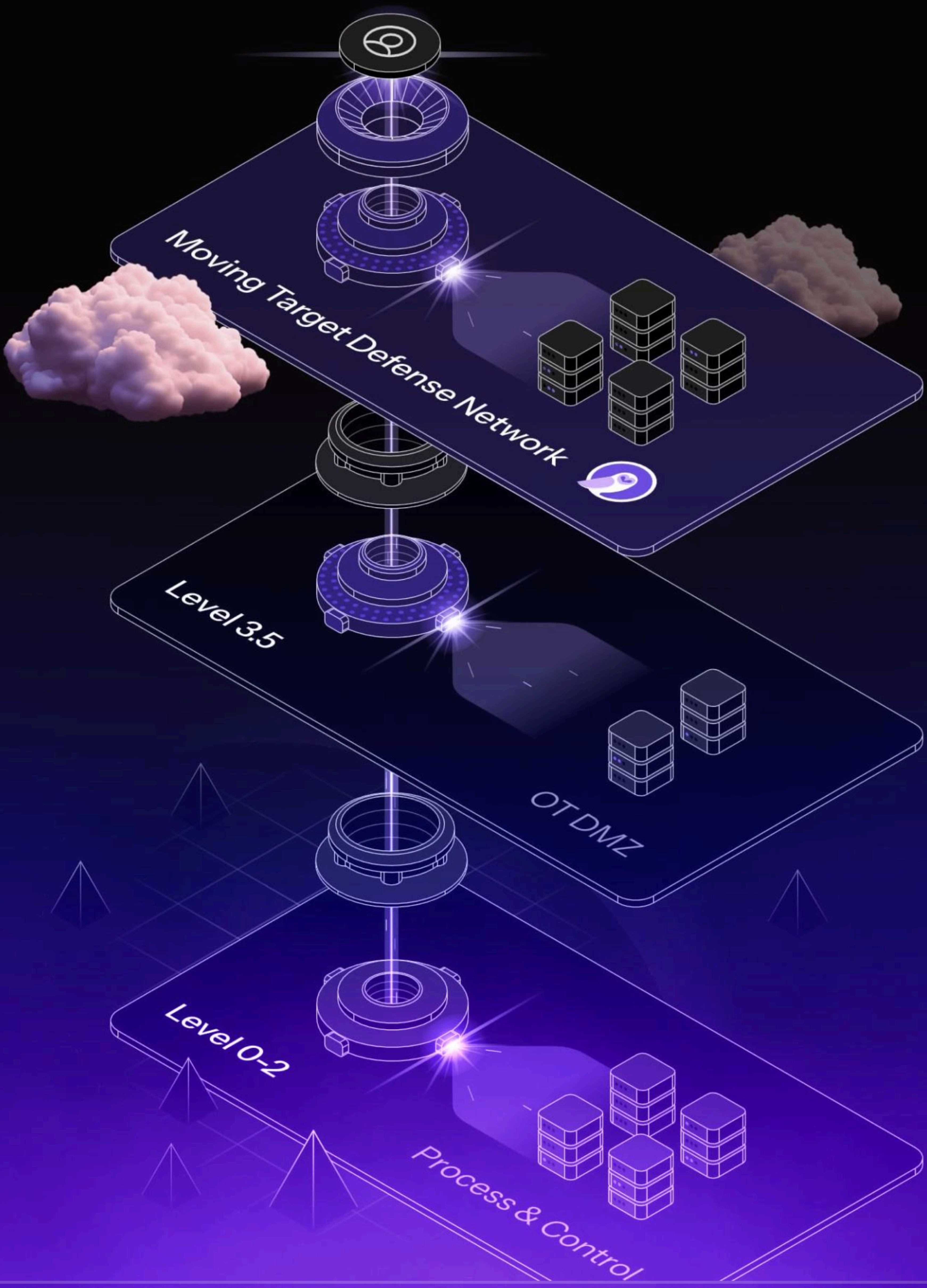
Dispel Zero Trust Engine

Total control. Full visibility. OT Secure Remote Access Simplified.



Product Brochure

Executive Summary

As industrial organizations accelerate digital transformation and IT/OT convergence, the need to securely connect remote operators, third-party vendors, and systems—without increasing cyber risk or operational complexity—is critical. This brochure introduces the Dispel Zero Trust Engine—a secure remote access solution built to meet the scale, complexity, and performance demands of OT environments. It highlights the platform's core capabilities, key features, and real-world use cases that help organizations simplify operations, eliminate jump servers, reduce risk, and enable secure, real-time access across industrial networks.

Table of Contents

Key Capabilities

Today’s Industrial Landscape

In today's interconnected industrial landscape, critical infrastructure sectors like manufacturing, electric utilities, water/wastewater, and oil & gas are rapidly embracing digital transformation and IT/OT convergence to improve business processes and enhance efficiency. This process unlocks new value across an organization, but it can also expose an organization to targeted cyberattacks and vulnerabilities.

With the rise of remote workforces and globally distributed operations, today’s operational technology (OT) environments are more complex—and more fragmented—than ever. Organizations often inherit a mix of factory acquisitions and fleets of equipment that vary by make, model, and year—de-standardizing their systems and introducing layers of inconsistency. These environments span everything from legacy systems that can’t support modern cybersecurity installations to IIoT devices and industrial protocols with unpredictable connectivity requirements.

OT Secure Remote Access (SRA) is critical to bringing order to this complexity. It enables organizations to securely standardize access across diverse systems—empowering internal operators, external contractors, and third-party vendors to efficiently monitor, manage, and access mission-critical ICS/OT assets without compromising security or performance.

Business Impact

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

—Gartner® Innovation Insight: CPS Secure Remote Access Solutions

Leveraging a purpose-built OT Secure Remote Access solution with Zero Trust principles not only safeguards critical infrastructure but also ensures measurable business value:

- Operational Continuity & Reliability – Ensures resilient, real-time access even in low-bandwidth or air-gapped environments, reducing costly downtime.
- Cost Efficiency & ROI – Lowers operational expenses by reducing onsite visits, eliminating jump hosts, and simplifying legacy system maintenance.
- Compliance & Risk Management – Aligns with OT-specific regulations (IEC 62443, NERC CIP, NIST 800-82) while providing full auditability and session oversight.
- Enhanced Productivity & Collaboration – Enables fast, secure access for engineers, operators, and vendors while supporting multi-user collaboration and real-time supervision.
- Vendor & Protocol Flexibility – Supports industrial and proprietary protocols, ensuring seamless remote access across diverse OT environments.
- Enhanced Security Posture – Reduce the attack surfaces with micro-segmentation, MFA, IAM, just-in-time access and Moving Target Defense, minimizing cyber risks and preventing lateral movement.

We Understand the Roadblocks You're Up Against

Industrial organizations face unique challenges and security threats that traditional IT remote privileged access management (RPAM) and secure remote access solutions simply were never designed to handle. Many organizations fail to allocate adequate resources for OT security, often attempting to extend IT-focused solutions into OT environments, leaving critical systems exposed to these unique threats and vulnerabilities.

