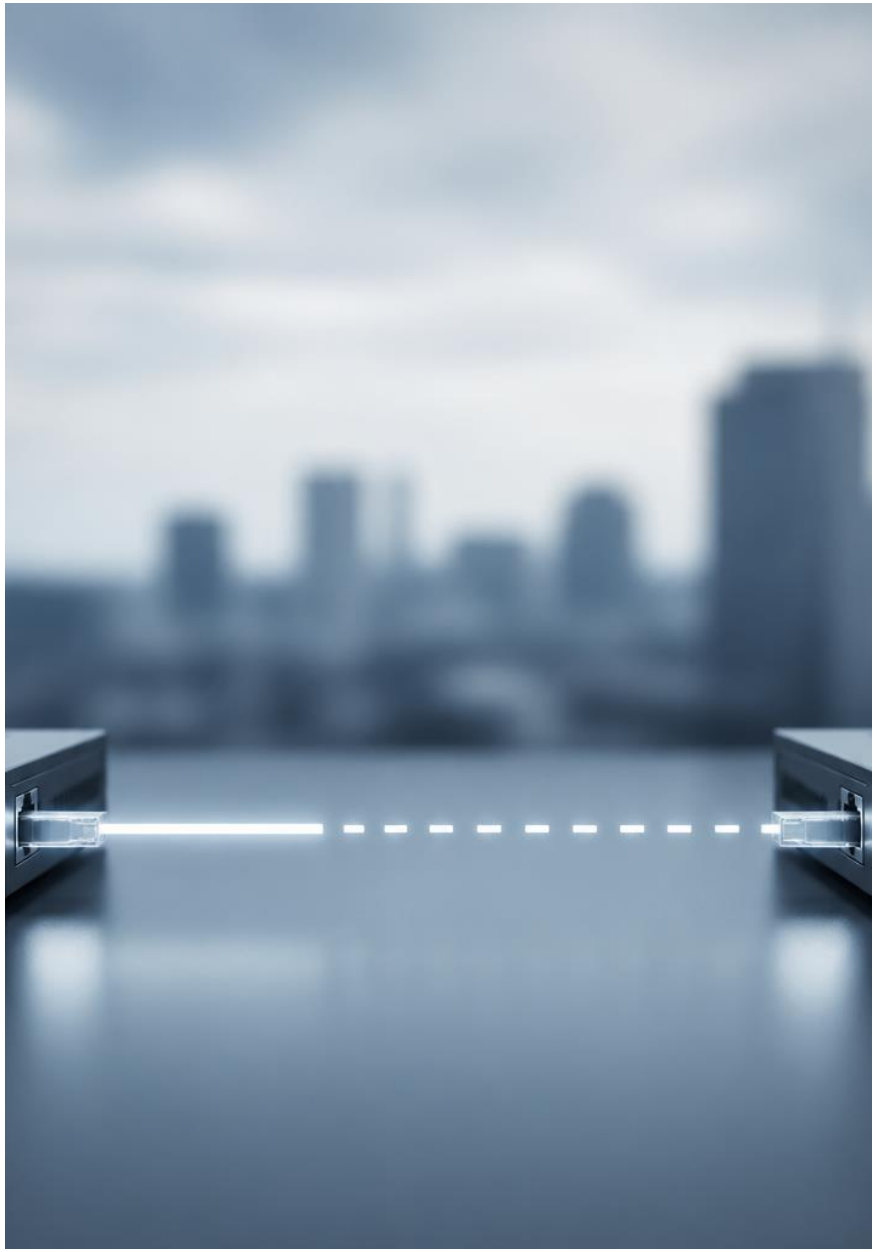
Operational Reality:

- Military and government teams frequently operate through denied, degraded, intermittent, or limited connectivity (DDILC).

Consequence:

- Enforcement, visibility, and control weaken precisely when adversary pressure and mission dependency increase.

Zero Trust cannot depend solely on reach-back for its effectiveness.



Security Imperative

DDIL: Adapting the Enforcement Model

The security architecture must maintain trust decisions even when the network is no longer dependable.

From Connected Enterprise to Disconnected Operations:

- **Denied: No reliable path to cloud or enterprise services.**
- **Degraded: Constrained bandwidth, high latency, or unreliable transport.**
- **Intermittent: Periodic check-ins with long gaps between policy updates.**
- **Limited: Only critical services or low-bandwidth telemetry can pass.**

The security architecture must survive this full operational lifecycle.

