FORTINET

WHITE PAPER

# The Promise of SD-WAN Can Be Realized in OT Environments

## Executive Overview

**Digitization of operational technology (OT) is driving the importance of maintaining solid connections to the internet and cloud. Software-defined wide-area networking (SD-WAN) is emerging as one potential solution for replacing slow and expensive traditional WAN infrastructures. But as internet-connected information technologies (IT) increasingly merge with OT, organizations must address the need for greater visibility into all distributed operations, remote deployment, and easier management of solutions. Perhaps most critical of all, however, is enhanced security controls to protect against a rising tide of OT-specific attacks.**

## IT/OT Convergence Brings New Capabilities and Risks

In the industrial, manufacturing, and critical industry sectors, OT systems are increasingly converging with IT technologies to enable new efficiencies and capabilities. But this growing intersection is creating a need for new tools and solutions to address the altered nature of OT.

Digitization brings greater complexity and risk exposure to OT-connected organizations. As a result, OT managers now need a holistic view of the organization's extended network infrastructure. A majority (78%) of organizations today have only partial centralized visibility of their OT environments.[1] Without full visibility, any parts of the infrastructure that cannot be seen also cannot be protected.

As a result of widespread IT/OT convergence, the "air gap" that kept OT systems secure through isolation is nearly gone. This means any threat capable of a successful IT breach now has a pathway to vulnerable and potentially valuable targets on the OT side. Adversaries can penetrate organizations on a north-south axis (from outside to inside OT environments) as well as move laterally across the organization on an east-west axis. Without visibility tools to immediately spot intruders, damages tend to compound. The time from an attacker's first action in an event chain to the initial compromise of an asset is typically measured in minutes—while the time to discovery is more likely to be months.[2]

Organizations also need new infrastructure that can perform double duty across both IT and OT environments—in order to simplify operations, training, and reporting while reducing overall costs. Infrastructure complexity of adding disparate tools and products from different vendors not only adds higher capital expenditures (CapEx) but it also increases deployment, management, and monitoring burdens on limited staff resources. This raises operating expenses (OpEx) as well.

## Traditional WAN Connections Carry High Costs

Costs are an ongoing issue with most OT organizations—and existing WAN infrastructure offers an opportunity for savings. Traditional WAN relies primarily on expensive multiprotocol label switching (MPLS) or satellite connections. To maintain centralized control and visibility, traffic is backhauled to an on-premises data center—which can impact performance due to security bottlenecks.

SD-WAN has become a popular way to connect remote locations for corporate enterprises. SD-WAN uses a variety of commodity internet connections such as Long-Term Evolution (LTE), digital subscriber line (DSL), or cable to replace MPLS/satellite links at significant

**Experts predict increasing attacks against critical infrastructure: botnets mounting distributed denial-of-service (DDoS) attacks against OT networks; attacks on manufacturing systems that use cloud services; supply chain attacks where third-party vendors are compromised as springboards for threat actors to target critical sectors.[3]**

## The Unique Physical Needs of OT

OT organizations operate in all kinds of environments, and in sites of all kinds of sizes—from large campuses with air-conditioned buildings to small installations in remote locations without any carpeted spaces. Some environments can be prohibitively harsh for normal IT gear due to extreme physical conditions, such as:

- Electrical substations
- Oil rig platforms
- Factories
- Hydroelectric plants
- Warehouses/distribution centers
- Airports
- Ships

cost savings. To ensure application performance and user experience, SD-WAN manages traffic routing based on performance (e.g., latency, jitter) and connectivity costs to deliver a reliable, high-quality connection.

Broad SD-WAN adoption in enterprise organizations suggests that OT environments will be next, once gear that meets the needs of OT environments exists. That starts with ruggedized SD-WAN equipment designed for industrial, manufacturing, and critical infrastructure environments—situations with demanding environmental conditions (e.g., oil rigs, electrical substations, assembly lines, maritime cargo).

SD-WAN solves several OT challenges at the same time, including rapid deployment, fast connectivity to cloud applications, and unified management to reduce IT overhead.[4] It can also improve productivity. Users on-site who connect to a cloud service (e.g., Microsoft 365, Oracle Cloud, or applications in AWS) in a multi-cloud architecture can have access directly from the location. This can provide lower latency and a far better user experience than connecting to the internet via a central data-center firewall.[5]

## The Question of SD-WAN and Security

The security implications of direct access to cloud and internet resources can potentially have even greater impact in an OT environment than they would in a typical SD-WAN deployment.[6] Shifting from traditional WAN to SD-WAN adds additional risk exposure, since internet-connected traffic is no longer backhauled to a data center for centralized security checks. Unfortunately, most SD-WAN products are based on routing technology—designed primarily to look for the best connectivity path for traffic. Most SD-WAN solutions on the market today do not offer built-in security.