RPAM is not purpose-built for OT

While RPAM solutions are effective in IT environments, they face significant limitations in OT settings due to the fundamental differences in infrastructure, workflows, and security requirements:

- Limited compatibility with legacy systems and proprietary protocols common in industrial control systems.
- Credential vaulting and role-based models don't always align with OT's device- and interface-based access.
- Requires persistent, bidirectional connectivity that conflicts with segmented or air-gapped OT networks.
- Introduces latency through proxies, disrupting real-time control, diagnostics, and maintenance workflows.
- Lacks process-level visibility, offering no insight into specific actions taken on industrial equipment.
- Designed for IT administrators, not field technicians—leading to usability friction and operational delays.

Gartner underscores that while RPAM solutions effectively manage IT systems and standard protocols, they typically fall short in OT contexts, leading to integration challenges, operational disruptions, and compliance gaps.

Why Jump Servers Fall Short for OT Secure Remote Access

Jump servers, also called jump hosts or bastions, were once a go-to solution for remote access in OT environments, but as threats evolve and operational complexity grows, their limitations have become increasingly unsustainable.

- Violates least privilege principles by granting broad access or requiring one jump server per asset, neither scalable nor secure.
- Lacks granular session control, JIT access, user visibility, and safeguards against risky actions like file transfers.
- Creates significant operational overhead from manual patching, configuration, and content management, especially in resource-constrained OT environments.
- Fails to scale securely, forcing a trade-off between risk (multi-asset access) and admin sprawl (hundreds of jump servers).
- Uses shared credentials, obscuring individual accountability and complicating incident response and compliance audits.
- Retains access for former employees and vendors, increasing insider risk.

RPAM and Jump servers were not built for the modern OT attack surface

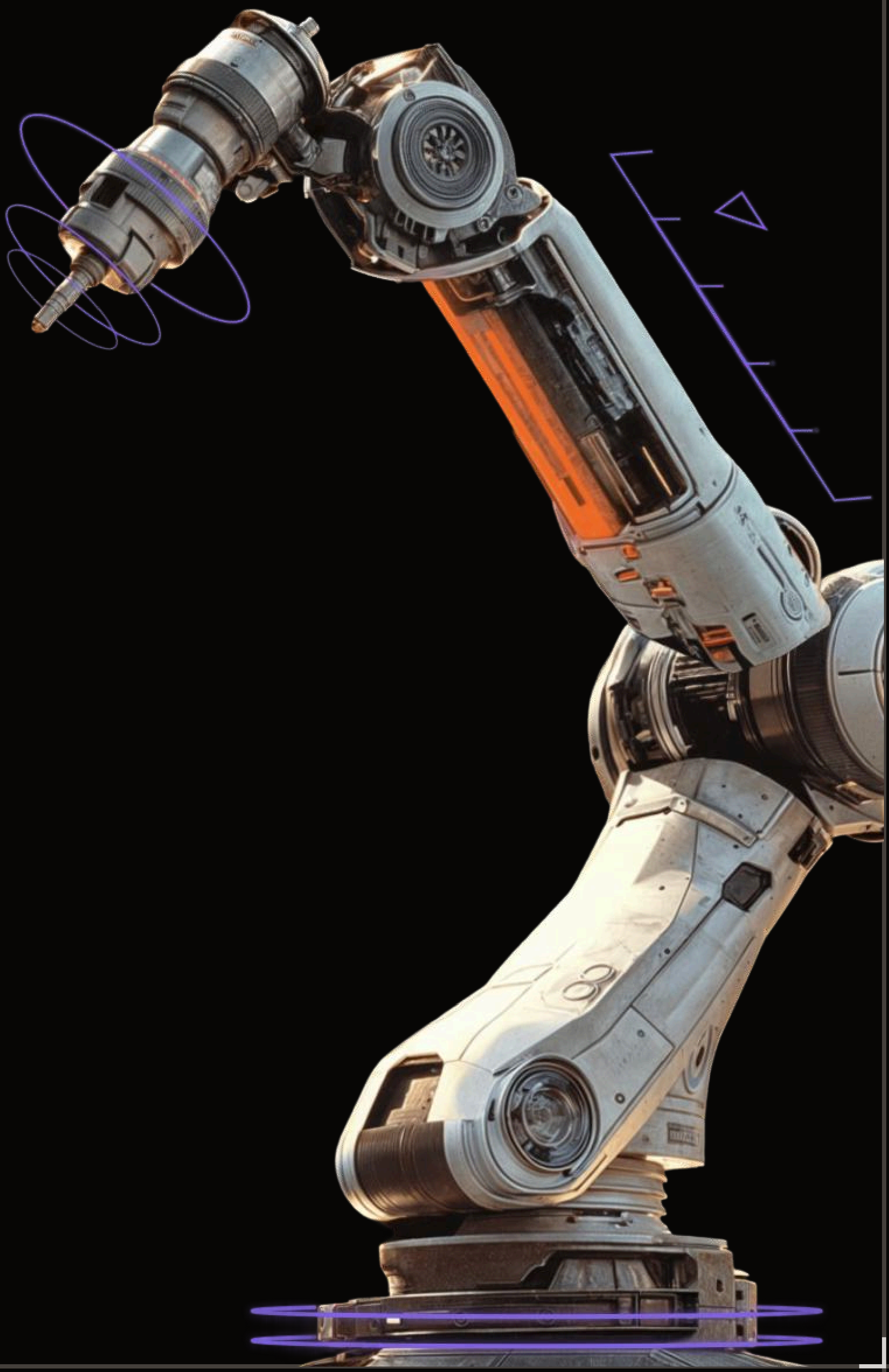
Recent reports reveal that 80% of manufacturers have experienced a rise in security incidents across their IT/OT environments, with ransomware groups focusing more than ever on utilities, with a 42% surge in attacks over the past year. In another report, intelligence shows 65% of assessed OT environments had insecure remote access conditions, including misconfigurations, outdated systems, and weak segmentation.

In 2024, the same report shows over 50% of ransomware incidents stemmed from compromised remote access services, with attackers exploiting unpatched VPN appliances, or remote access applications, leading to severe operational disruptions. The inherent weaknesses of traditional remote access methods, such as corporate VPNs and jump servers, have expanded attack surfaces, exposing OT networks to escalating cyber threats.

SRA Tool Sprawl in OT: A Growing Security and Operational Risk

Industrial organizations often rely on a patchwork of VPNs, RPAM tools, jump servers, and vendor-specific portals to support 30–40+ distinct remote access user profiles. This ranges from engineers and operators to system integrators and third-party vendors. This tool sprawl leads to fragmented visibility, inconsistent policies, and complex access management.

According to the SANS ICS/OT Cybersecurity Survey, 42% of organizations use three or more remote access tools, and 20% use five or more, often without centralized oversight. Dragos highlights remote access complexity and lack of standardization as a top contributor to OT cyber incidents. Industry analysts like ARC Advisory Group and Gartner recommend platform consolidation to improve visibility, control, and resilience.