What Breaks When Zero Trust Depends on Reach-Back

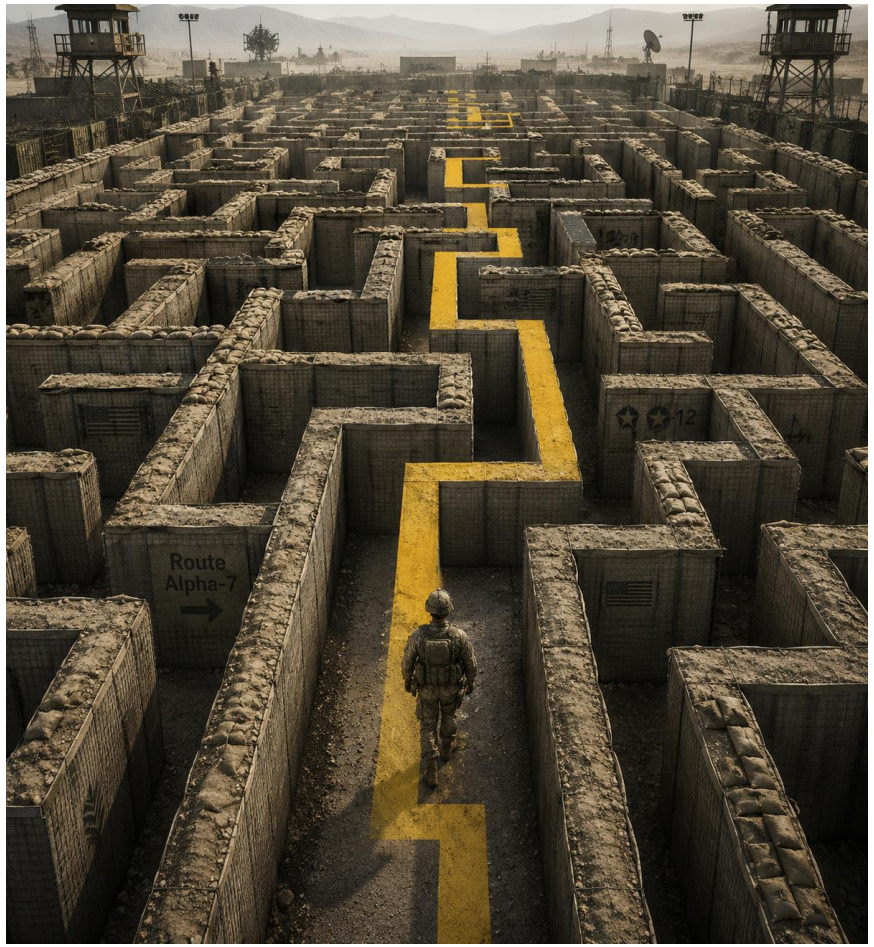
The failure is often in the dependency chain, not a single tool.

- **Identity**
  Token refresh, MFA, or federation failures can prevent authentication.
- **Policy**
  Live calls to central policy engines become impossible, halting access decisions.
- **Device Posture**
  Compliance state becomes stale without evaluation/reporting, leading to potential vulnerabilities.
- **Telemetry**
  Security signals arrive late, partially, or not at all, hindering real-time threat detection.
- **Credentials**
  Static credentials become tempting, insecure workarounds when dynamic methods fail.
- **Lateral Movement**
  Weak segmentation increases the blast radius in flat environments when core controls are bypassed.

Design Goal: Keep least privilege and enforcement intact even when parts of the chain are unavailable.

Reframe Zero Trust for Disruption

Zero Trust must operate *through* DDIL, not around it.



- **Shift from Network-First Access**

  Focus shifts from network-centric security to a more granular approach.

- **Shift from Live Policy Dependency**

  Policy enforcement is embedded at the endpoint and workspace, not solely reliant on real-time network checks.

- **Shift from Static Exception Paths**

  Utilize controlled execution environments to limit the impact of potential breaches.

- **Shift from Visibility Only When Connected**

  Ensure telemetry and policy state are synchronized even when connectivity is temporarily lost.

The Omnissa Lens

The Digital Workspace as the Enforcement Plane

- **User + Identity Context**

  Role, entitlements, authentication strength, mission context.

- **Device Posture**

  Compliance, configuration, patch state, risk signals.

- **Application Access**

  Approved apps, secure delivery, entitlement validation.

