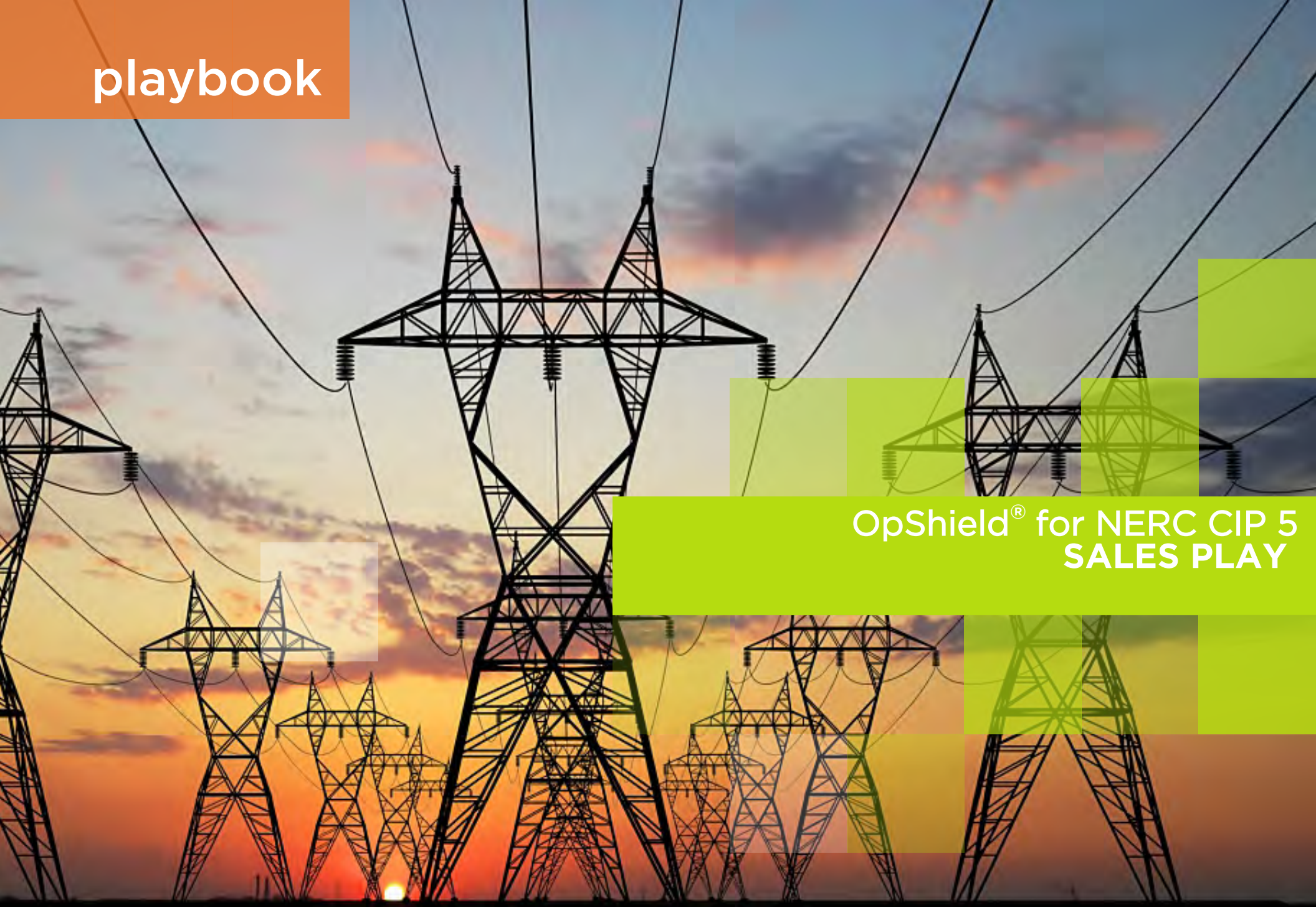
playbook



OpShield® for NERC CIP 5
SALES PLAY

wurldtech™
A GE Company

OpShield for NERC CIP 5

The Problem

U.S. bulk power entities are federally mandated to comply with NERC CIP requirements that dictate industrial security and remediation technology; NERC CIP 5 compliance is required by April 2016. In conjunction, ICS/SCADA equipment is difficult or impossible to patch, yet under frequent attack. Customers need to address known ICS vulnerabilities without disrupting operations. Electrical generation and distribution companies require a solution that is easy to implement and provides visibility into the industrial network and compliance.

