

OT Secure Remote Access, Simplified

Standardize your environment. Improve operational efficiency. Scale with confidence.

Presented by:

Name

Title

Email



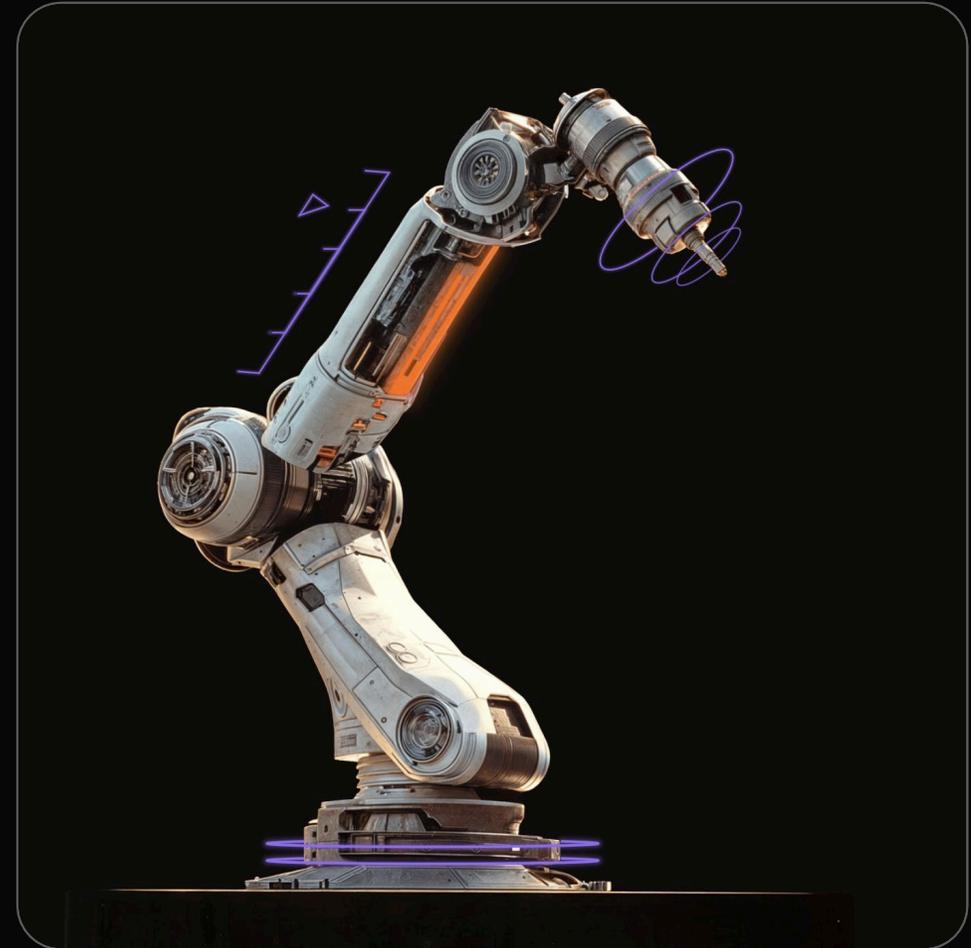
Operational Efficiency

“Unplanned downtime costs \$125,000 per hour”

–ABB, *Value of Reliability Report*

How “just making it work” tools drags on efficiency:

- Delays caused by inconstant vendor access
- Slow response times and troubleshooting
- High-maintenance and not built for OT workflows or automation
- Complex to manage access for operators, contractors, and OEMs
- Lack of visibility and control over remote session





Cyber Resilience

“By 2028, the percentage of attacks on CPS using remote access vectors will grow to over 15%.”

