STEALTH
by UNISYS

EXECUTIVE OVERVIEW

Cyber Threats Challenging Your Reliability?

UNISYS STEALTH KEEPS THE LIGHTS ON AND TARGETS DARK

Keep Critical Infrastructure Secure

Zero Incidents: Your Goal. Our Mission.

Because of the “always available” requirement and the catastrophic implications when service is disrupted, electric power organizations are rich targets for hackers seeking to disrupt critical operations and exfiltrate sensitive data. Power generation and distribution systems are increasingly vulnerable to cyber-attack.

An advanced persistent threat (APT) by cyber-terrorists or the introduction of viruses and worms could bring down portions of power grids. The three weakest links subject to cyber threats on the power grid are:

1) Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. Legacy technologies, combined with traditional perimeter defenses and air gap approaches are vulnerable to risk from APTs and other sophisticated, coordinated threats.

2) Command and control centers. The operating systems that the human-machine interface (HMI) applications rely on to communicate with ICS/SCADA equipment are ripe targets for hackers and malicious code.

3) Smart grid components. In addition to multiplying risks, these devices will generate huge amounts of data required for existing and pending energy regulations and audits.

How can electric power organizations strengthen mission-critical mission-critical security, reduce costs, and improve agility—all at the same time? With Unisys Stealth™, you can:

Go invisible. Make servers, devices, and other endpoints dark and undetectable to hackers and unauthorized users inside and outside your enterprise.

Isolate segments of your data center based on user identity. Define and control access to mission-critical systems and information based on need-to-know access.

Secure data-in-motion. Protect data with point-to-point encryption.

Consolidate. Reduce reliance on physical IT infrastructure.

Scale and adapt. Upgrade legacy systems, easily meet emerging needs and compliance requirements with agile, software-based security.

Stop Cyber Assaults Before They Happen

Unisys Stealth takes a radically different approach to addressing security concerns by making ICS/SCADA endpoints connected to the network command and control centers invisible to unauthorized users and by securing data-in-motion across any network. This is how Stealth can help electric power organizations *Get to Zero Incidents*.

By creating highly-trusted communities of interest (COI), Stealth is designed to allow only authorized users to access devices, applications, and systems critical to the safe operation of electric power providers, from power generation to customer distribution. In addition to strengthening mission-critical protection, electric power organizations can reduce infrastructure costs by safely modernizing their industrial controls and software with one unified security solution. And as regulatory mandates change, Stealth can deliver the agility enterprises need without requiring costly upgrades or extensive reconfiguration.

Why Stealth Now?

Unisys Stealth is the innovative, mission-critical security that electric power utilities need to maintain reliability:

No operational disruption. Stealth works with existing firewall, intrusion detection, and other security systems with easy installation so you can upgrade your systems without compromising security.

Reduces risk. Make endpoints invisible. Isolate critical systems from the rest of the enterprise. Tighten access control based on user identity.

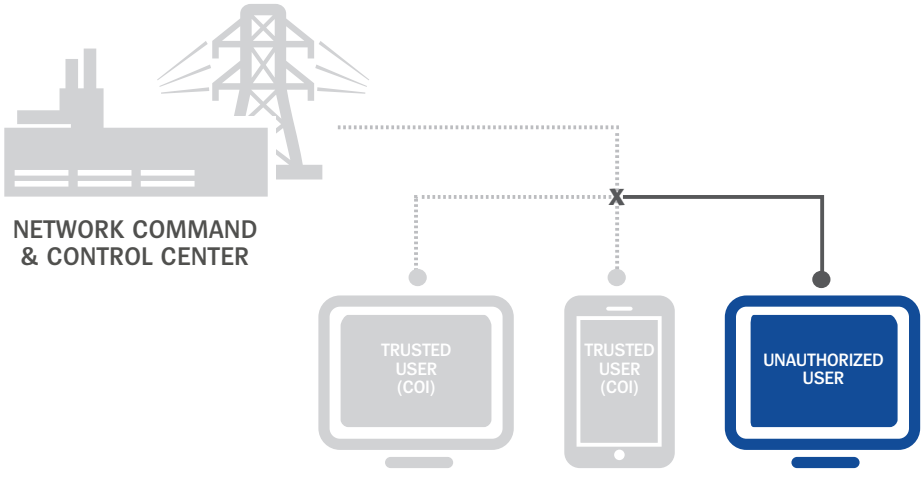
Facilitates compliance. Stealth can help achieve compliance with NERC CIP, the Executive Order on Improving Critical Infrastructure Cybersecurity, and other regulatory requirements and recommendations.

Reduces costs. Protect enterprise customer data, accounting, distribution, and ICS/SCADA with one cost-effective security solution—Stealth can cover both business and power and distribution processes.