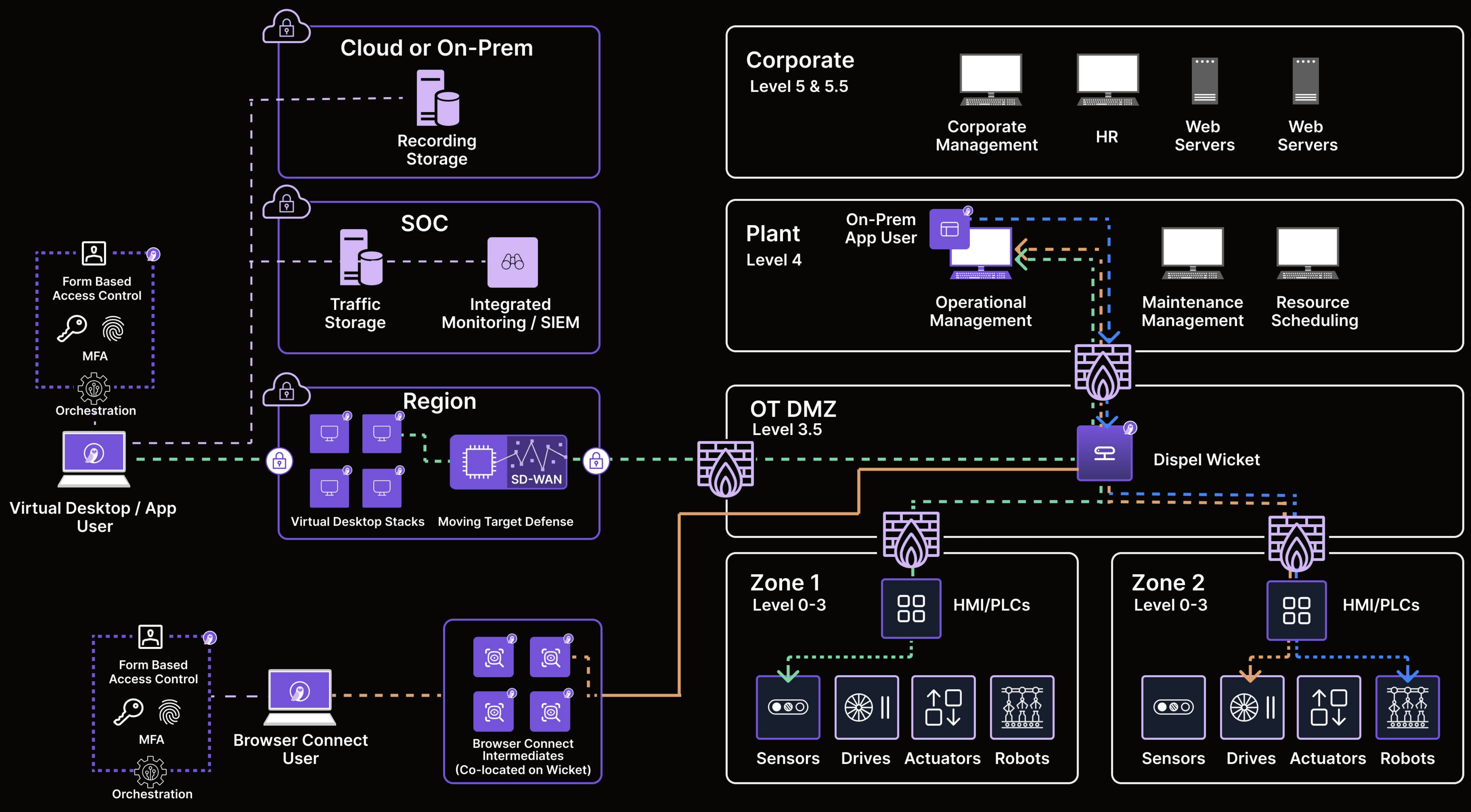


Standardizing OT Secure Remote Access with Dispel

The most comprehensive secure remote access solution, purpose built for your unique ICS/OT environment

The **Dispel Zero Trust Engine** delivers OT secure remote access, industrial data streaming, and integrated threat monitoring—giving industrial organizations complete control and full visibility, standardizing access across legacy systems, modern IIoT, and distributed OT environments, all from one unified, scalable platform.

Built on Zero Trust principles of "never trust, always verify" and powered by Dispel's industry-leading Moving Target Defense (MTD) and compostable SD-WAN architecture, this plug-and-play solution enables secure access to OT systems in under 30 seconds. Easy to use. No delays. Because every second matters.



This diagram illustrates the Dispel Engine's flexible, tiered connection methods. Deploy the industry-standard, clientless Browser Connect for rapid access. Scale up to best-in-class, single-tenant Virtual Desktop workstations as a jump server replacement—offering the highest security posture available. Or extend control with the Local Application for legacy systems and custom tooling needs. These options enable users to securely access ICS/OT systems for a wide range of use cases—all through a single, unified platform.

Key Capabilities

1. OT Secure Remote Access

Securely connect internal operators, external contractors, and third-party vendors to mission-critical OT assets—replacing high-maintenance jump servers with a faster, more efficient, and scalable remote access solution.

Designed for How OT Really Works

The Dispel Zero Trust Engine delivers tailored OT secure remote access for every role and every use case, offering the flexibility to scale up or down without compromising performance or security.

Whether it's internal operators, third-party vendors, or external contractors, Dispel provides precise, role-based access aligned to operational needs. Simply choose the connection method that fits your team's needs:

- **Clientless Browser Connect** – An industry-standard for rapid, no-install access
- **Virtual Desktop** – Best-in-class, single-tenant workstations with unmatched security
- **Local Application** – Ideal for legacy systems and custom tooling

From streamlining internal and external workflows to enabling burst capacity access for remote vendors, with the ability to scale up hundreds of vendors in minutes—Dispel delivers the full spectrum of remote access through a single, unified platform.

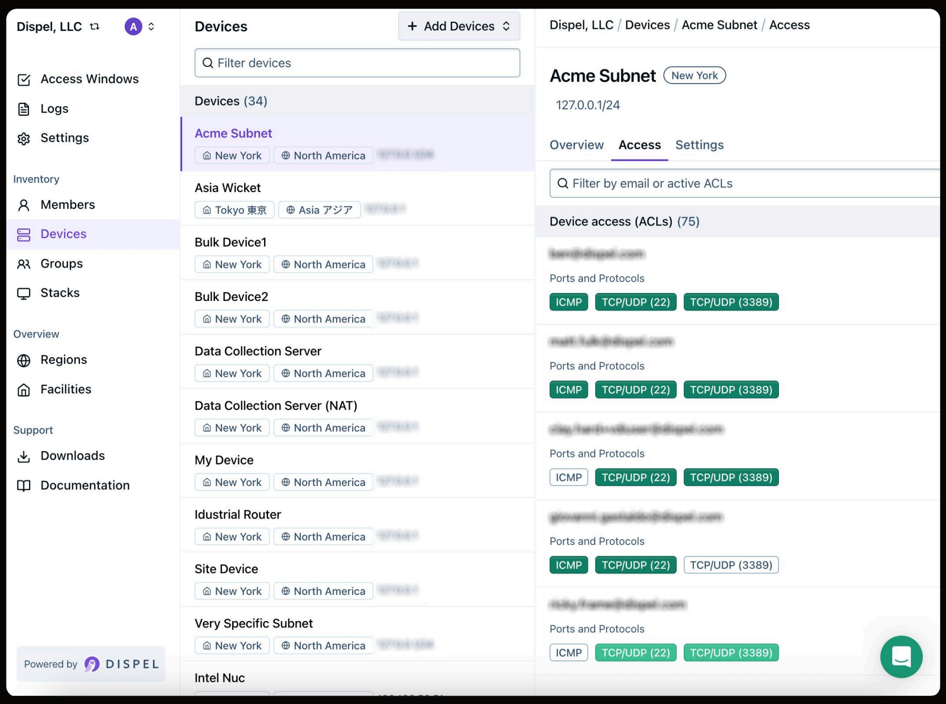
Only Dispel Virtual Desktop workstations let you:

- Replace high-maintenance jump server to improve operational efficiency
- Flex up 100+ vendors in minutes, with no local infrastructure required for emergency access

Simplified Remote Access Management

Give your admins the power to automate OT workflows with bulk device management, automated patching, and seamless vendor onboarding.

With granular control and full visibility into every remote access session, they can easily track and revoke privileges based on user, device, port, protocol, or time, ensuring every session is auditable and secure.



Dispel, LLC

Access Windows
Logs
Settings

Inventory
Members
Devices
Groups
Stacks

Overview
Regions
Facilities

Support
Downloads
Documentation

Powered by DISPEL

Devices

+ Add Devices

Filter devices

Devices (34)

Acme Subnet
New York · North America · [redacted]

Asia Wicket
Tokyo 東京 · Asia アジア · [redacted]

Bulk Device1
New York · North America · [redacted]

Bulk Device2
New York · North America · [redacted]

Data Collection Server
New York · North America · [redacted]

Data Collection Server (NAT)
New York · North America · [redacted]

My Device
New York · North America · [redacted]

Idustrial Router
New York · North America · [redacted]

Site Device
New York · North America · [redacted]

Very Specific Subnet
New York · North America · [redacted]

Intel Nuc

Dispel, LLC / Devices / Acme Subnet / Access

Acme Subnet New York

127.0.0.1/24

Overview Access Settings

Filter by email or active ACLs

Device access (ACLs) (75)

[redacted]
Ports and Protocols
ICMP TCP/UDP (22) TCP/UDP (3389)

[redacted]
Ports and Protocols
ICMP TCP/UDP (22) TCP/UDP (3389)

[redacted]
Ports and Protocols
ICMP TCP/UDP (22) TCP/UDP (3389)

[redacted]
Ports and Protocols
ICMP TCP/UDP (22) TCP/UDP (3389)

[redacted]
Ports and Protocols
ICMP TCP/UDP (22) TCP/UDP (3389)

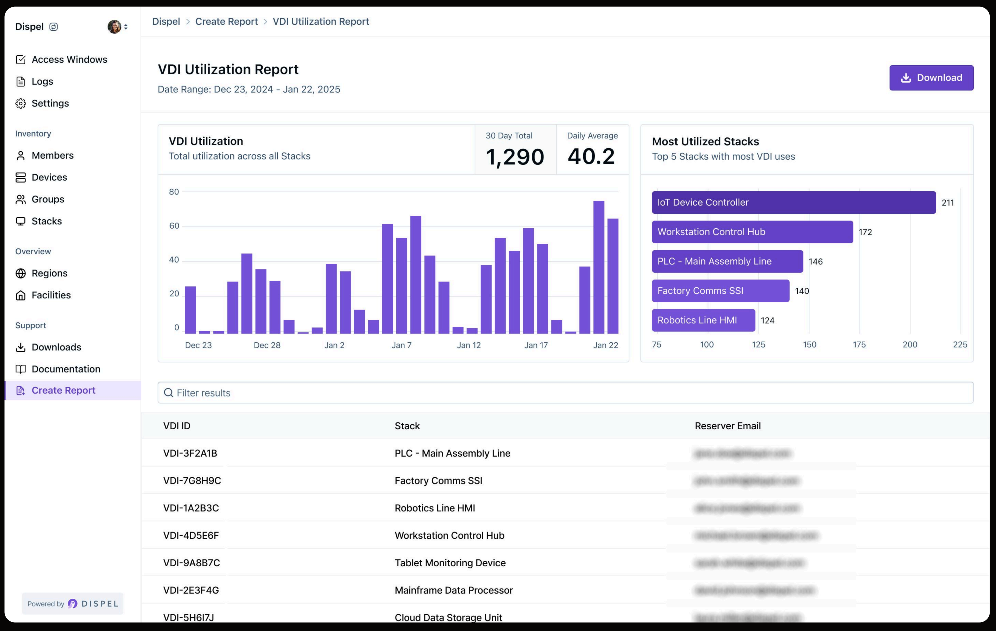
Total Visibility into Remote Users Across Your OT Environment

The Dispel Engine Dashboard delivers centralized visibility and control over remote access, supporting both cybersecurity enforcement and day-to-day operational oversight.

With native logging, screen recording, and session playback, administrators gain full insight into user actions, system usage, and access patterns. Powerful filtering by event type, user role, location, and authentication status enables rapid investigation and policy enforcement.

Track key metrics like virtual desktop (VDI) utilization, session start/end times, and MFA status to ensure authorized access while streamlining resource planning and operational workflows.

Dispel helps teams monitor access trends against security baselines, reducing risk while improving efficiency across industrial environments.



VDI Utilization Report

Date Range: Dec 23, 2024 - Jan 22, 2025

VDI Utilization

Total utilization across all Stacks

30 Day Total 1,290

Daily Average 40.2

Most Utilized Stacks

Top 5 Stacks with most VDI uses

VDI ID	Stack	Reserver Email
VDI-3F2A1B	PLC - Main Assembly Line	[redacted]
VDI-7G8H9C	Factory Comms SSI	[redacted]
VDI-1A2B3C	Robotics Line HMI	[redacted]
VDI-4D5E6F	Workstation Control Hub	[redacted]
VDI-9A8B7C	Tablet Monitoring Device	[redacted]
VDI-2E3F4G	Mainframe Data Processor	[redacted]
VDI-5H6I7J	Cloud Data Storage Unit	[redacted]

Compliance & Control

The Dispel Engine is purpose-built to meet strict OT cybersecurity requirements, with SOC 2 Type 2, ISO 27001, and IEC 62443 certifications. Organizations inherit these robust security controls out of the box—streamlining compliance with frameworks such as NIS2, NIST 800-53 High Baseline, and NERC CIP. This far exceeds the capabilities of traditional RPAM and SRA solutions, delivering the strong security foundation industrial environments require.

With total access control and full visibility, the Dispel Engine provides just-in-time access windows, MFA, IAM, and password vaulting—enabling granular access control so users only access your environment for a defined period of time. Zero Trust security ensures end-to-end encryption, micro-segmented pathways, session isolation, posture checking, audit logging, reporting, and screen recording—delivering the layered protection needed to defend against threats.

