CHECKLIST

Choosing an SD-WAN Solution for Operational Technology Environments: 5 Requisite Capabilities

Operational technology (OT) industries are rapidly undergoing digital transformation just like other organizations. However, the nature of OT environments means they will require security and networking features that IT-only environments may not. Locations may be remote and/or require equipment that can stand up to unusual environmental conditions. Nonetheless, distributed OT assets need to be connected to the enterprise in a safe, reliable, and cost-effective manner.

With a software-defined wide-area networking (SD-WAN) solution designed for OT, organizations can achieve:

- Lower total cost of ownership (TCO)
- More reliable connectivity and better user experience
- Reduced complexity and improved efficiency
- Increased bandwidth

Top Five Requirements for SD-WAN in OT

While SD-WAN offers connection reliability benefits that support new digital innovations, few SD-WAN solutions offer consolidated networking and security features optimized for industrial environments. When evaluating SD-WAN solutions, look for the following capabilities.

☑ Compatible with OT protocols

SD-WAN solutions deployed in OT environments must be able to communicate using the protocols found there. An appropriate solution will be compatible with the industrial protocols found in that environment. Look for a solution that fits naturally to avoid the complexity of having to add and string together multiple disparate products.

☑ Management flexibility and zero-touch deployment

Given that OT locations rarely have a dedicated security team, flexible management options and zero-touch deployment (ZTD) are key.

- **Management flexibility:** Avoid solutions that require always-on cloud management and won't work if the connection goes down. An ideal solution will provide management capabilities from different environments such as the enterprise, the cloud, or even the SD-WAN device itself. This lets each OT operator integrate SD-WAN with their own operating mode and regulatory constraints.
- **ZTD** can drastically reduce the amount of time it takes to deploy SD-WAN. ZTD enables a device to be plugged in at a remote location and then automatically configured at the main office via broadband connection. This reduces the need for security expertise at remote OT locations.

☑ Self-healing WAN and application prioritization

Connectivity alone isn't enough, especially in a remote work-heavy environment.

- **Self-healing WAN.** Many SD-WAN solutions only support limited use cases, limited numbers of users, and/or specific environments. To be effective, a solution needs to identify a broad set of applications to meet all use cases. Self-healing connection capabilities through adaptive WAN remediation make the application experience much more resilient. This advanced self-healing WAN automation will provide consistent user experience on any transport for any user.
- **Application steering.** Application steering ensures that applications are routed along the best path required to meet specific parameters or service-level agreements (SLAs), taking into account latency, jitter, and bandwidth, among other variables.

☑ Integrated security

SD-WAN without built-in security introduces great risk when connecting directly to the internet. Further, when the WAN layer and the security layer reside in two separate products, there are more opportunities for misconfiguration and nonoptimized performance. Nonintegrated solutions lead to security gaps and increased complexity across the WAN, security, routing, management, and possibly even intrusion prevention systems (IPS).

A secure SD-WAN model builds enterprise-grade security directly into the connection with firewalls and virtual private network (VPN) functions. They may also include encryption, IPS, antivirus, and sandboxing. Only with secure SD-WAN can networking, connectivity, and security functions be tightly integrated into a unified platform to meet the full range of secure connectivity needs.

Finally, the SD-WAN solution should be able to block known OT vulnerabilities.

☑ Ruggedized hardware

OT environments sometimes require rugged gear to withstand conditions such as extreme temperature, vibration, and electromagnetic interference. Limited space and power sources are also considerations. Look for a solution that can withstand harsh physical conditions and extend the benefits of SD-WAN to the edges of the operation.

Secure SD-WAN Reduces Costs and Risks for OT Organizations

For industries that depend on OT control systems, a secure SD-WAN solution can provide an extra level of protection. A truly integrated solution not only provides WAN improvements and savings but also furnishes a single cybersecurity approach that reduces complexity and prevents the exploitation of OT vulnerabilities that lead to costly production downtime.

FORTINET

www.fortinet.com

April 7, 2021 9:42 AM

D:\Fortinet\2021 Rebranded templates\Checklist\April\SD-WAN OT\cl-FA-sdwan-solution-for-ot-environments-472021\cl-FA-sdwan-solution-for-ot-environments-472021

952208-0-0-EN