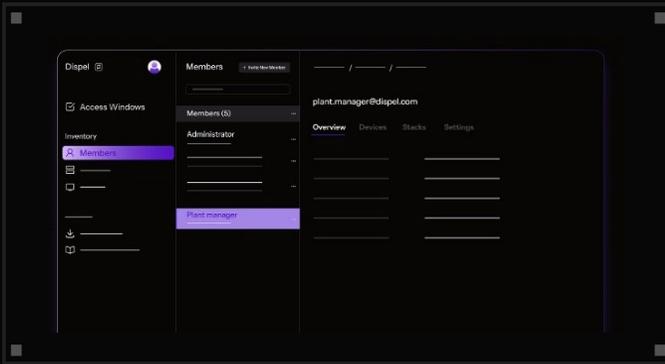
-Gartner® Innovation Insight: CPS Secure Remote Access Solutions

Don't leave the door open to your OT environment:

- RPAM not built for ICS/OT; lacks protocol support and control
- VPNs & Jump hosts expand the attack surface with broad access
- No audit logs, session isolation, or live monitoring
- Compliance risk from misalignment with IEC 62443, NIS2, and more

Redefine How You Connect to OT

Built for both OT and security teams, Dispel reduces operational costs and delivers immediate value—through a unified Zero Trust platform designed for how OT really works.



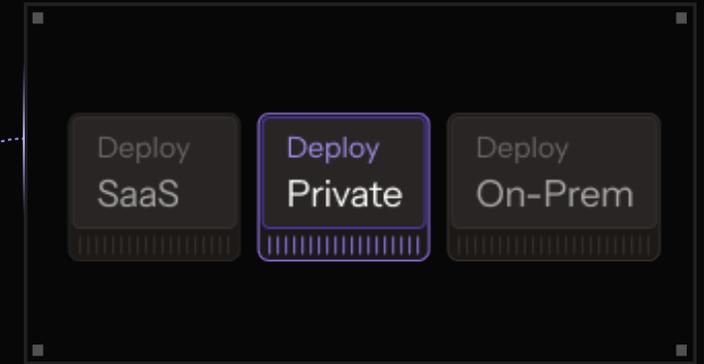
Dispel Zero Trust Engine

- OT Secure Remote Access
- Industrial Data Streaming
- Integrated Threat Monitoring
- OT DMZ Unification



Tiered Connection Suite

- Browser Connect
- Virtual Desktop
- Local Application



Deployment at Scale

- SaaS
- Private
- On-Prem
- Hybrid

OT Secure Remote Access, Simplified

Connect fast. Cut downtime. Enforce Zero Trust. Simplify operations.

- **Boost Productivity** – Access in under 30 seconds—faster response times without delays and bottlenecks
- **Reduce Overhead** – Eliminate management and maintenance burden of jump servers
- **Streamline Vendor Access** – Rapidly onboard contractors and OEMs without friction or risk
- **Strengthen Security Posture** – MTD eliminates static pathways, reducing your attack surface.



Designed for How OT Really Works

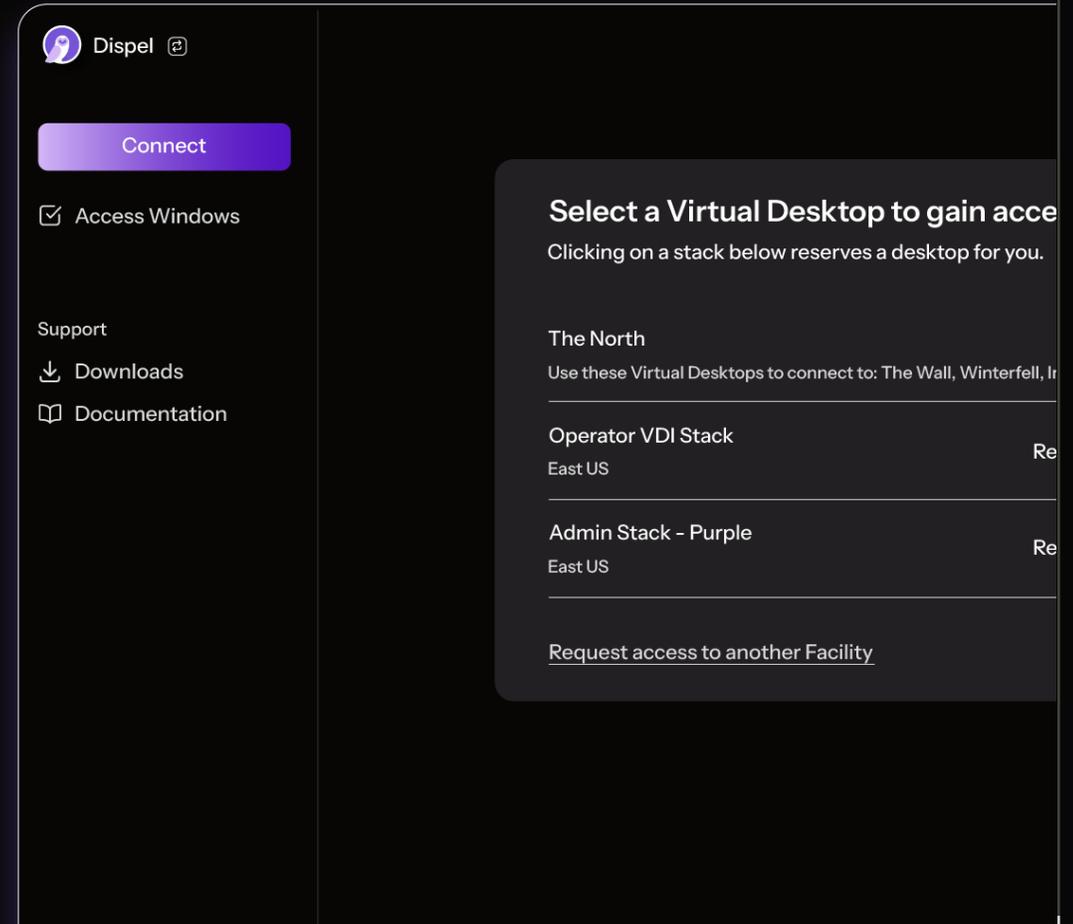
Streamline operational and security workflows through one unified platform.