- **Session + Execution State**

  Controlled virtual session, runtime risk, data movement policies.

- **Telemetry + Remediation**

  Experience, security signals, local actions, sync when available.

Control follows the user, device, application, and session—not just the network path. Enforce locally. Synchronize globally.

A Practical Architecture Pattern for DDIL Zero Trust

A cloud-operating model when connected. Local enforcement when disconnected. Synchronization uponrestoration.

Define desired state, access policy, and compliance baseline in the cloud.

Push policy, keys, and configurations to managed endpoints or edge services.

Evaluate posture, entitlement, session state, and execution controls without continuous reach-back.

Queue events and reconcile policy state, compliance status, and audit data when connectivity returns.

Capability Model: What Needs to Keep Working Offline

Device Posture

Local compliance checks, configuration state, and encryption.

Session Control

Least privilege within the workspace; restrict data movement.

Identity Context

Cached entitlements, token, and session handling.

Data Protection

Reduce credential exposure and limit sensitive data execution.

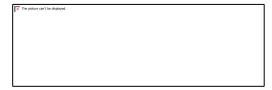
App Control

Guaranteed delivery, allow/deny rules, and approved access paths.

Auditability

Store telemetry locally and synchronize events when connected.

Offline means policy enforcement must survive disconnection, not cease.



Mission Workflow Example

A phased operational pattern

Policy, apps, posture baseline, and mission entitlements are staged.

Users access only approved resources through managed devices/sessions.

Posture drift or high-risk behavior triggers local restrictions.

Telemetry and state reconcile when communications return.

How Omnissa Capabilities Align

A Unified Platform for Endpoint Management, Virtual Apps/Desktops, Experience Telemetry, and Security Controls

Core Components

Workspace ONE®

Device posture, UEM, app delivery, configuration, compliance.

Horizon

Controlled desktops/apps, session isolation, entitlement, execution environment.

Intelligence

Telemetry, experience signals, automation, proactive remediation.

Security + Compliance

Access workflows, posture, least privilege, audit support.

VALUE PROPOSITION: CONVERGENCE ACROSS IDENTITY, DEVICE, APP, SESSION, TELEMETRY, AND REMEDIATION.

Outcomes for DoW Components

Resilient Zero Trust – secure access that survives disruption.

Maintain Least Privilege

Access based on identity, device posture, entitlements.

Reduce Credential Exposure

Limit reliance on static credentials.

Limit Lateral Movement

Contain compromises within smaller boundaries.

Preserve Mission Continuity

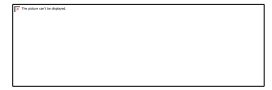
Users continue working within policy during DDIL.

Improve Auditability

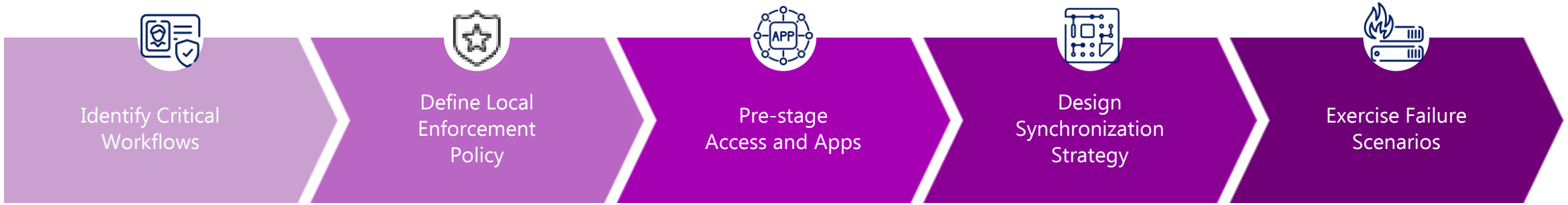
Synchronize telemetry and state for compliance.

Support Cloud Operating Model

Govern centrally, enforce locally, operate anywhere.



A Practical Path Forward



Which users, apps, devices, and sessions must function in DDIL?

What decisions can be made based on device posture, identity, and session state?

What entitlements, apps, and configurations are needed offline?

What telemetry and state must reconcile upon reconnection?

Test degraded and disconnected operations before mission dependence.

Start by identifying and controlling critical workflows that must operate in DDIL.

Zero Trust Built for Disruption

For DoW environments, the critical question is not if Zero Trust works when things are connected, but if it keeps working when the mission is not.