FORTRA®

DATASHEET (TRIPWIRE)

NERC CIP-013 Compliance

Supply Chain Risk Management with Fortra's Tripwire

More attention is being paid to risks around the supply chain in the bulk electricity system (BES). When third-party vendors introduce new products, software and personnel into a power supplier's environment, the potential for new cyber risks increases.

For this reason, the North American Electric Reliability Corporation (NERC) recently added a new set of requirements to its Critical Infrastructure Protection (CIP) standards: CIP-013 Supply Chain Risk Management.

The energy sector is normally mandated with meeting the minimum level of security described in NERC CIP standards. Now, with the introduction of CIP-013 they'll need to provide evidence for controls around managing risk—specifically focusing on the myriad vendors and products within their supply chain. Vendors help energy utilities perform at their best, but vendor access to sensitive systems and information poses serious potential threats.

NERC CIP-013 enforcement began in 2020. Though utilities have to categorize their systems and sites in terms of the impact they have on the bulk electric system in terms of high, medium or low impact, the CIP-013 requirement only applies to high- and medium-impact systems.

How to Align with NERC CIP-013

Essentially, the three mandates of the new CIP-013 requirements are to have a plan, implement that plan, and periodically review it.

For creating and implementing a plan, the requirements essentially either involve communication or coordination between the utility and vendor, or there is some level of technical control in place around verifying software packages prior to introducing them to the protected environment.

For the first part, Tripwire is seeing a few instances of utility customers asking for language in our services contracts to formalize communication and coordination. Again, it seems there are not enough examples to point to any specific emerging language or approach. There are probably many instances of utility/vendor pairs working on language, and in the long run it will be helpful for all to support convergence.

NERC CIP-013 PURPOSE

To mitigate cybersecurity risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

What CIP-013 is Not

While NERC doesn't give prescriptive guidelines on how to fulfill CIP requirements, it's worth clarifying potential misinterpretations of CIP-013:

- It's not a requirement to stop using appliance-based products. An appliance should not, however, be treated as a magical approach that mitigates the weaknesses of any subcomponents.
- It's also not a prohibition on using open source software, as it is possible to verify open source software authenticity and integrity just as with commercial off-the-shelf software.

As for the technical aspect of the control, approaches are still emerging as well. For instance, utility customers have expressed interest in Tripwire capabilities around automated hash confirmation of OS patches. There is also the capability to include in monitoring scope any binaries or similar critical files to be whitelisted against their hashes.

Organizations Trust Tripwire for NERC CIP Compliance

Tripwire has helped registered entities achieve and maintain NERC CIP compliance since 2008. This has allowed Tripwire to develop a team of consultants well versed in NERC CIP compliance and the product extensions and CIP-specific content now embedded in the Tripwire NERC Solution Suite.

As a recognized leader in solutions for IT and OT security and compliance, Tripwire has extensive experience helping customers automate compliance for numerous standards across almost any device, platform and system.

With the Tripwire NERC Solution Suite, electric utilities have a comprehensive solution — from products to customized extensions and content and expert consulting — to help them automate and simplify NERC compliance.

By meeting NERC compliance, these companies take important steps towards securing their IT/OT systems against inadvertent misuse and intentional, malicious attacks. In turn, these secure systems help these companies ensure the reliability of North America's bulk electric system.

Further reading: Tripwire NERC Solution Suite solution brief

FORTRA®

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.