

A FORTINET POINT OF VIEW

SD-WAN Isn't Just for Retail

An Important Technology for Critical Industries

In any organization, being responsible for cybersecurity is a complex job entailing interactions with the teams managing software development, servers, databases, storage, and networking. It becomes even more challenging where there is also a need to protect industrial installations and the Operational Technology (OT) that runs them in critical industries such as manufacturing, energy, and extraction.

Although it is not always on the OT security team's radar, in the IT networking world Software Defined Wide Area Network, or SD-WAN, is the hot topic right now and it is just as applicable to the world of OT. However, SD-WAN has major security implications which might have even greater impact in an OT environment than they would in a typical SD-WAN deployment

The concept behind SD-WAN is to reduce the cost of connecting branch offices and remote locations by using relatively inexpensive broadband internet access as either a partial or complete replacement for expensive private WAN technologies such as MPLS. This is an excellent solution for reducing overall networking costs and managing traffic flows. However, it raises security issues because now tens, hundreds, or thousands of sites are directly connected to the internet. Although this allows organizations to add more bandwidth inexpensively and users at those sites to have direct and high-quality access to internet-based resources, it also exposes them directly to incoming attacks from the internet.

In manufacturing, remote sites are not simply offices. They range from huge plants with hundreds of machines and thousands of workers to small remote locations such as automated oil or gas wells. Or anything in between. They are crucial to the business because they produce what the business sells. They don't support the business, they are the business. No product, no business.



Key Points

- SD-WAN is an important networking technology that can provide substantial cost benefits
- It connects remote sites, including industrial and manufacturing locations, to corporate applications and to the internet
- Sites with internet connections are exposed to cyber criminals attacking IT assets and Operational Technology such as Industrial Control Systems
- The solution is Secure SD-WAN, with advanced cybersecurity protection that is built-in not added on
- Fortinet SD-WAN and FortiGuard Industrial Security Service combine to provide the most advanced connectivity and protection available for manufacturing and critical industries

Cost Savings, But At What Price?

Replacing (or reducing) expensive private connections with internet access at all of those sites saves money. It can also improve productivity because users onsite who connect to a cloud service (Microsoft Office 365, Oracle Cloud, or applications in AWS, for example) can have access directly from the location rather than traversing the corporate backbone network. This provides lower latency and a far better user experience. But these advantages are not without downsides. Security tools in the data center such as firewalls, IDS/IPS, URL filtering, or even antivirus are useless at remote factories directly connected to the internet. In addition, as IT and OT networks converge, the OT environment is no longer protected by the air gap of the past, leaving these Industrial Control Systems vulnerable to malicious actors trying to access them from the IT side of the house. Preventing attacks not only ensures that production continues as usual, it also protects the safety and reliability of the plant and its workers.

Most SD-WAN offerings are adequate at providing mechanisms to determine the best path, route the traffic, and prioritize higher-value traffic over lesser flows. However, because these products are usually based on routing technology, security is an afterthought, if it is thought of at all.

The Solution: Secure SD-WAN

Which is why, from the point of view of cybersecurity, SD-WAN does not go far enough. What is required is Secure SD-WAN, where the traffic control is integrated with security features like next generation firewall (NGFW) advanced threat protection, application inspection, IPS, URL filtering and botnet protection. In industries that rely on OT, the capabilities and protections that Secure SD-WAN provides to the IT environment can be extended into the OT space and can provide an extra level of security beyond what may already exist in an IT/OT gateway.

Implementation of technologies such as SD-WAN, much less Secure SD-WAN, at remote locations can be challenging because these sites often have limited or no technical personnel. This problem can be solved with zero-touch provisioning tools, which are available with many (although not all) SD-WAN solutions. But that isn't enough from a security point of view: in addition to route selection, coherent security policies are a must in order to protect the site from the very first moments the system is up and running. In addition, the centralized Security Operations Center needs 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. One example of a secure SD-WAN solution is provided by Fortinet's FortiGate Next-Generation Firewall, which combines Advanced Threat Protection, IPS, Anti-virus, Application Control, URL Filtering, VPN and native SD-WAN functionality with advanced OT protocol inspection and security. To complete this robust security posture, Fortinet's Secure SD-WAN solution is supported by threat intelligence from FortiGuard, Fortinet's threat intelligence arm. FortiGuard ensures that the different security capabilities are keep up to date, continuously and automatically.



Threat Intelligence Specifically For OT

OT/ICS systems are no more immune to attacks than IT systems, and older implementations are substantially more vulnerable than newer ones. Fortinet's FortiGuard Industrial Security Service is specifically designed to support ICS environments. This service continuously updates signatures to identify and police most of the common ICS/SCADA protocols, providing security staff with granular visibility and control. This service can provide vulnerability protection for applications and devices from the major ICS providers. This combination results in highly sophisticated application control of the traffic between zones and enables the FortiGate NGFW to detect attempted exploits of known vulnerabilities.

What this all means is that the cybersecurity team must actively take part in any SD-WAN decision. This is true in any industry, but especially in manufacturing, where OT system vulnerabilities can lead to costly production downtime or worse. A truly secure SD-WAN solution will not only provide WAN savings, it will furnish a single cybersecurity approach that reduces complexity and extends needed visibility and control deep into both the IT and the OT network.