OT Workflows & Automation

- Site specific administration and approvals
- Easy vendor and contractor self-onboarding
- Just-in-time, access windows, MFA, password vaulting, patching

Protocol Support

- Supports 65,000+ TCP/IP protocols including SSH, RDP
- Supports proprietary OT systems such as Rockwell FactoryTalk, Siemens TIA Portal, and Mitsubishi GS Works



Built for Efficiency, Secure by Design

Extends “never trust, always verify” across OT networks to protect every session

Zero Trust Cybersecurity

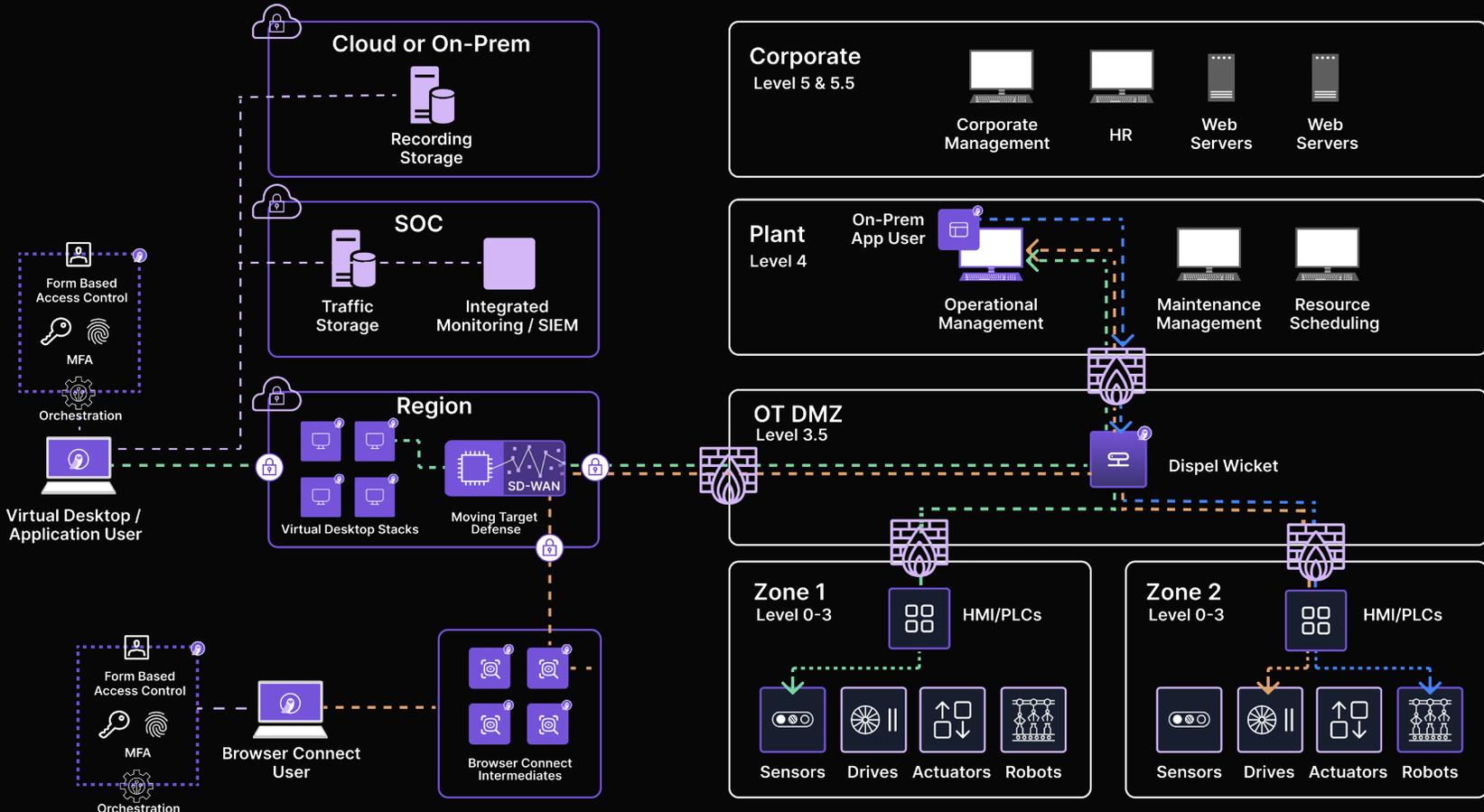
- Moving Target Defense SD-WAN, eliminates static pathways, reducing your attack surface
- Encryption, session isolation, segmented pathways, integrated threat monitoring, and audit logging

