Title:

Embracing Zero Trust: Verification, Visibility, and Validation (Blog 1 of a 7-blog series)

Author

Andrew BOHAN, Global IT Security Director, Assets, Vulnerability & Incident Response, Schneider Electric
David GALLET, Digital Risk Leader, IT & OT Security for Industrial Sites, Schneider Electric

Text

Intro

In a recent blog[1], Schneider Electric shared its view on the importance of extending zero trust beyond IT environments into operational technologies. We also shared our seven Cyber Assurance Principles which embody our execution of zero trust within our company. Now, through a seven-part series, we want to provide a real-life perspective on how we practically and continuously apply zero trust through these principles, starting with our first principle: **continuous verification, visibility, and validation**.

For this Cyber Assurance principle, zero trust means that Schneider Electric assumes the users and devices in our IT and OT environments may be potential threats or are vulnerable and at risk of a cyber security incident. We therefore assure the authenticity of the users and validate the devices they are using by verifying their security posture on a continuous basis.

We start with visibility as an obsession

What does being obsessive about visibility look like in a global organization that has hundreds of facilities and tens of thousands of people and devices around the world? We understand that we cannot verify and validate — or protect — what we can't see.

To ensure we have visibility into our own assets and systems, we have technologies, foundational principles, and processes for inventorying the systems and devices used in our IT and OT infrastructures so we may see them and properly protect them. As one might imagine, this is a complex task for an organization of our size, as no one single data source can provide us with everything we need to know about what's on our network. Therefore, to build a complete picture, we use multiple data sources from a wide array of sophisticated IT and OT cybersecurity tools throughout our organization.

[1] https://cybertechaccord.org/from-it-to-ot-extending-zero-trust-principles-for-greater-resiliency/

As an illustration, we scan and inventory the devices on our global IT networks continuously to check for new people and devices and identify them via digital fingerprinting. We also employ asset lifecycle management so that with the proper onboarding and offboarding of our assets, we can ensure higher data quality and improve the accuracy of our inventory which ultimately enhances security, software licensing, and finance.

Extending IT and OT visibility throughout the organization

To extend visibility across our organization, we utilize a discovery and inventory capability that aggregates disparate data from all our inventory tools into a single pane of glass for a holistic view of our assets. This allows us to democratize the data, making it accessible to all our teams, including our global security executives. These executives are responsible for the implementation of our security policies in various geographies, operations, and business units.

The aggregated data provides us with a comprehensive baseline of our assets so we can proactively secure and protect them. For instance, our Security Operations Center (SOC) can use this data to enrich incident response activities. Data can also be used to determine if we have devices that are non-compliant with our internal policies.

Extending visibility to OT

For our OT security, we use some of the same IT tools and data for inventorying assets and detecting threat issues or suspicious activities. In addition, we perform vulnerability scans on our OT assets on a regular basis. Any new manufacturing machines are validated to ensure they comply with a cybersecurity framework for industrial sites that aligns with the key tenets of the IEC/ISA 62443 suite of standards for cybersecurity. When an OT asset does not comply, we employ a “ring-fencing” security protocol to ensure non-compliant machines cannot connect to the internet.

Without this obsession with visibility, our IT and OT cybersecurity teams would be forced into guesswork due to a lack of understanding of our basic asset inventory.

The future: Linking asset management to risk profiles

One of our future goals in the planning stage is to build a data-driven approach that would automatically add context to who is using an asset, where it is being used, and for what purposes. This approach would also assign a level of risk to the person, the asset, and the usage. For instance, is it a VIP, a customer-facing machine, an OT lab, or it a third-party contractor in an R&D lab? That level of context enhances our visibility and strengthens our security posture.

One last thought: Strong security fundamentals are critical

At the end of the day, foundational governance is sometimes more critical than anything else, as other larger endeavors will fail without it. One thing we like to keep in mind is that there are core cyber security practices which can have a big impact. For instance, basic hygiene is highly important. Discovering something as simple as machines that are missing an antivirus tool can prevent a major, costly incident. Yes, we keep rolling out large strategic projects, but we make sure we take care of the basics too.