Dispel and Nozomi Networks OT Security

Accelerate your Digital Transformation Journey through integrated OT/IoT Secure Remote Access and Comprehensive Network Visibility Solutions

In today's interconnected world, industrial control systems (ICS) and operational technology (OT) in critical infrastructure sectors such as manufacturing, electric utilities, oil & gas, and water/wastewater are increasingly targeted by cyberattacks. The rise in remote work and the expansion into distributed locations have made secure remote access (SRA) solutions essential. These tools enable operators, contractors and third-party vendors to remotely diagnose issues, apply updates, and monitor systems without requiring on-site visits, ensuring workforce productivity and operational continuity.

However, ICS/OT environments have unique requirements, protocols, and compliance constraints that traditional IT remote access solutions fail to address. Many times, organizations have turned to corporate VPNs and Jump Hosts to connect to OT devices, but these tools are costly to maintain and limited, as well as inadvertently expand the attack surface, exposing networks to potential intrusions and exploitation of trusted access.

To truly protect critical infrastructure remote access, organizations need purpose-built solutions that deliver complete asset visibility and security to reduce risk to the business, while simultaneously driving compliance and efficiency in ICS/OT environments.

Market Forces Driving Change

Digital Transformation
All organizations recognize the need to modernize to stay competitive in an evolving landscape.

IT/OT Convergence
Teams which have long been segmented need to work closely together to drive bottomline targets.

Internet of Everything
Juniper Research
83 billion IoT connections by 2024; 70% in Industrial sector

Threat & Risk Management
IBM Cost of a Data Breach Report 2023
The frequency, sophistication, and associated cost of cyber attacks continue to increase YoY to $4.45mm in 2023.

Joint Solution

Dispel and Nozomi Networks have partnered to deliver a flexible solution with on-prem and cloud-based options for asset visibility and secure remote access, purpose-built for ICS/OT networks. This integrated offering leverages Dispel's industry-leading Moving Target Defense (MTD) SD-WAN infrastructure to deliver unmatched security and fast, scalable access control tailored to your organization's unique requirements. By combining secure remote access, comprehensive asset visibility, advanced threat detection, and actionable operational and security insights, this solution enables organizations to protect their critical infrastructure while enhancing seamless operations.

The Dispel Zero Trust Engine delivers secure remote access and data streaming, purpose-built for ICS/OT to ensure compliance with critical standards like IEC 62443, NIST 800-82, and NIST 800-53. The Dispel Engine provides end-to-end encryption, micro-segmentation, multi-factor authentication (MFA), Identity and Access Management (IAM), granular access controls, isolated sessions, just-in-time access, and password vaulting.

The Nozomi Networks Platform empowers organizations to view and manage their security risk across all OT and IoT systems effectively, leveraging AI-powered analytics, real-time security alerts, user-defined risk scoring and benchmarking data. Network, endpoint, and wireless sensors provide flexible data collection options to generate comprehensive asset inventories, vulnerability data and security insights, even in the most sensitive industrial environments.

