FORTINET

CHECKLIST

Top 6 Considerations for Implementing Zero Trust in OT Environments

The zero-trust security model is often part of corporate security strategies, but including zero trust in operational technology (OT) environments tends to be deferred or ignored due to production, infrastructure protection, and personnel safety priorities.

Today, the convergence of IT and OT networks means that ever-evolving cyberthreats now have easier access to previously air-gapped OT environments. So, the need to apply a zero-trust cybersecurity model to OT has become increasingly important. Zero trust provides additional security by continuously verifying the trustworthiness of users and devices.

When deploying zero trust in OT environments, make sure to take these six key considerations into account.

☑ **Identify Barriers**

OT networks are often older and more diverse than IT networks, with industrial spaces built upon automation vendor solutions and system integrators, so you need to identify any barriers to implementing zero trust. Find out if the warranty language of any current automation vendors restricts or limits what can happen on the network.

☑ **Verify Compatibility**

Assessing whether OT networks and devices can support zero trust is critical, particularly given that industrial control systems (ICS) can have 20-year life cycles. Determine if the new technology is compatible with the legacy technologies found in your OT environment. Much of the ICS/OT technology stack has no user interface, and IP addresses are often static, so make sure your zero-trust solutions can support these “headless” OT components.

☑ **Manage Passwords and Active Directory**

Because OT environments have historically been air-gapped, they sometimes rely on static passwords rather than those managed in Active Directory with secure credential management policies. Make sure your new solutions can address any static password challenges.

☑ **Evaluate OT Protocol Support**

Some OT components, such as programmable logic controllers and human-machine interfaces, may not support the technologies or protocols required to fully integrate with zero-trust implementation. In some cases, zero trust may not be practical for certain OT devices or systems.

☑ **Verify Safety and Operational Boundaries**

Some ICS technologies within the OT environment may be designated for safety operations and require timely and uninterrupted access to systems to execute safety functions. Verify that zero trust support for these ICS elements won’t impede the safety aspects of the infrastructure. The nuances of OT environments can be complex, and skilled security operators can be scarce, so look for solutions built specifically for OT that can work seamlessly with their IT counterparts to support time and safety constraints.

☑ Look for Consolidation and Convergence Opportunities

When considering options, look for opportunities to consolidate vendors and determine if solutions can span IT and OT networks. For example, the Fortinet OT Security Platform includes zero-trust and supports single-vendor consolidation.

Fortinet Solutions for OT

Once you have identified zero-trust barriers and limitations, you can begin deploying Fortinet OT-specific solutions, such as FortiPAM privileged access management with secure remote access, FortiAuthenticator multi-factor authentication, and FortiToken with FortiNAC and network access controls for OT, which has built-in OT protocol support to enable zero trust for unique OT devices. All of these Fortinet solutions are part of the OT Security Platform, an extension of the Fortinet Security Fabric, which naturally converges IT and OT.

April 9, 2024 8:56 PM

2637224-0-0-EN