The Wurldtech Solution

Our solution is purpose-built to support your NERC CIP security and compliance program. It protects industrial and SCADA operations by offering advanced security, simplicity and visibility. This industrial network security solution monitors and blocks malicious activity to support high-availability, industrial operations. It aligns with NERC CIP mandates by supporting requirements for malicious code prevention, interactive remote access management and configuration change management process.

Why Wurldtech

Focused on industrial security

- Operational technology (OT) cyber security solution combines industrial and SCADA-specific baselining, protocol inspection, vulnerability and threat signatures, and command-level whitelisting
- Industry-leading threat intelligence delivers updated protection and remediation for known ICS vulnerabilities to secure unpatched systems (and systems between patch cycles)

Easy security administration

- Includes easy-to-use graphical interfaces and visibility across the network for alerts/incidents
- Delivers breakthrough drag and drop virtual segmentation and zoning (without rewiring)
- Supports easy ICS communications policy review and data flow audit

Industrial security expertise

- Expertly combines deep understanding of ICS, cyber security and compliance in one solution
- Our deep experience in critical infrastructure includes detailed analysis of the most extensive set of devices and systems from the largest critical infrastructure manufacturers
- Solution feature requests are based on 200+ hands-on, customer security assessments

High Potential Targets

- US Electric Utility entities who have identified medium sites in scope for NERC CIP Standards
- Target personas include:
  - C-suite accountable for NERC CIP across fleets
  - Operator accountable for NERC CIP across fleets
    - Cyber Security Director
    - NERC CIP Compliance
    - Critical Infrastructure Manager

WHAT IS THE PLAY?

After years of hands-on experience with electric utilities and deep acumulated ICS security expertise, Wurldtech has created a NERC CIP solution. By combining the OpShield OT cyber security solution with professional services including installation, training and annual tuning, Wurldtech customers can efficiently align with NERC CIP requirements for malicious code prevention, interactive remote access management and configuration change-management process.

Customer Imperatives

Business/Compliance

- NERC CIP compliance and remediation requirements
- Addressing known vulnerabilities without disrupting operations

Security

- ICS/SCADA equipment is difficult or impossible to patch
- OT protocols can easily be misused to disrupt critical systems
- Industrial networks very hard to rewire for proper segmentation
- Complete lack of visibility into attacks on the industrial network

CYBER INDUSTRY STATS

- Pike Research predicted in 2011 that global utility cybersecurity spending would reach $14 billion through 2018, with about 63 percent of that spending aimed at the industrial control systems and SCADA networks used to control today's grid assets.

  (Wilder claims: GlobalData's prediction of a $79 billion global market by 2020, which exceeds total smart grid spending figures in most of the world.)

- U.S. utilities will spend a cumulative $7.25 billion in security from now until 2020

BEST TARGETS

The primary value of the OpShield OT cyber security solution for NERC CIP constituents is that it provides generators with effective vulnerability remediation until they can apply patches to targets or upgrade operating system software. It leverages technical innovation and automation, while simultaneously improving the security posture of power generation companies.

Ideal Targets

- Regulated power generators with more than one NERC CIP medium site (See list)
- Recently experienced either a public breach or shutdown due to vulnerability (Calpine)
- Recently received a regulatory fine or sanction (NextEra)
- Recently announced new joint ventures or mergers (Exelon/ Constellation)
- Customers already buying CAP at multiple sites

Qualify Out

- Independent power producers without a large installed base
- Smaller, local utilities without plans for large growth or expansion
- Companies that have already heavily invested in enterprise-wide security in OT
- Companies without a defined NERC CIP program and Executive sponsorship

Selected Medium Site Customers in the Energy Industry:

AEP American Electric Power · County of Los Angeles California · DTE Energy · Dominion · Duke Energy · Entergy · FirstEnergy · New York Power Authority · Newfoundland Labrador · NiSource · Ontario · ppl · Southern Company · TVA · TECO Energy

BUYERS & INFLUENCERS

NERC medium sites (sites with 1,500 mW and greater) have monthly patching requirements that require additional staff and drive expensive upgrades due to operating system end of life and lack of vendor support. If the customer has a large fleet of NERC CIP Medium sites, it is likely that the sale will take place at the corporate level where budget resides for any cross-site initiative. If the primary use case is a NERC CIP program being managed by plant maintenance and operations, the sale will likely take place at the plant level where most technology investments are funded. The most important buyers and influencers are listed below.

