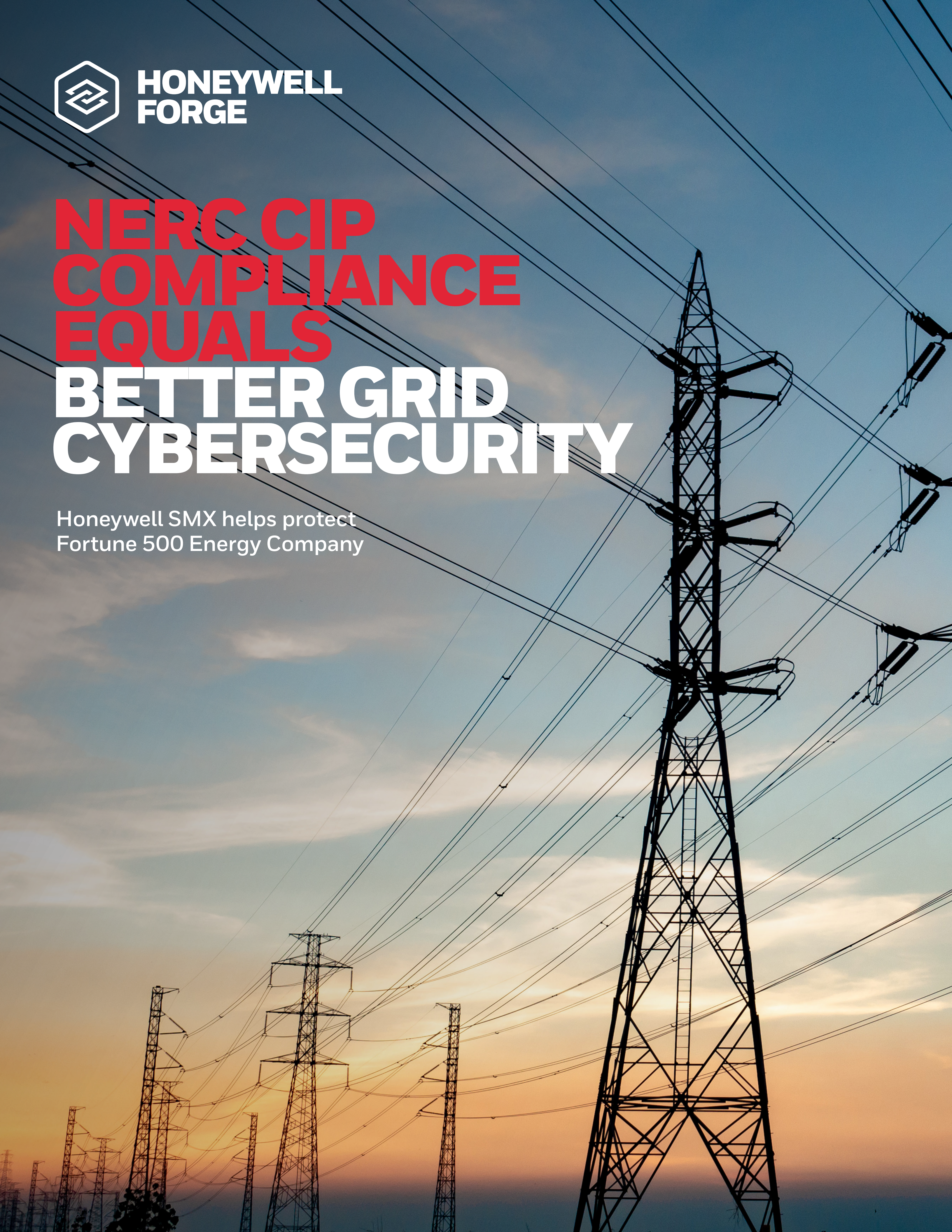
HONEYWELL FORGE



NERC CIP COMPLIANCE EQUALS BETTER GRID CYBERSECURITY

Honeywell SMX helps protect Fortune 500 Energy Company

A POWERFUL ASK

This Fortune 500 company provides something so essential it's life-changing–power. Energy to a massive grid, this company's day-to-day work affects millions of people.

Cyber attacks can reduce the reliability of these massive grids ultimately, impacting numerous lives. That's why the North American Electric Reliability Corporation (NERC) was established along with the Critical Infrastructure Protection (CIP) standards for cybersecurity. This is a federally-imposed set of requirements, specifically designed to ensure cybersecurity helps increase the reliability for operating North America's bulk electric system.

