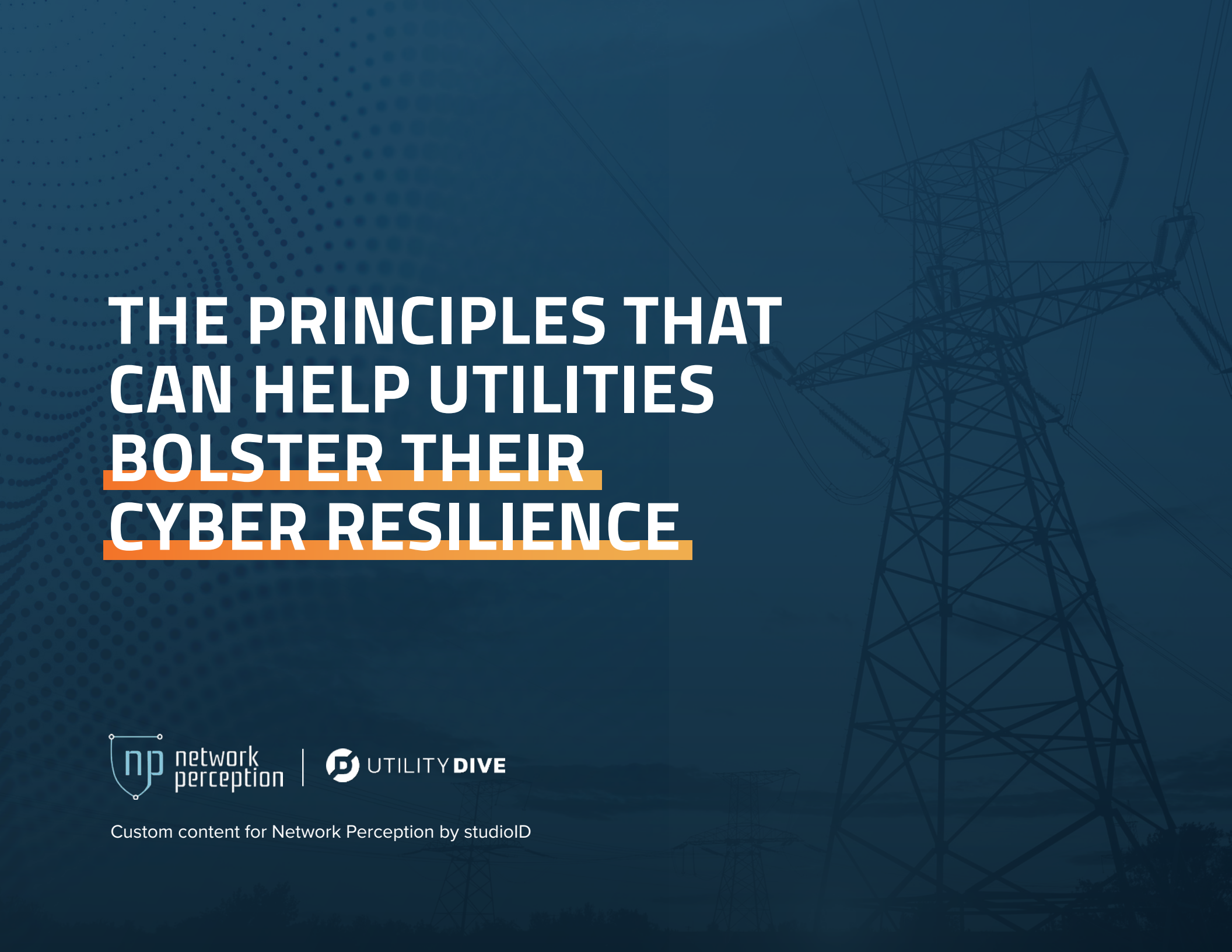
THE PRINCIPLES THAT CAN HELP UTILITIES BOLSTER THEIR CYBER RESILIENCE



network perception | UTILITY DIVE

Custom content for Network Perception by studioID

Last May, the public learned how vulnerable America's energy infrastructure is to cybercriminals. Hackers had launched a successful ransomware attack that shut down a 5,500-mile pipeline that carries nearly half of the East Coast's fuel supply. Amidst a rash of headlines about the attack and its effect on the price and availability of gasoline, the owners of the pipeline paid $4.4 million in bitcoin to cybercriminals to resume operations.