Turnkey Compliance

- Inherit alignment out of the box NIS2, IEC 62443, NIST 800-53, and NERC CIP controls



Tailored OT Secure Remote Access for Every Role, Every Use Case



Tiered Connection Suite



INDUSTRY STANDARD
**Clientless
 Browser Connect**
 For rapid access.



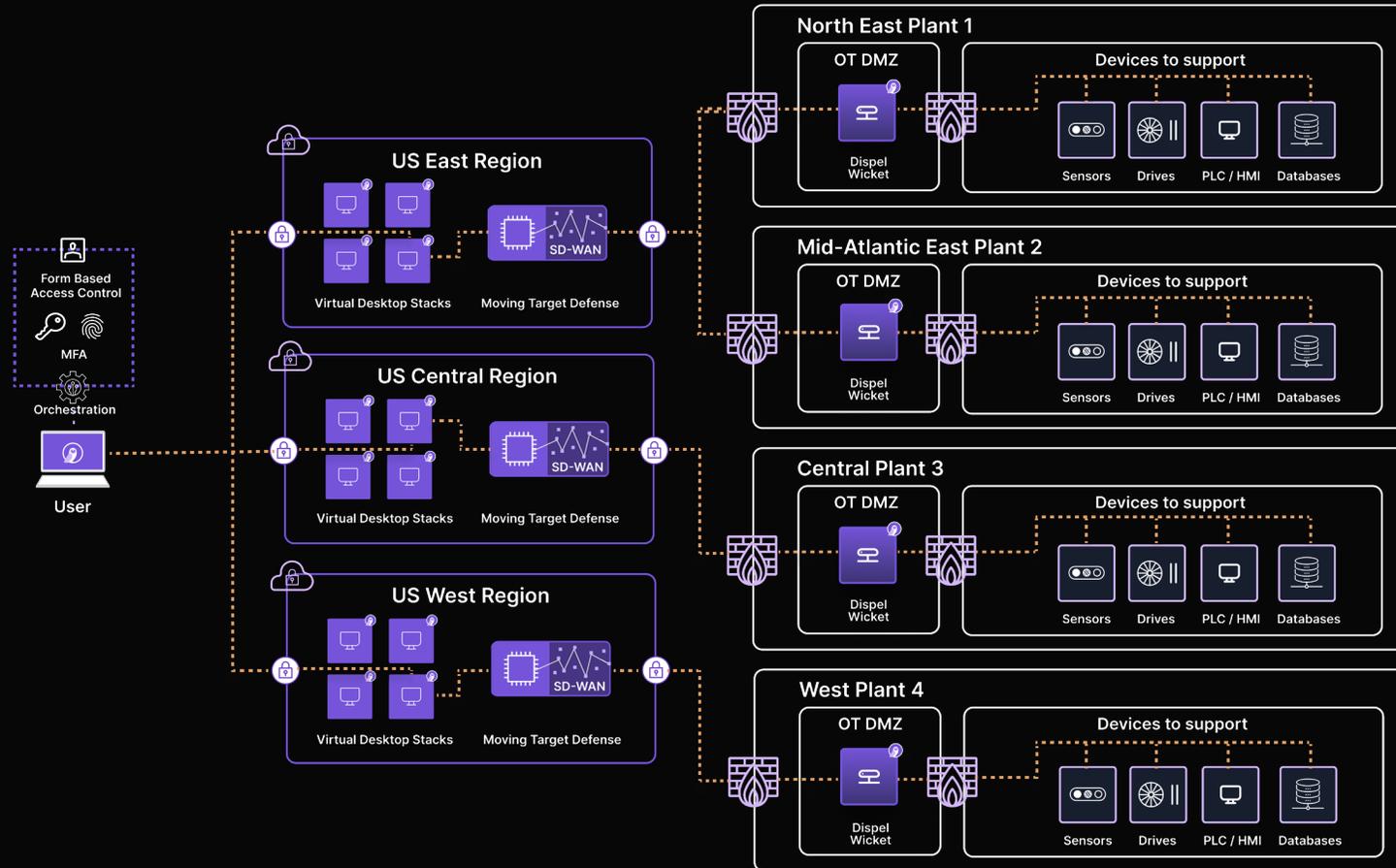
BEST-IN-CLASS
Virtual Desktop
 Full workstation with
 highest security posture.