Senior manager, critical infrastructure security and compliance, principal manager for reliability and cybersecurity, NERC CIP leader

Economic buyer

Key concerns are compliance to standard, effectively managing risk and demonstrating they are good stewards of compliance dollars.

Network security manager, NERC CIP engineer

Technical buyer

Key concerns are sufficient staff for NERC CIP compliance, and the ability to maintain the product's capability to support NERC CIP technology.. May have a technology they are already championing.

CIO, CISO or regulatory affairs executive

Champion/influencer

Key concerns are appropriately addressing security, having visibility into risk across the fleet and being able to articulate aggregate risk.

OBJECTIONS & COMPETITION

On the way to a sale, you're likely to encounter competitors (including the status quo) and some objections. The following common objections and responses will help you to confidently overcome roadblocks.

OBJECTION	RESPONSE
Will NERC CIP auditors accept OpShield as an effective remediation measure against known vulnerabilities?	OpShield has been widely vetted by industry. The product has been viewed as a significant control to remediate known vulnerabilities on equipment that no longer has vendor support or for equipment that cannot be patched outside of maintenance windows.
How can you assure me that your signatures will address known vulnerabilities for my critical cyber asset?	Wurldtech's purpose-built Deep Packet Inspection (DPI) engine has the industry's largest collection of known ICS vulnerabilities. In addition, Wurldtech's industry-leading threat research team closely monitors vulnerability disclosures (such as ICS-CERT) to ensure that our work is on the latest and most pressing vulnerabilities.
We already have IT security measures.	IT security measures do not properly address industrial control systems. OpShield is purpose-built to recognize, understand and inspect industrial protocol traffic in-depth. IT solutions do not have this visibility. In addition, the Wurldtech threat intelligence team is focused on researching and testing protection profiles including signatures to specifically address ICS vulnerabilities. Therefore, OpShield can specifically provide the remediation and protection needed to secure ICS for NERC CIP.
We do not have the expertise to install OpShield and fine-tune ICS communications policies and IPS/IDS.	The solution includes the OT security product as well as installation services, training and annual tuning. This allows our security experts to ensure that your ICS protection is optimally configured. We will also perform yearly service to properly adjust policy and rule settings.
Your solution costs too much to implement.	OpShield and Wurldtech services are investments that return increased ICS security and NERC CIP compliance, particularly for malicious code prevention, interactive remote access management and configuration change management process in the ICS environment.

SUCCESS TIPS & RESOURCES

The purpose of this playbook is to help you have a successful business conversation with the right people to get them interested in achieving NERC CIP 5 compliance more efficiently with OpShield. A key differentiator is our expertise in the security for the energy industry and how that's reflected in Wurldtech's products and services.

Don't give up if a potential buyer doesn't immediately see the need. Find someone at a different plant who understands the need for NERC CIP compliance while improving the organization's overall security posture. Once convinced, that individual may champion an enterprise-wide solution.

Sales Tools:

- Customer presentation (has internal content in back up to be deleted before forwarding)
- Technical Solution Brief
- Budgetary Proposal
- Technical FAQ
- List of GE NERC CIP Medium sites

NERC CIP 5 Resources:

- NERC Main Page
- CIP 5 Transition Program
- Reliability Assurance Program
- NERC Roster
- Critical Infrastructure Protection Committee
- CIP Meeting Minutes

Regional Transmission Organizations:

- NERC Region Map
- Florida Reliability Coordinating Council (FRCC)
- Northeast Power Coordinating Council (NPCC)
- SERC Reliability Program
- Southwest Power Pool (SPP)
- Texas Reliability Council (TRE)
- Western Electric Power Pool (WECC)

NERC CIP INDUSTRY BLOGGERS

- Joel Langill Blog
- Comparison of NERC CIP Revisions