Therefore, when it was time to achieve compliance with NERC CIP requirements, the Fortune 500 energy company looked to Honeywell as experts in industrial control systems (ICS) and operational technology (OT) cybersecurity to get the job done. Implementing stronger, safer, more secure procedures and infrastructure to better protect its power and pass the audit is no small task. After all, the company's core competency is producing power, not cybersecurity.

That's where Honeywell comes in. Already recognized by the customer as a trusted ICS/OT cybersecurity partner, we were asked to lend our expertise to the compliance preparations.

SECURING THE GRID

The customer needed to prove that they were compliant with NERC CIP's requirements; thus, Honeywell cyber experts helped the customer to achieve compliance across the many critical infrastructure facilities the customer has across North America. Additionally, the customer needed to monitor them from one centralized location. The specific NERC CIP-003 technical requirements cover the following: a security awareness program, physical security, electronic security, and incident response.

The customer quickly decided that Honeywell Forge Secure Media Exchange (SMX) was the answer to these new removable media compliance requirements. By being easy-to-use and simple to deploy, SMX was the optimal solution.

In addition to mandatory malicious code prevention programs, the responsible entities for low impact BES cyber systems must establish a plan for removable media as of April 2020. For medium and high impact BES cyber systems, they must establish removable media plans as of July 2020. As of today, all BES cyber assets must have malicious code prevention and removable media plans in place to be compliant.

Per the NERC CIP Standards, the customer and Honeywell needed to:

- Deploy methods to prevent and mitigate the threat of detected malicious code (CIP-007-6 R3)
- Implement a documented plan to mitigate the risk of introducing malicious code from removable media (e.g., a USB memory stick) (CIP-003-8 R1.2 and CIP-010-3 R)
- Mitigate malicious code on the removable media by scanning it before connecting it to the cyber asset (CIP-003-8 Attachment 1 Section 3 and CIP-010-3 Attachment 1 Section 5).
- Detect malicious code and generate alerts that allow the Responsible Entity to investigate if it is an attempt to compromise (CIP-007-6 R4 and CIP-008-6 R1.2)

THE SMX SOLUTION

The team first established functional requirements, including supporting the SMX installation on Honeywell and non-Honeywell control systems. Also, in order to monitor the enterprise deployment of SMX systems from a central location, Honeywell needed to monitor the following information:

- SMX connectivity status
- Control and visibility into the more secure use of removable media
- Manage the use of removable media across the enterprise
- Ensure AV signature is up-to-date on SMX units

And for cyber assets, Honeywell set out to implement protection from USB borne malware, as well as providing device white-listing, which would only allow authorized USB devices to be connected without user intervention via conscious authorization. The team achieved that and more by providing the support in the form of:

- Guidance to meet applicable NERC CIP requirements related to removable media and Malicious Code Prevention
- On-site and remote support for the customer to upgrade their enterprise deployment of SMX systems whenever the latest release is available
- Offering customers full control of how and where USB-based devices can be used including mice, keyboards and cell phones through the Honeywell client driver software: TRUST V2. The capabilities and configurations of rules allowed the Honeywell team to create a list of authorized devices and a list of unauthorized devices
- An installation of the SMX client driver on Honeywell and non-Honeywell systems plus showcasing audit logs from the end nodes. Also, by providing a practical demo of use cases, for instance, when removable media device is first connected, who connected it, and which files were accessed and copied from the device
- Configurations of the SMX enterprise threat management portal for customer and demonstration of portal features, capabilities, alert configurations

PROJECT SUCCESS

SMX surpassed the customer's expectations not only in passing the compliance audit but also by providing control and visibility into all USB device and removable storage use—across the whole enterprise.

> “SMX allowed us to achieve NERC CIP compliance with ease. The solution was simple to install and provides us with USB protection for employees, contractors and any site visitors. The ability to better manage and enforce our USB security policy helps our team to feel more confident that we are taking the right steps to ensure the efficiency and security of our production facilities.”
>
> **– SENIOR OPERATIONS MANAGER**

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. The quantified product benefits referenced are based upon several customers' use cases and product results may vary. Any descriptions of future product direction, intended updates or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion. All product screenshots shown in this document are for illustration purposes only; actual product may vary.

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.honeywellforge.com

Honeywell