The intense focus on the hack of the pipeline quickly faded. But the reality is that the threat to critical infrastructure symbolized by the pipeline attack is only increasing in volume and sophistication. Over the summer, in fact, U.S. Department of Energy (DOE) Secretary Jennifer Granholm said cybercriminals have the ability to black out America's power grid.

Sobering assessments about the grave societal consequences of a successful cyberattack are not hard to find. IBM recently released a report that found the U.S. energy sector was the third most targeted sector in the U.S., behind only financial services and manufacturing. The DOE was blunt about the stakes in its Multiyear Plan for Energy Sector Cybersecurity. ***"The frequency, scale, and sophistication of cyber threats have increased, and attacks have become easier to launch. Nation-states, criminals, and terrorists regularly probe energy systems to exploit cyber vulnerabilities in order to compromise, disrupt, or destroy energy systems."***

None of this is news to utilities, policymakers, and regulators. A recent survey of 1,000 business leaders showed that those in the energy industry feel more exposed to cyberthreats than their colleagues in retail, financial services and other industries. Regulators are also increasingly taking steps to ensure the energy sector can secure its most critical assets against cyberattacks. For instance, North American utilities must comply with the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards.

NERC CIP, along with cybersecurity regulations issued by the National Institute of Standards and Technology and the U.S. Nuclear Regulatory Commission, acts as a "committed catalog" of various security measures to protect equipment and components from digital attackers. Through research and collaboration spearheaded by the Electric Power Research Institute, the utility industry evaluates new technologies and methodologies **to improve cyber resilience.**

Why cyberthreats multiply quickly

A big reason utilities and the grid are so vulnerable to cybercriminals is that the electric power system is rapidly transforming. Indeed, the grid is shifting from large central station power plants sending electrons in one direction to a far more distributed and digital power system where power flows in two directions.

This shift is most evident in the huge influx of sensors, smart meters and distributed energy resources (DER), such as rooftop solar and battery storage connecting to the distribution and transmission grids. For example, last year consultancy Wood Mackenzie forecast that the cumulative DER capacity in the U.S. would reach 387 gigawatts by 2025 and that 1.3 billion smart meters would be installed across the globe by the same year.

A transformed power grid has plenty of upsides, including everything from accelerating decarbonization to collecting and analyzing data that can help utilities identify equipment problems before they lead to outages. The potential for a more personalized, decarbonized and resilient grid is real. Yet it all rests on a foundation of cyber resiliency.

And for those charged with keeping the grid safe, the proliferation of equipment connected to the grid vastly expands the attack surface cybercriminals can target. Which is why designing, implementing and continuously evolving a cybersecurity strategy to protect the critical assets that keep power flowing are so essential today.

"Twenty years ago, you could run a utility without depending on cyber systems, but today that is impossible," said Robin Berthier, co-founder and CEO of Network Perception, a company that provides software and services to utilities to monitor and protect their most critical assets. "Cyber systems are mission-critical assets, because if they go down, your operations can go down. We work with utilities to improve their cyber resiliency, which is about adopting the right principles when we design networks so that they are much better prepared to stop attacks and can recover faster if those mission-critical assets get compromised."

> *"Twenty years ago, you could run a utility without depending on cyber systems,* ***but today that is impossible."***
>
> **Robin Berthier**
> Co-founder and CEO of Network Perception

Three principles to improve utility cyber resiliency

The approach Network Perception has developed to help utilities simultaneously bolster their cyber resilience while also ensuring NERC CIP compliance is based on three fundamental principles: verification, visibility, and velocity. These principles have their roots in pioneering academic work conducted at the University of Illinois at Urbana-Champaign and in real-world engagements to help NERC auditors assess utility cyber defenses in a low-touch, lightweight manner.