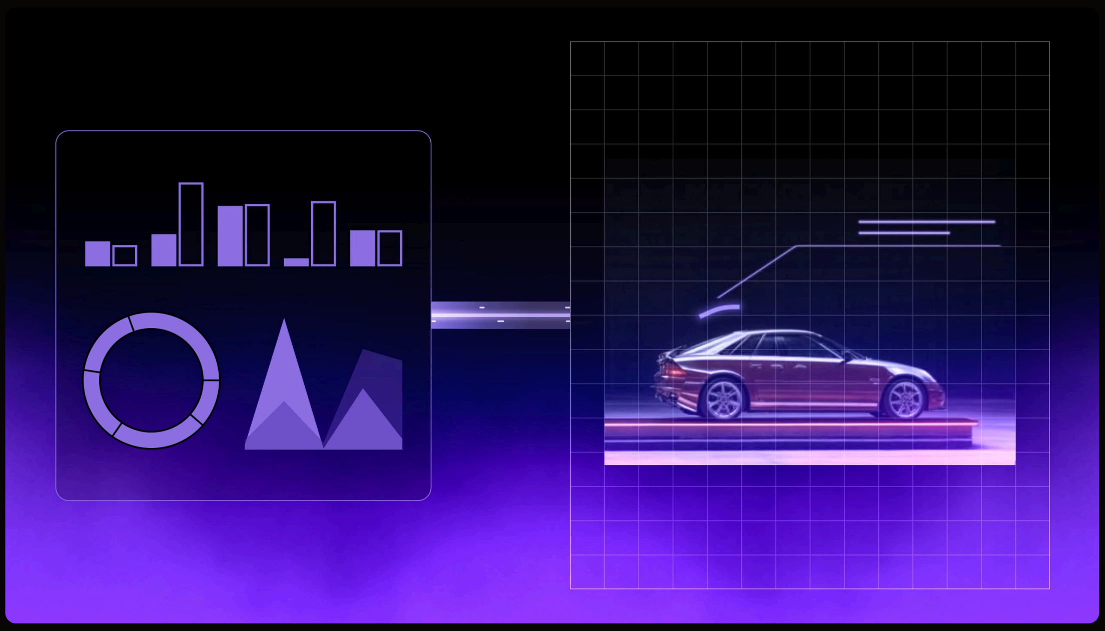
Protocol & Platform Support

Dispel's unique architecture enables communication across all 65,000+ TCP/IP protocols, in addition to commonly used ones like SSH, RDP, and VNC. It also provides native support for proprietary OT systems such as Rockwell FactoryTalk, Siemens TIA Portal, and Mitsubishi GS Works—ensuring seamless integration across complex, multi-vendor industrial environments.

2. Industrial Data Streaming

Simplify device-to-device transfer of real-time operational, diagnostic, and system data between industrial assets and cloud environments—enabling bidirectional and unidirectional flows to support predictive maintenance and streamline system updates for greater efficiency.

Secure, policy-controlled data streaming empowers industrial organizations to accelerate digital transformation and IT/OT convergence. By automating device-to-device communication—such as sensor data streaming, log extraction, supply chain alerts, and update management—teams eliminate manual bottlenecks, reduce overhead, and enable faster, safer integration between OT and IT systems.



Unlike traditional remote access tools, the Dispel Zero Trust Engine is the only platform that delivers intelligent, programmable data streaming—both locally and to the cloud. From enabling real-time analytics with AI models to streamlining global rollout of updates, Dispel turns raw OT data into a strategic asset. Organizations can perform consolidated backups, enhance ransomware recovery readiness, and deploy secure, programmatic services across sites—gaining unprecedented efficiency, improved resilience, and the ability to scale operational improvements across the enterprise.

Stream Critical Industrial Data Directly Into Your Cloud Environment

- **Data Export Files** – Transmit logs, reports, and other essential exports.
- **Vibration Data** – Enable real-time equipment monitoring and predictive maintenance.
- **Offsite Diagnostics** – Centralize fault diagnostics to accelerate issue resolution.
- **Supply Chain Logistics** – Improve operational visibility with real-time data flow.
- **WSUS Server Updates** – Securely automate patch and update management.
- **Custom Data Streams** – Adapt to unique industrial data needs with flexible architecture.

This solution integrates seamlessly with industrial data sources like PLCs, HMIs, SCADA systems, Windows directories (physical or virtual), and industrial sensors, making it ideal for energy, utilities, manufacturing, and other critical infrastructure sectors. Data can be securely transmitted to a variety of endpoints, including physical machines, local and cloud-based VMs, Azure Blob Storage, and modern platforms like Snowflake, ensuring compatibility with existing IT and OT environments. The Dispel Zero Trust Engine bridges the gap between incompatible systems, allowing for secure and reliable data transfer across different operating systems, file types, and formats.

Bidirectional and Unidirectional Data Streaming for Resilient Operations

Dispel Zero Trust Engine supports both bidirectional and unidirectional data streaming, giving industrial organizations the flexibility to securely share real-time data, perform diagnostics, and deploy updates, without compromising OT security or network isolation.

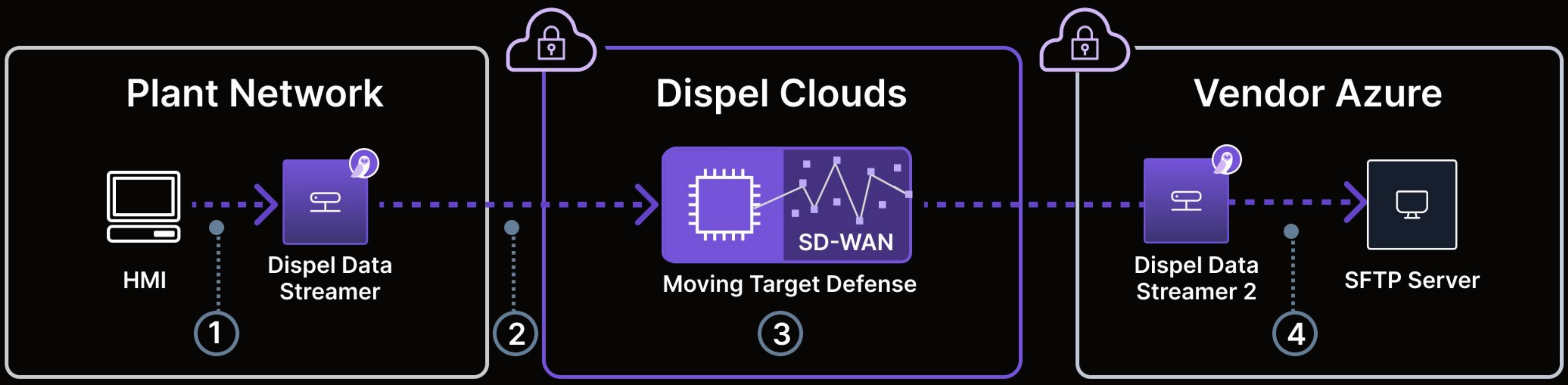
Unidirectional Data Streaming

Protects high-security or air-gapped environments while maintaining data visibility:

- Preserve intellectual property (IP) & Enable Analytics – Share data securely without exposing control systems
- Maintain Network Isolation – Meet strict compliance for sectors like nuclear or pharma
- Prevent Downtime – Eliminate inbound threats to safeguard critical production assets

Use Case 1: Stream On-Prem HMI Data to Azure for Data Analysis

A remote vendor in Europe needs data generated on an HMI in the US. The data must reach an internal SFTP Server running in the vendor's Azure network. Dispel forms the backbone for this data transfer by installing an on-premise data streamer in the US, a cloud data streamer in the vendor's Azure, and providing secure networking to connect the two endpoints.