Improves agility. Stealth allows for quick, easy changes to accommodate rapidly evolving regulatory requirements or mission/business needs.

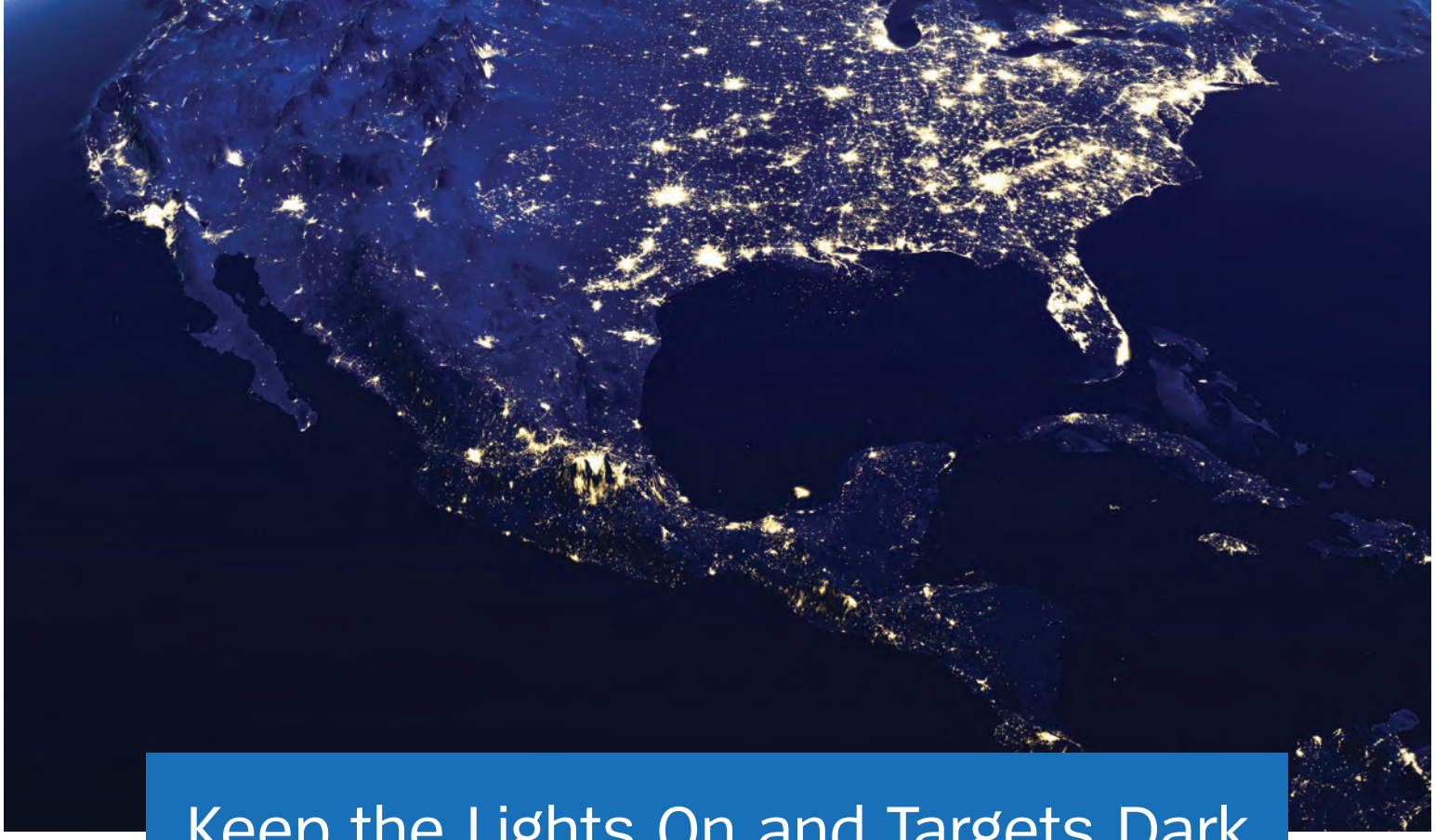
You Can't Hack What You Can't See

STEALTH COMMUNITIES OF INTEREST



Go Invisible.
You control who can access—or even see—SCADA/ICS, command and control centers, and smart grid components.

STEALTH by UNISYS



Keep the Lights On and Targets Dark

Stealth is What Innovative Security Looks Like

When it comes to critical infrastructure, there can be no compromise. Stealth can help move your organization from vulnerable to mission-critically secure. But don't take our word for it. Read *Network World's* May 2014 independent review of Stealth and see why Stealth might just be "a great way to hide from hackers."

www.unisys.com/gettozero

Contact us:
stealth@unisys.com

GET TO ZERO Incidents

YOUR GOAL. OUR MISSION.

STEALTH by UNISYS