"NERC auditors have a challenge, which is to audit networks without being inside the networks," Berthier said. "As an auditor, you can't say to a utility, 'I need to come with my equipment, plug my cable into your infrastructure and then audit your network. That's not possible. They needed a solution to audit networks offline."

network perception

The following insights are key to Network Perception's development of the three cyber resilience principles:

VERIFICATION

VISIBILITY

VELOCITY

VERIFICATION

Every utility has a collection of technologies, processes and people devoted to protecting their critical assets. The verification principle is devoted to understanding what makes up a utility's current defenses and finding any gaps and vulnerabilities.

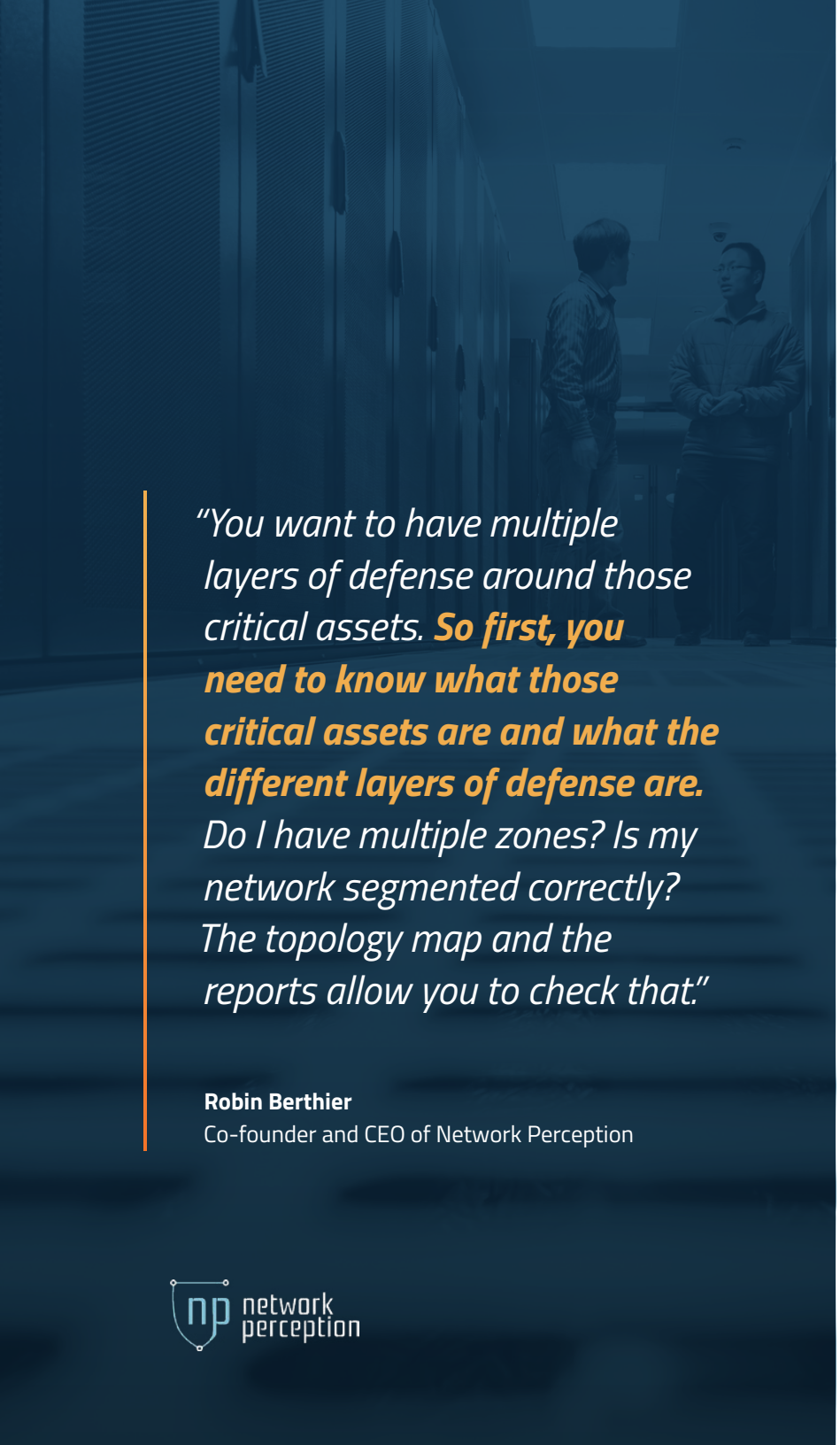
Inevitably, utilities' cyber defenses have many gaps. For instance, it's common for utilities to have multiple brands of firewalls and routers inside their network. This can translate into misaligned or inadequate rules governing permissions and alerts. The thorough analysis during verification can identify these vulnerabilities and ultimately fix them.