EXTEND CONTROL
Local Application
 For legacy systems and
 custom tooling.

Deployment at Scale

Dispel makes large-scale OT operations agile, secure, and ready to connect.



Deploy at Enterprise Scale

Go live in 3 hours, scale to 100 sites in 90 days



Flexible Deployment Options

SaaS, Private, or On-Prem to fit your infrastructure



Burst Capacity Vendor Access

Scale remote access surges for 100+ vendors in minutes



Operational Downtime

“40% reduction in maintenance costs with Predictive Maintenance”

—Siemens, *The True Cost of Downtime 2024*

Relying on siloed, outdated data exfiltration results in:

- **Limited Predictive Maintenance impact** – Without real-time data, downtime and emergency repairs rise.
- **Supply chain blind spots** – Partners can't optimize without direct data access.
- **Manual updates** – Scaling patches is resource-heavy with significant O&M costs
- **Operational inefficiency** – Disjointed systems hinder growth from mergers and acquisitions



Drive Operational Growth with Industrial Data Streaming

Real-time industrial data streaming that empowers manufacturers, utilities, and OEMs to scale predictive maintenance, simplify updates, and drive AI-powered productivity.

Scale improvements across your operations with:

- **Standardize operations** across merged or multi-site roll-up
- **Scale predictive maintenance** and condition monitoring
- **Streamline system updates** and patch management
- **Accelerate compliance**, AI adoption, and data-driven analytics initiatives

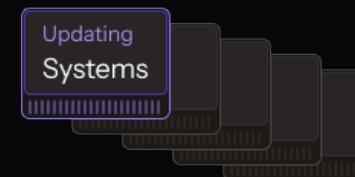
Standardize Operations

Unify data across sites for faster roll-up efficiency.



Simplify Updates

Push patches and configs across fleet securely.