1. HMI on the Plant Network pushes SFTP packets to the SFTP server, using Dispel Industrial Data streaming as the next-hop gateway.
2. Data Streamer proactively reach out to connect to the MTD Network, requiring no inbound firewall ports on either the Plant Network or the Vendor Azure.
3. Dispel MTD Network and Data Streamers automatically creates a unidirectional, encrypted pathway for traffic to route from the HMI to the SFTP server.
4. SFTP traffic reaches the SFTP Server in Vendor Azure securely, without requiring the HMI in the Plant Network to have direct internet access.

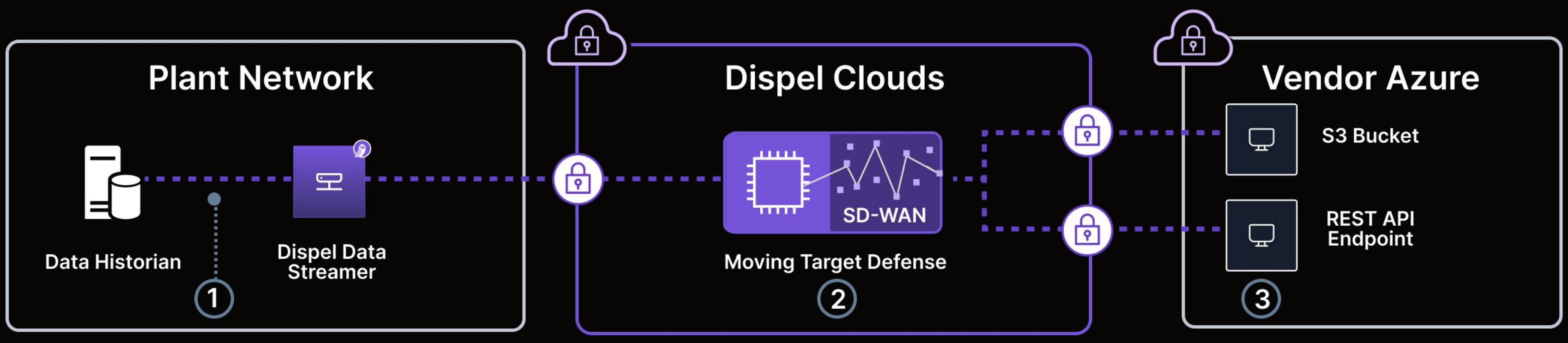
Bidirectional Data Streaming

Enables secure, real-time data exchange to support operational efficiency and uptime:

- **Vibration & Diagnostics** – Monitor assets continuously for predictive maintenance
- **System Logs & ICS Data** – Enable proactive issue detection and root cause analysis
- **Secure Updates** – Deliver authenticated patches to Windows, ICS, and firmware systems

Use Case 2: Extract and Stream Manufacturing On-Prem Historian Data to Amazon S3

A petroleum facility in the US has an on-premise data historian which records critical data that indicates when additional supplies will be needed. Selected data is streamed out to two endpoints: an Amazon S3 bucket, and a 3rd party proprietary REST API. Dispel proactively initiates this data transfer by pulling data from the historian, pushing the correct data payloads into their respective endpoints, and providing the secure network through which this data stream is achieved.



1. Dispel Industrial Data Streaming proactively pulls data from an on-prem Data Historian. Customer is able to input which data is sent where, and how often. Data Streamer then pulls the data, packages it into payloads (such as json blobs) as required, and pushes them through the MTD Network.
2. Dispel MTD Networks automatically create end-to-end encrypted pathways and securely route each payload to its intended destination. Payloads are pushed through separate nodes for each destination, preventing vendors or attackers from correlating data streams.
3. Data payloads reach their destination in the format and frequency as defined by the customer. Destinations can be any cloud storage bucket or REST API endpoint.

With Dispel Industrial Data Streaming, you can securely move critical data, monitor operations in real time, and optimize remote workflows, without exposing your network to risk. It's time to rethink remote access as seamless remote connectivity, built for the way you operate.

3. Integrated Threat Monitoring

Enable proactive, real-time detection, response, and recovery from OT remote access threats—seamlessly integrated into your cybersecurity ecosystem to strengthen visibility, resilience, and operational continuity.

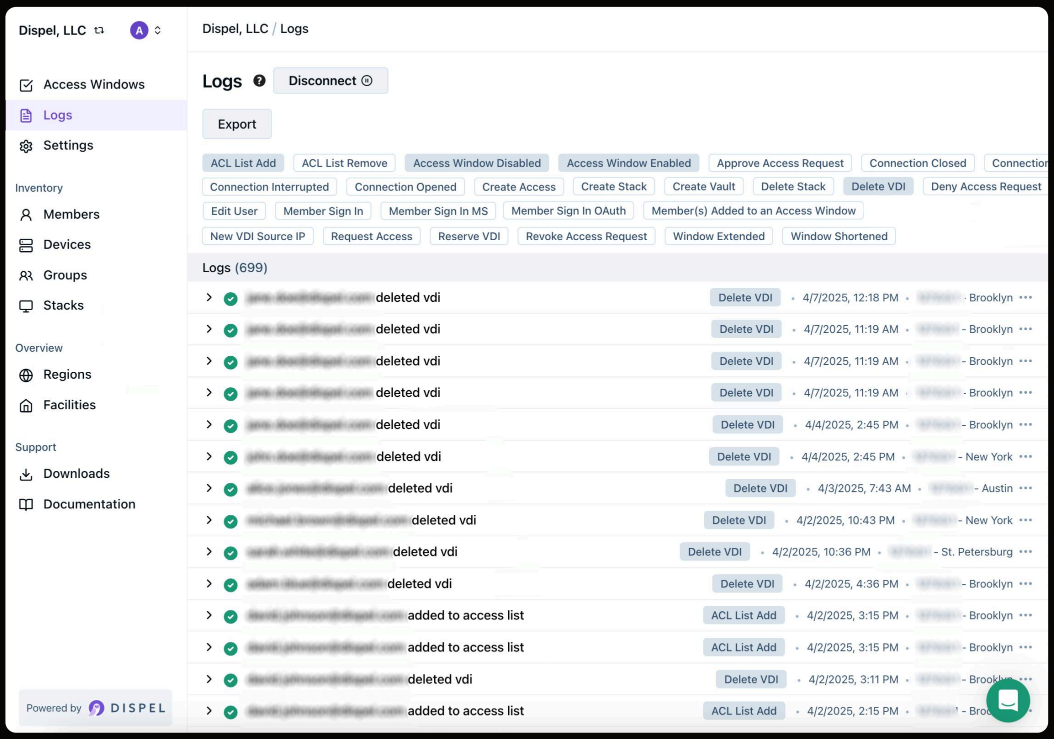
SIEM-Ready SOC Integrations

Dispel Zero Trust Engine integrates seamlessly with existing Security Information and Event Management (SIEM) platforms, enabling security teams to detect and respond to unauthorized OT remote access attempts in real time. Logs are curated to reduce transfer and storage costs, while preserving depth and integrity for threat monitoring and compliance.