"If you have a rule that allows traffic from any source toward a critical server, then we can flag and report that rule," Berthier said. "That way you have a workflow to mitigate that risk and change your rule. Part of verification is also making sure no one is introducing a rule that would open up an unexpected access into your critical network."

Verification also involves identifying and rectifying potential compliance problems associated with existing rules. Addressing these issues requires capturing metadata about the who, when and why around rule changes. All too often, this information is stored in Excel files.

"With NERC CIP, you have to justify every rule that enables traffic to your critical assets," Berthier said. "Sometimes that can mean opening a port for a new application on your network. The metadata added to the rule is crucial to understand who added the rule, why, and when. Most of the time, utilities capture that information in a spreadsheet and there can be a mismatch between what's in Excel and what is in the firewall. It's hard to keep up to date and the process may be inconsistent across teams and business units."

These gaps and mismatches are why Network Perception provides utilities with a uniform process for storing metadata that allows for consistent change management.



"You want to have multiple layers of defense around those critical assets. ***So first, you need to know what those critical assets are and what the different layers of defense are.*** *Do I have multiple zones? Is my network segmented correctly? The topology map and the reports allow you to check that."*

Robin Berthier
Co-founder and CEO of Network Perception

network perception

VISIBILITY

Berthier once worked with a manager who oversaw cybersecurity at his utility. Each week, his staff would hold a multiple-hour firewall review meeting. For the manager, it was a difficult few hours. ***"He would listen to a very technical discussion about the latest device deployed and the latest rule changes," Berthier said. "For years, he could not follow the discussion because it was too technical and complex."***

The need for an easily understood and common language about a utility's network segmentation and how critical assets are protected is vital. Which is why visibility is such an important pillar of cyber resilience. A number of elements go into visibility. An important one is a clear understanding of the criticality of the servers, workstations and equipment that make up a network. For instance, computers that manage generators producing electricity are critical — in fact, NERC CIP requires that a cyber asset that could affect the operation of the bulk electric system within 15 minutes of a compromise be identified as a BES critical asset.

Network Perception combines the need for a common language and the concept of criticality into its visualization of the topology of a utility's network. This allows utilities to label the criticality of assets and their defenses and promotes easy understanding among technical and nontechnical audiences. ***"You want to have multiple layers of defense around those critical assets," Berthier said. "So first, you need to know what those critical assets are and what the different layers of defense are. Do I have multiple zones? Is my network segmented correctly? The topology map and the reports allow you to check that."***

VELOCITY

Velocity. A common observation about achieving and maintaining utility cyber resilience is this: Cybercriminals adapt and evolve their attacks much more rapidly than those in charge of security can respond. It's a real challenge, one that is made worse when utilities don't assess and respond to risks and attacks in real time.

"If you check your network once a year for vulnerabilities, that leaves 12 months of exponential growth in risk to take place," Berthier said. "So then the next time you check, it's a huge amount of work to fix it. The principle of velocity is to not allow the risk profile to get out of control by verifying and visualizing your risk continuously."