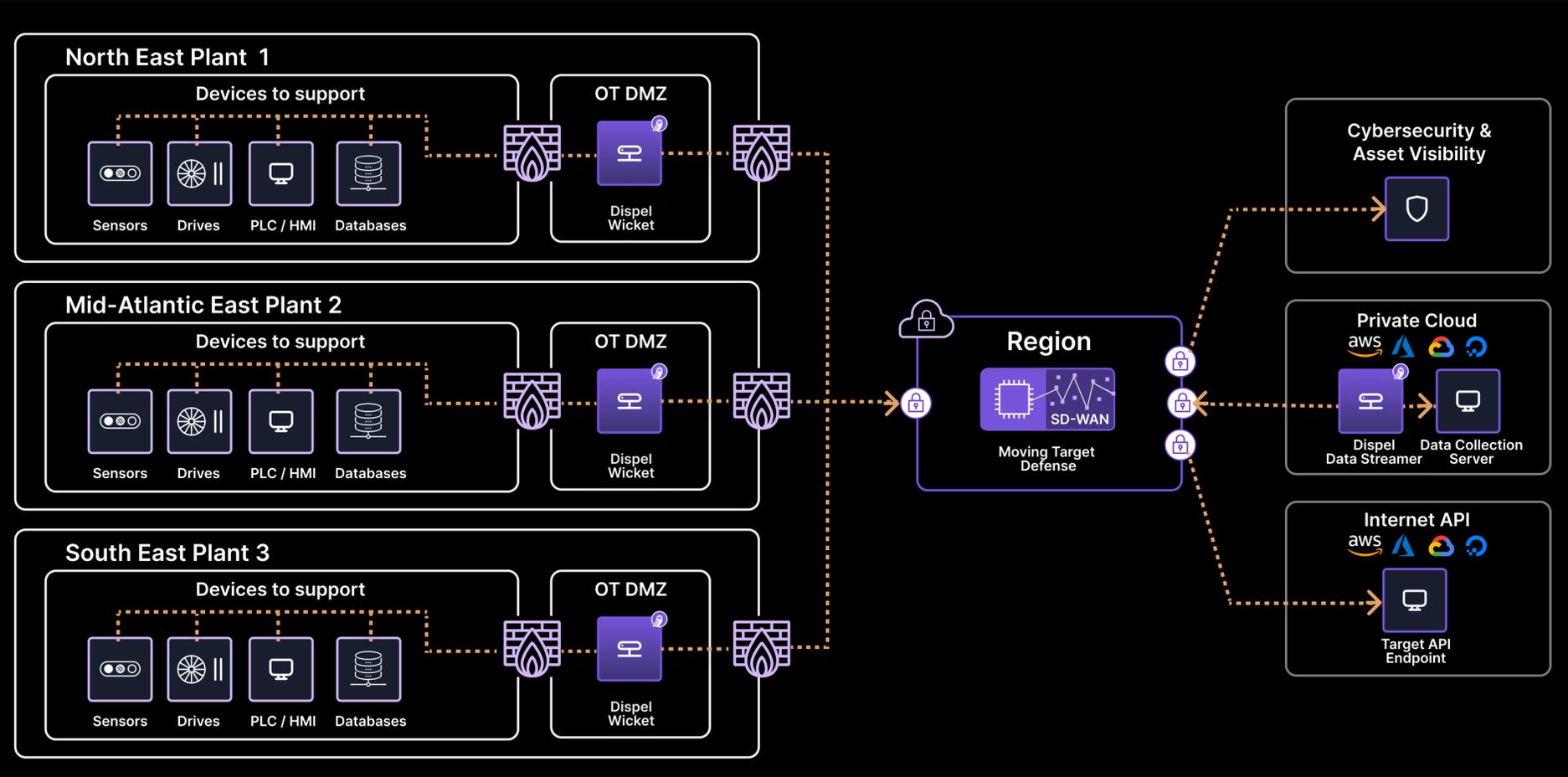
Power Predictive Maintenance

Stream real-time data to Pdm platforms



Industrial Data Streaming

Simplify device-to-device transfer of real-time operational, diagnostic, and system data between industrial assets and cloud environments—enabling format- and data-type-agnostic transport layers.



Why Industrial Teams Choose Dispel

We're Not Just Another Remote Access Vendor—We're Built for OT.