Dispel provides immutable logs and automated backups to preserve a complete record of remote activity for forensic investigations and compliance. Network and application logs can be exported in Syslog, JSON, XML, Plain Text, or CSV formats, or forwarded to external systems, supporting flexible analysis, portability, and long-term retention.

Remote Session Visibility & Anomaly Detection

The Dispel Engine's network logging tracks all user activity, including dropped connection attempts, giving admins full visibility into when and how access was attempted. Within Dispel Virtual Desktops, event logging captures OS-level application, security, and system activity, enabling anomaly detection and continuous monitoring across OT sessions.



Logs (699)

```
[redacted] deleted vdi            Delete VDI    • 4/7/2025, 12:18 PM • [redacted] - Brooklyn
[redacted] deleted vdi            Delete VDI    • 4/7/2025, 11:19 AM • [redacted] - Brooklyn
[redacted] deleted vdi            Delete VDI    • 4/7/2025, 11:19 AM • [redacted] - Brooklyn
[redacted] deleted vdi            Delete VDI    • 4/7/2025, 11:19 AM • [redacted] - Brooklyn
[redacted] deleted vdi            Delete VDI    • 4/4/2025, 2:45 PM • [redacted] - Brooklyn
[redacted] deleted vdi            Delete VDI    • 4/4/2025, 2:45 PM • [redacted] - New York
[redacted] deleted vdi            Delete VDI    • 4/3/2025, 7:43 AM • [redacted] - Austin
[redacted] deleted vdi            Delete VDI    • 4/2/2025, 10:43 PM • [redacted] - New York
[redacted] deleted vdi            Delete VDI    • 4/2/2025, 10:36 PM • [redacted] - St. Petersburg
[redacted] deleted vdi            Delete VDI    • 4/2/2025, 4:36 PM • [redacted] - Brooklyn
[redacted] added to access list   ACL List Add  • 4/2/2025, 3:15 PM • [redacted] - Brooklyn
[redacted] added to access list   ACL List Add  • 4/2/2025, 3:15 PM • [redacted] - Brooklyn
[redacted] deleted vdi            Delete VDI    • 4/2/2025, 3:11 PM • [redacted] - Brookl
[redacted] added to access list   ACL List Add  • 4/2/2025, 2:15 PM • [redacted] - Bro
```

Managed SOC Advanced Monitoring Services

Dispel's managed security operation center (SOC) services strengthen your existing security operations by providing real-time detection, response, and investigation support for OT remote access. By aggregating network logs and security events across your environment, Dispel enables centralized event correlation and anomaly detection, without additional burden on your internal team.

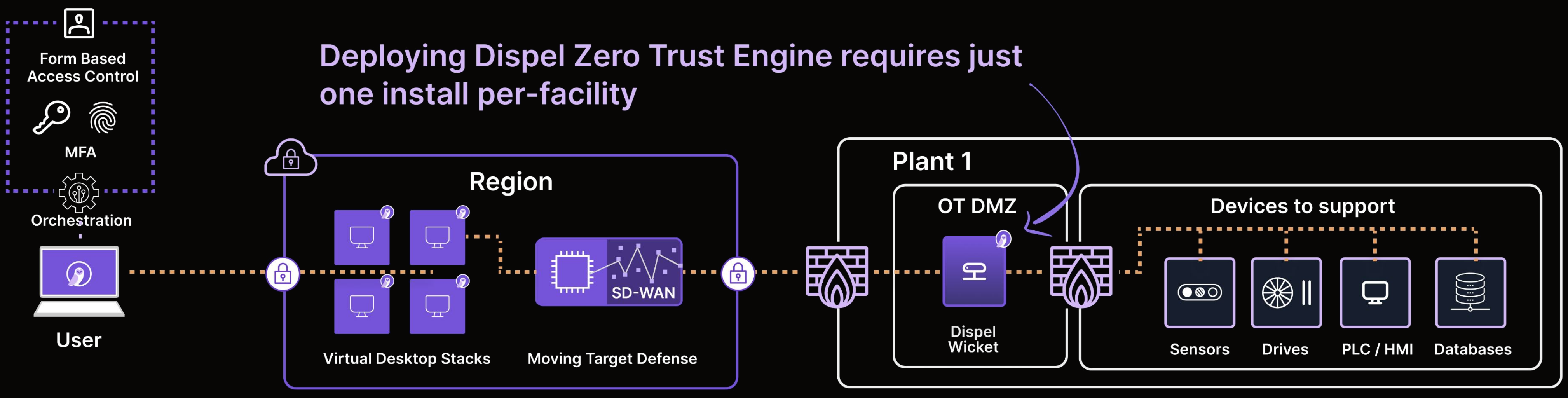
Session recordings and live playback give analysts full visibility into user actions, helping verify activity, support forensic investigations, and ensure compliance. With monitoring fully managed by Dispel, you gain expert-level oversight, deeper threat insights, and enhanced accountability, delivered as a service to empower your team and secure your OT environment.

Flexible Deployment Model

Deploy Dispel Your Way—SaaS, Private, or On-Prem

Dispel offers flexible deployment options to match your security posture, cloud strategy, and operational requirements—ensuring secure remote access without disrupting your infrastructure.

- **Dispel Cloud (SaaS):** A fully managed SaaS deployment that delivers scalability, security, and ease of use. Ideal for organizations that want turnkey remote access without the burden of infrastructure management.
- **Your Cloud (Private):** Deploy entirely within your own cloud environment for full ownership and control. Best for organizations with strict data governance or regulatory mandates. Seamlessly migrate from Dispel's cloud at any time.
- **On-Prem (Offline or Hybrid):** For organizations not ready to move to the cloud, Dispel's on-prem deployment delivers the same granular access controls and seamless connection workflows—fully offline. It's ideal for internal usage, IT/OT segmentation, and compliance-driven industries such as NERC-CIP-regulated power generation. Hybrid options are also available for organizations that require both internal and external remote access.



Deploying Dispel Zero Trust Engine requires just one install per-facility

Wicket Industrial Gateway

The Dispel Wicket is an on-premises edge gateway that connects industrial environments to the Dispel Zero Trust Engine—enforcing local security policies while enabling secure, scalable, and adaptable connectivity for OT secure remote access and industrial data streaming from devices to cloud services.