Network Perception's ability to ingest configuration files and data allows utilities to model their networks and visualize their risks and vulnerabilities in real time. This is what injects velocity into a utility's cyber resilience, allowing companies to proactively identify and mitigate risks as they happen. ***"When we can combine asset criticality with an understanding of the pathways that lead to vulnerabilities, we can fuse those layers of information together," Berthier said. "Then we can make informed decisions around which vulnerable assets to patch first, what zones to better segment, and which access policy gaps to close in priority."***

> *"If you check your network once a year for vulnerabilities, that leaves 12 months of exponential growth in risk to take place. So then the next time you check, it's a huge amount of work to fix it.* ***The principle of velocity is to not allow the risk profile to get out of control by verifying and visualizing your risk continuously."***
>
> **Robin Berthier**
> Co-founder and CEO of Network Perception

Austin Energy's cyber resilience journey

Few people have as deep and as wide-ranging experience in utility cyber resilience as Thomas Standifur. Standifur spent a decade as a cybersecurity consultant before joining Austin Energy nine years ago as a program manager for critical infrastructure protection compliance. ***"My first project was to build a NERC CIP compliance program because they had just been through an assessment that was not looking as good as they wanted," Standifur recalled.***

Fast-forward nine years and Austin Energy's cyber resilience is widely viewed as one of the best in the industry. Which is even more of an accomplishment because the cyberthreats Austin Energy faces have only become more complex. ***"Austin is one of the fastest-growing cities in America, and we have a large service area as well as about 1,500 miles of routed fiber, which is not very common for a utility," Standifur said. "Because we have such a large service territory, we are adding far-flung substations, and every time you build a new substation or transmission facility, you are increasing your threat vector significantly."***

When Standifur first began building Austin Energy's NERC CIP compliance program, he focused on shifting the culture. Like a lot of utilities, silos separated information technology and operational technology. Standifur's first task was to demolish them. ***"From the get-go, I said we don't do compliance, period," Standifur said. "We do great cybersecurity, and compliance is a byproduct."***

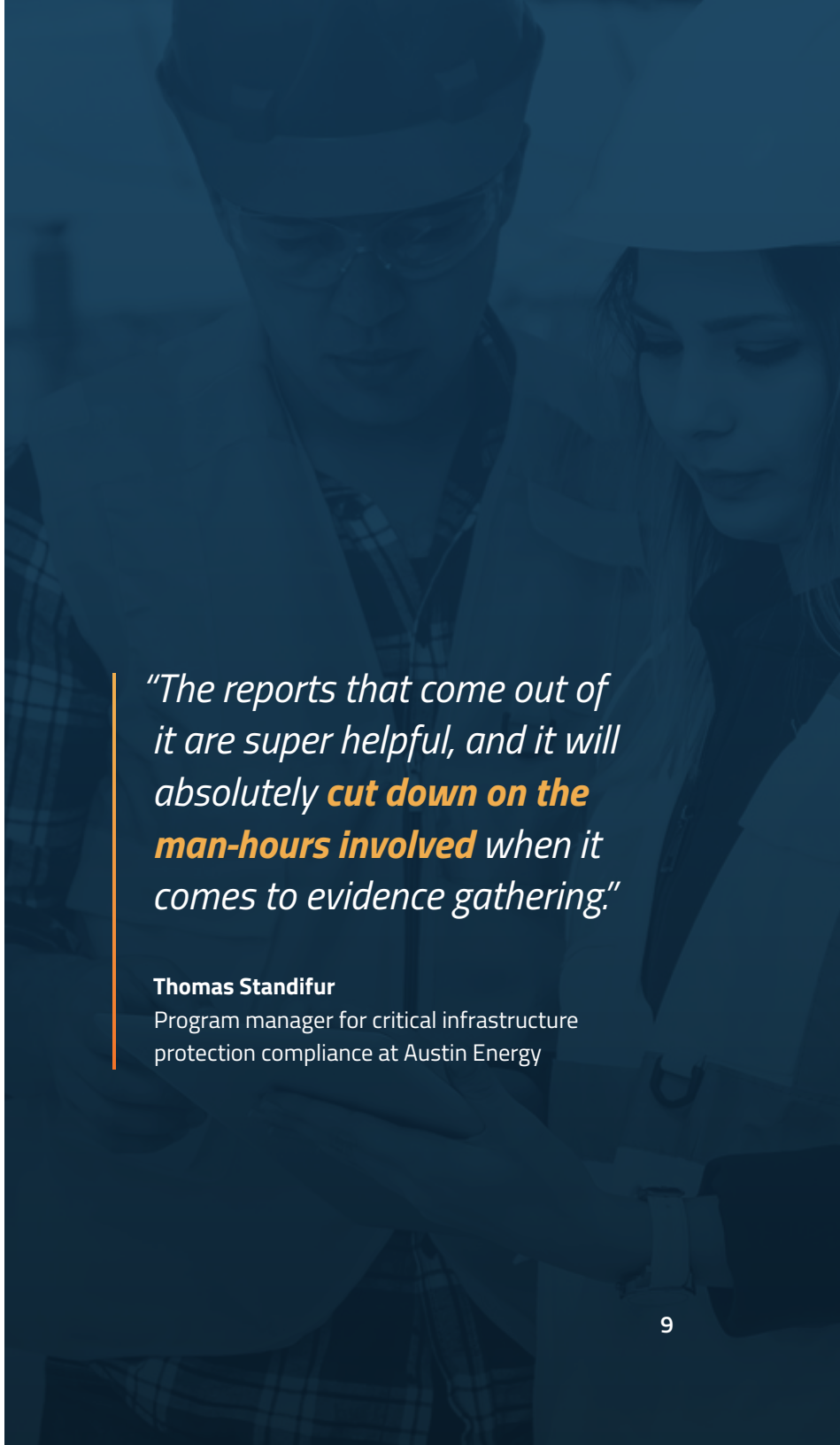
At Austin Energy, that has meant locking the organization down against the threat of internal cyberthreats and moving toward a future where all access to critical assets is controlled and where just-in-time permission is possible.