Any increase in OT vulnerability is a serious issue, since these industries are facing an onslaught of targeted attacks. The vast majority (90%) of organizations experienced at least one OT system intrusion in the past year—and 65% had three or more.[7]

OT outages or disruptions caused by an attack can have a huge impact on productivity, efficiency, and even safety. Malware attacks are now specifically being designed to target vulnerable industrial control (ICS), supervisory control and data acquisition (SCADA), and safety systems.[8] This risk exposure includes critical infrastructure (e.g., hydroelectric dams, nuclear power plants, oil, and gas pipelines)—where a successful breach can directly impact human lives or the environment.

Industrial networks require protected and prioritized connectivity to control centers and cloud applications. Smart sensors based on Industrial Internet of Things (IIoT) and Internet-of-Things (IoT) communication protocols like Open Platform Communications Unified Architecture (OPC UA), Message Queuing Telemetry Transport (MQTT), and Hypertext Transfer Protocol (HTTP), among others, must be secured. The transfer of telemetry and control information from the process control network to the corporate IT network or across the internet may use inherently insecure protocols such as Modbus, BACnet, or SafetyNET. These must be placed on different segments and inspected, prioritized, and protected. A typical SD-WAN solution offers none of these critical security capabilities.

### Remote Deployment, Management, and Monitoring

Another key problem of adapting SD-WAN to OT environments comes from the common need to implement these technologies at remote locations, which can be challenging because these sites often have limited or no technical personnel.[9] In remote deployment situations, the SD-WAN solution needs coherent security policies that protect the site from the very first moments the system is up and running.

## The Unique Physical Needs of OT (contd.)

Locations such as the above require specialized electronic equipment that can function within common OT environmental conditions, such as:

- Temperature extremes
- Moisture
- Extreme or constant vibration
- Electromagnetic interference (EMI)
- Small spaces for equipment
- Operations that use different types of power (beyond 110V or 220V)
- Certified for the different OT industry regulations

**The worldwide SD-WAN market is forecasted to grow 168% through 2024 and surpass $3.2 billion.[10]**

**Cyber criminals are maximizing their opportunities by simultaneously targeting both older OT vulnerabilities as well as new ones that appear on an expanding attack surface.[11]**

In addition, the organization's security operations center (SOC) needs centralized visibility to each and every site to monitor threat levels, manage the gateways between the IT and OT networks, and quarantine systems found to be infected in order to limit malware propagation.

## The Need for a Reliable, Secure, and Cost-effective SD-WAN for OT

As cyber criminals of all sorts (from hacktivists, to nation-state attackers, to organized crime syndicates) increasingly seek to disrupt or damage OT systems for their own objectives, organizations need to maximize the benefits of digitalization while minimizing the new risk exposures these technologies introduce to their sensitive environments.

Productivity and cost savings are critical drivers for any business. But industries that rely on OT systems cannot afford to place either of those above the safety and security of their operations. The increased risk exposure that direct internet connections bring into OT environments requires SD-WAN with integrated security, centralized visibility, and remote management capabilities. Further, to apply the benefits of SD-WAN to modern industrial environments, it will take ruggedized solutions natively designed for the unique physical demands of OT deployments.

[1] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, June 30, 2020.

[2] "2019 Data Breach Investigations Report," Verizon, April 2019.

[3] Bruce Sussman, "15 Cyber Threat Predictions for 2020," SecureWorld, December 12, 2019.

[4] Nirav Shah, "SD-WAN: More Than A Retail Solution," Network World, July 15, 2020.

[5] Joe Robertson, "What Manufacturing CISOs Need to Know About SD-WAN," LinkedIn, December 20, 2019.

[6] Nirav Shah, "SD-WAN: More Than A Retail Solution," Network World, July 15, 2020.

[7] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, June 30, 2020.

[8] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 8, 2019.

[9] "SD-WAN Isn't Just for Retail," Fortinet, April 3, 2020.

[10] "SD-WAN Market Expected to Increase 168 Percent by 2024," BBC Magazine, July 8, 2020.

[11] Derek Manky, "Operational Technology: Why Old Networks Need to Learn New Tricks," Dark Reading, December 31, 2019.





November 18, 2020 7:21 AM

D:\Fortinet\White Paper\Red White Paper\SD-WAN for OT\wp-FA-the-promise-of-sdwan-can-be-realized-in-ot-environments-11172020

839530-0-0-EN