Competitive Edge

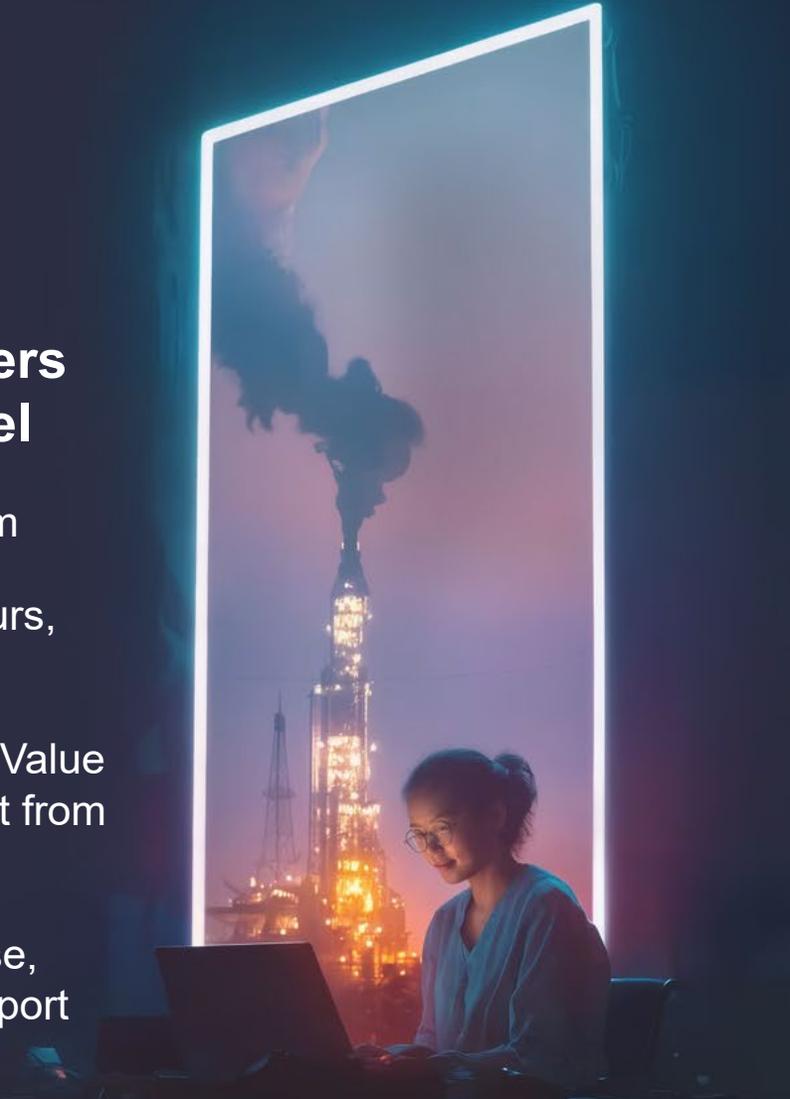
- Purpose-built for OT environments
- Tiered connections that scale with your operations, now and in the future
- Best-in-class Virtual Desktop workstations
- Compostable MTD SD-WAN infrastructure

Security Backed by Innovation

- Defense is in our DNA
- 10 years of innovation with 43 patents
- Aligned with Your Frameworks IEC 62443, NIST 800-53, NERC CIP
- Seamless integration with your tools and partner ecosystem

Why Customers Choose Dispel

- Unified platform
- Deploys in Hours, Not Months
- Rapid Time-to-Value with minimal lift from your team
- Effortless to use, scale, and support



Real-world impact. Proven at scale.

Daimler gained centralized control, visibility into third-party access, and faster response times across global operations.

Dispel simplifies access workflows and closes the loop between service tickets and security monitoring for both IT and OT teams.

-Daimler



Case Study | Watercare

Utility for 84% of New Zealand's population.

- Mission critical asset.
- Variable OT network layouts with numerous legacy systems.
- Dependent upon global network of technicians to keep the system running.

Objectives

- Defend New Zealand's water supply from nation state cyber attacks.
- Assert control over, and get visibility into, connections made to OT assets.
- Standardize how OT assets were being accessed across plants.
- Reduce downtime by letting vendors remotely fix equipment.
- Cut operating costs by minimizing travel.
- Implement a system that could be fully sustained by Watercare.
- Enable geographic redundancy for access to the underlying network.
- Future proof posture of facilities by deploying NIST 800-53 aligned system.

Key Outcome

- Consolidated, self-sustaining network for accessing water systems.

Ringfenced the OT environment, standardized system access, and established a self-sustainable network environment.



DISPEL

Before you ask, that is a kiwi bird.