As part of its evolution to improve cyber resilience, Austin Energy partnered with Network Perception. Initially, Austin Energy relied on Network Perception's NP-View product to improve audits and analysis of its firewall, router, and switch configurations. NP-View Professional allows for automated analysis that can be easily exported into the compliance reports NERC requires. ***"We used it for our audit, which was extremely helpful because it was what the auditors were looking for and it gave us the opportunity to run through everything and make sure it looked good before we sent it off in a configuration file," said Standifur. "We were able to give them a locked configuration file and they didn't necessarily have to be on our network."***

> *"From the get-go, I said we don't do compliance, period. We do great cybersecurity,* ***and compliance is a byproduct."***
>
> **Thomas Standifur**
> Program manager for critical infrastructure protection compliance at Austin Energy

That positive experience led Austin Energy to implement NP-Live Enterprise, Network Perception's continuous monitoring solution. While implementation is just wrapping up now, Standifur is eager to use the platform because he believes it will help streamline the data collection that is inevitably important to cyber resilience and compliance. ***"The reports that come out of it are super helpful, and it will absolutely cut down on the man-hours involved when it comes to evidence gathering," Standifur said. "The fact that the solution is lightweight and allows you to quickly hunt information down when you're doing validation and configuration makes it invaluable."***

Even as Standifur implements new solutions to improve cyber resilience at Austin Energy, he remains focused on the culture shift he began nearly a decade ago. Today, that means shifting the definition of what critical infrastructure actually is. ***"Critical infrastructure isn't just what falls under the scope of NERC," Standifur said. "I want people to understand that when they walk into Austin Energy, they are working with critical infrastructure. If you're answering phones and helping customers, you're working with critical infrastructure. That's the mentality we are driving toward."***



> *"The reports that come out of it are super helpful, and it will absolutely* ***cut down on the man-hours involved*** *when it comes to evidence gathering."*

Thomas Standifur
Program manager for critical infrastructure protection compliance at Austin Energy

network perception

Network Perception delivers critical infrastructure industries with a pioneering risk visualization technology empowering their cybersecurity and compliance teams to achieve high level of cyber resiliency through verification, visibility, and velocity. Built by a government funded research team comprised of cybersecurity, government and industry experts in network security and critical infrastructure protection, the NP-View platform is the industry standard to verify network segmentation and visualize industrial control network environments. It provides organizations with the ability to make informed determinations of configuration alignment as well as ensuring that best practices and regulatory standards are met.

LEARN MORE

BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

LEARN MORE