Joint Solution | Deployment Architecture

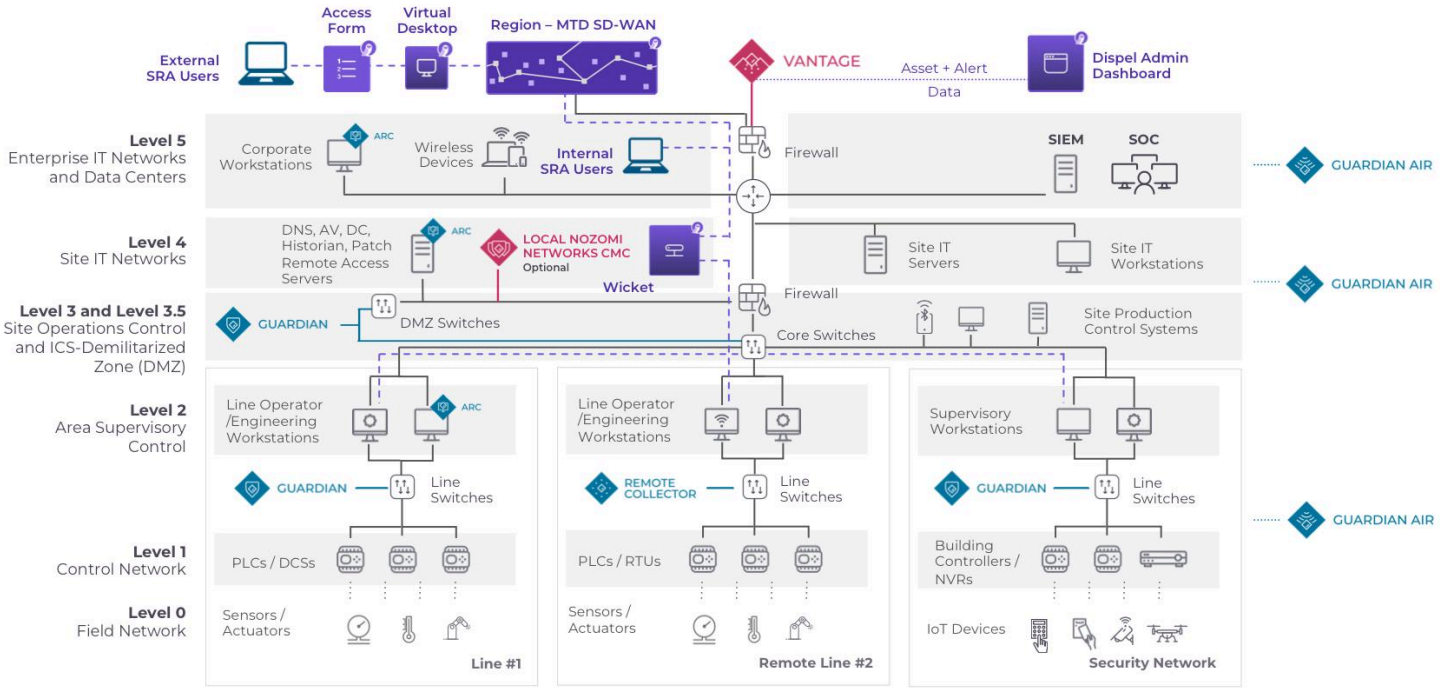

Diagram: A Purdue model logical representation of an integrated Dispel and Nozomi Networks deployment.

How it works: Discover with Nozomi Networks, Take action with Dispel

This cloud-to-cloud based integration is scalable to support all facilities. In under two minutes, an organization can easily synchronize OT asset inventory and management from The Nozomi Networks Platform with the Dispel Zero Trust Engine and begin to deliver remote access securely to those devices.

Administrators can seamlessly manage and monitor remote access connections across all facilities and systems. Asset and alert information on all OT, IoT, and ICS assets, such as PLCs, HMIs, and servers, including their ports and protocols, are synchronized to the Dispel Engine dashboard so administrators can easily choose from a list of possible remote connections to enable.

When deployed together, Nozomi Vantage™ establishes a baseline of normal device-to-device traffic patterns. During a secure remote access session, if a user demonstrates abnormal behavior, such as attempting unauthorized east-west traffic by initiating an SSH connection to another device, The Nozomi Networks Platform promptly alerts an administrator. Using the Dispel Zero Trust Engine dashboard, the admin can quickly terminate the session, preventing a potential attack before it escalates.

Joint Solution | Technical & Business Benefits

- **Reduce Business Risk**: Quickly detect and respond to unauthorized or anomalous behavior with enhanced asset visibility and robust policy enforcement.
- **Ensure Compliance**: Meet critical regulatory standards, including IEC 62443, NIST 800-82, and NIST 800-53.
- **Simplify Operations**: Streamline implementation, ports, and protocol configuration, reducing administrative overhead with scalable cloud-to-cloud deployment.
- **Accelerate ROI**: Achieve faster project rollouts, improving visibility and access control efficiency ahead of schedule.

Learn more about the partnership:
https://dispel.com/resources/integrations/nozomi-networks

DISPEL | NOZOMI NETWORKS

Book a demo today dispel.com/book