Deployment Options to Fit Any OT Environment

- **Virtual Appliance** – Virtual Appliance – Ideal for virtualized environments and cloud VPCs, with pre-configured Wicket (ISO, OVA, VHD, or container formats) for seamless, hardware-free deployment.
- **Small Hardware** – Compact and DIN-rail mountable; ideal for space-constrained or cellular-connected sites (e.g., OnLogic CL210).
- **Large Hardware** – High-performance, fanless units for industrial server rooms (e.g., OnLogic ML340g [2U], SEL 3350 [1U] with conformal coating for harsh environments).

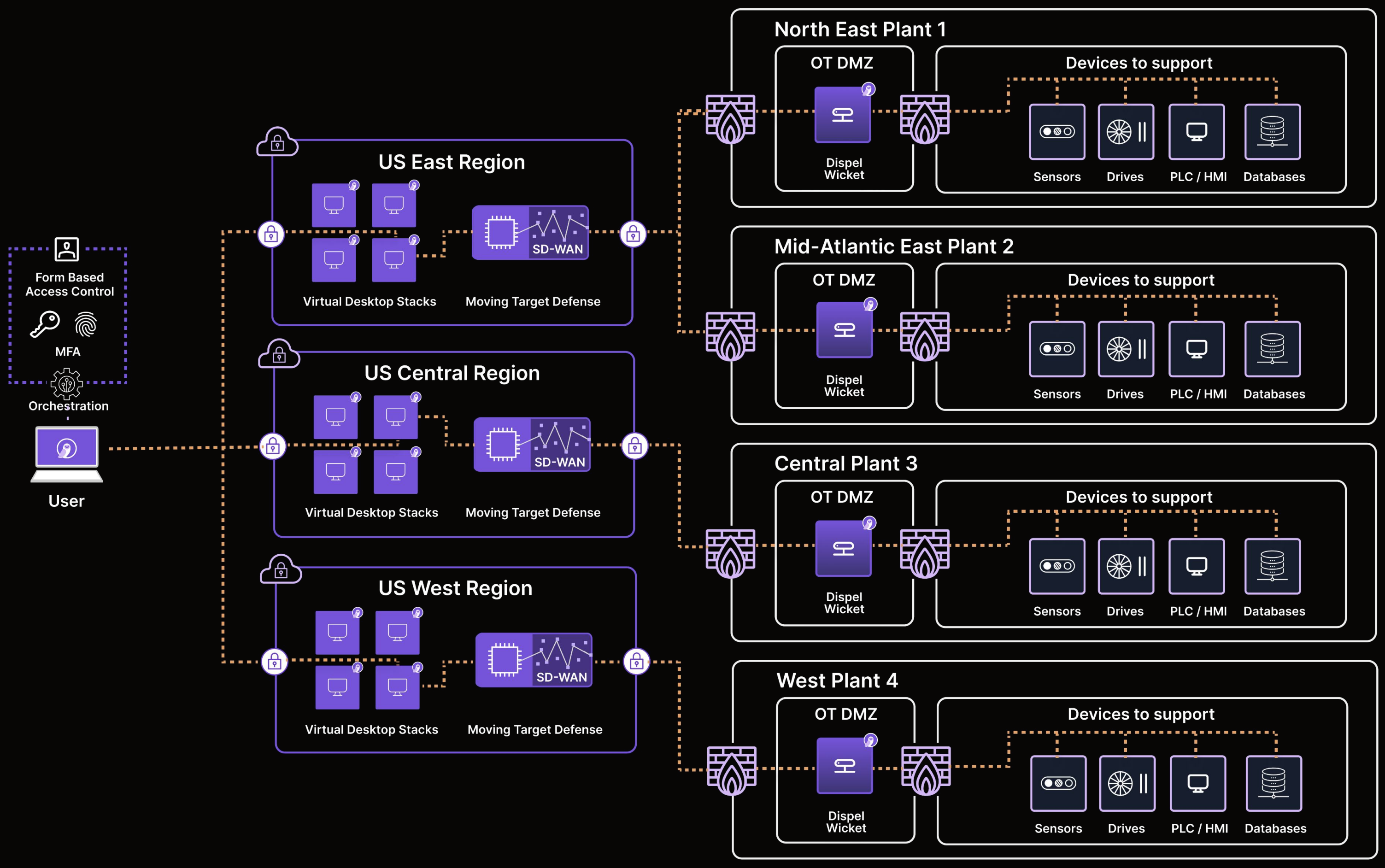
OT Secure Remote Access at Scale

Deploy at Scale in Hours, Not Months

Deploying remote access in OT environments often takes 6–12 months.

Dispel is different. Our flexible deployment models—SaaS, Private Cloud, On-Prem, or Hybrid—are purpose-built for OT environments and operational realities. Whether you're air-gapped or globally distributed, Dispel adapts to your architecture and security requirements.

We don't just drop off a box—we partner with your team from day one. Dispel handles onboarding directly, stays hands-on through deployment, and doesn't leave until the job is done. Dispel can deploy a site in under 3 hours and scale to 100 sites in under 90 days, ensuring fast time-to-value without sacrificing control or security.



OT Access at Enterprise Scale

The Dispel Zero Trust Engine is purpose-built to meet the size and complexity of OT environments—far beyond the limits of traditional SRA tools. It supports hundreds of thousands of access control rules, tens of thousands of endpoints, and thousands of users, operating seamlessly across globally distributed industrial networks.

From factory floors to remote facilities, maritime systems, satellite-connected sites, and rugged environments, Dispel delivers secure remote access wherever your operations are—at the speed and scale OT requires.

Only Dispel offers burst capacity access—spin up access for 100+ vendors in minutes, with no additional infrastructure required. Need to onboard a team of OEM engineers to update PLCs across multiple sites? With Dispel, it's a few clicks—not a months-long process of provisioning new jump hosts. Dispel makes large-scale OT operations agile, secure, and ready to connect.

Why Dispel

Dispel redefines how industrial organizations connect to OT. The Dispel Zero Trust Engine establishes a secure, scalable connectivity layer across all makes, models, and generations of equipment—enabling OT secure remote access, industrial data streaming, and integrated threat monitoring, even in the most complex environments. Dispel OTFusion accelerates digital transformation by standardizing data flows and unifying fragmented OT DMZs—maximizing operational efficiency.

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

Founded in 2015, Dispel pioneered network-level Moving Target Defense (MTD), holds 43+ patents, and today protects over $500 billion in manufactured goods annually while securing remote access for 54 million utility users worldwide. Trusted by global defense and industrial leaders, Dispel replaces outdated remote access tools with a modern platform built for industrial speed, scale, and resilience.

Defense is in our DNA. Learn more at dispel.com

Real-world impact. Proven at scale.

$42M

Annual OpEx Savings

A leading beverage manufacturer cut operating costs by $42 million per year by standardizing remote access with Dispel.

200+

Hours Saved Monthly

An oil & gas company eliminated 200+ hours of monthly IT workload, while securing $380M in new business.

10-Second

User Onboarding

A global food packaging manufacturer reduced onboarding time to just 10 seconds per user-streamlining admin operations at scale.

Ready to take the first step toward OT Secure Remote Access with Dispel?

Book a demo for a free 30-day trial today.

dispel.com/book

DISPEL

© 2025 Dispel, LLC All rights reserved.