



CUSTOMER SNAPSHOT

# Global Data Center Power Provider - Manufacturing OT Remote Access

A global data center power provider is retiring legacy VPN access on the factory floor with zero-trust remote access from Kasm Workspaces.

The manufacturer needed to give third-party vendors and internal engineers hands-on access to specific PLCs and VNC-connected machinery on a flat, unsegmented OT network — without a path to anything else. Kasm Workspaces, deployed with a Kasm services partner, is now the single zero-trust gateway for that access.



3 of 3

priority manufacturing use cases proven in the proof of concept



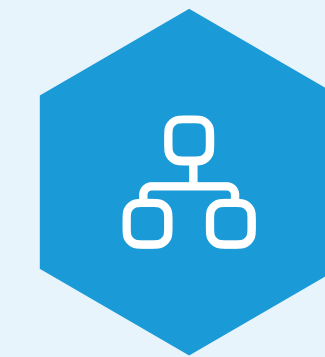
1–2 mo

target timeline to fully retire legacy VPN-based OT remote access



Zero

direct network access required for vendor sessions - proxied to one authorized workspace



Multi-site

manufacturing sites brought onto a single access architecture



## INDUSTRY

Energy onsite power generation for data centers and industrial customers



## ENVIRONMENT

Multi-site manufacturing · Windows PLC hosts · VNC floor equipment



## DEPLOYMENT

AWS-hosted control plane · connection proxies per site



## REPLACED

Legacy VPN-based remote access for vendors and internal staff



## The challenge

The customer designs, manufactures and services onsite power systems for data centers. Its factory floor runs on Windows-based PLC controllers and VNC connected equipment, serviced by internal engineers and third-party vendors including overseas OEMs supporting the machinery remotely.

Vendor access was the core problem. The OT network was flat, with no segmentation between sites or vendor tenants. A vendor who needed one machine received something closer to a full employee footprint - and every session was a potential path for lateral movement.

The incumbent general-purpose VPN tool was never designed for device specific OT access. As the environment scaled, the team needed to

- ✓ Expose only the specific PLC and VNC endpoints each vendor or engineer needs
- ✓ Enforce need-to-know access so one vendor's session can never reach another's equipment
- ✓ Carry RDP, VNC and secure web apps through one consistent access layer
- ✓ Scale across sites without rebuilding site by site
- ✓ Do it on a network never formally segmented or documented



## The Kasm solution

Working with a Kasm implementation partner, the team ran a structured proof of concept on three priority use cases: vendor access to Windows/VNC hosts running PLC software, controlled access to internal Kasm tool instances, and VNC access to other floor equipment.

### Single-zone PoC first

The Kasm web application and database were hosted in AWS, proxying directly to existing Windows and VNC endpoints. That validated gateway authentication, protocol translation and session isolation before any multi-site complexity was added.

### Protocol translation at the proxy

Kasm connection proxies translate the vendor's web-native session into RDP or VNC for the target machine. Vendors authenticate once at the gateway and are proxied only to the workspace they are authorized to reach — no VPN-level network access.

### Tenant isolation by policy, not by re-wiring

Group policy defines security zones per workspace, scoping each user group to specific endpoints, tools and DLP controls. One vendor's tenant has no visibility into another's — with no up-front network redesign.

Why the customer chose Kasm

The incumbent was a general-purpose VPN tool being asked to do device-level OT access control. Kasm Workspaces inverted the model: instead of placing a vendor on the network and constraining where they could go, it places them in a single, policy-scoped workspace and translates protocol to exactly one endpoint. Because isolation is enforced through group policy and security zones, the customer did not have to segment and document its flat network first — the access layer did the work.

Just as important, the PoC infrastructure carried forward. The customer's cloud engineering team confirmed that the AWS-hosted deployment could become the production control plane rather than being rebuilt, which directly reduced the professional services scope for the rollout



Vendors and internal staff now reach specific OT endpoints through a single, auditable access layer — with no direct network exposure.

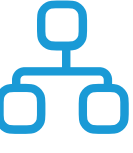
Proof-of-concept outcome, as validated by the customer's IT, security and cloud engineering teams



A modernization path for legacy Windows applications

In parallel, the team scoped a containerization track: packaging legacy Windows manufacturing applications into on-demand workspaces using Kasm's agent architecture. This gives the customer a longer-term option to reduce its dependence on full Windows VM sessions in favor of positive-security, purpose-built application delivery

Results

| Area                                                                                                       | Before                                                  | With  Kasm<br>WORKSPACES | Impact                                 |
|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|----------------------------------------|
|  Vendor access scope      | Near-employee network footprint via general-purpose VPN | Single authorized workspace, proxied to one endpoint                                                          | Lateral-movement path closed           |
|  Tenant isolation         | None — flat network, no segmentation between vendors    | Security zones and group policy per workspace                                                                 | Enforced without network redesign      |
|  Priority OT use cases    | Unsupported by incumbent tool                           | PLC/VNC hosts, internal tool instances, floor equipment                                                       | 3 of 3 validated                       |
|  Legacy VPN access for OT | Primary remote-access method                            | Retired site by site as use cases onboard                                                                     | Full retirement targeted in 1-2 months |
|  Multi-site scale         | Rebuild per site                                        | Central control plane; add proxies and agents per site                                                        | Scales without re architecting         |

What's next

-  SSO/MFA integration and a formal architecture review underway as part of production hardening — closing a documentation gap that predated the engagement
-  Expand Kasm coverage to the remaining manufacturing sites on the multi-zone model
-  Formalize a managed-services arrangement with a Kasm partner for day-to-day administration
-  Continue the containerization track for legacy Windows factory-floor applications

