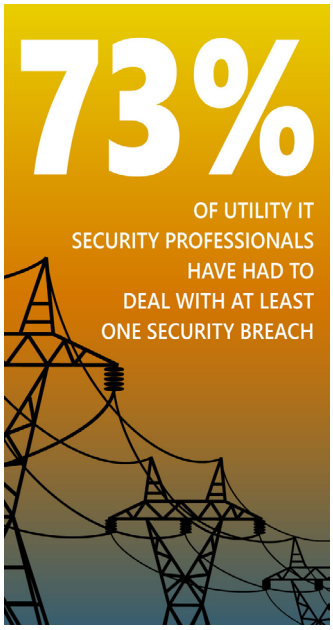
ZONES
First Choice for IT™

Utility Data Security
**WHITE PAPER**




# Addressing the Unique Challenges of Utility Data Security

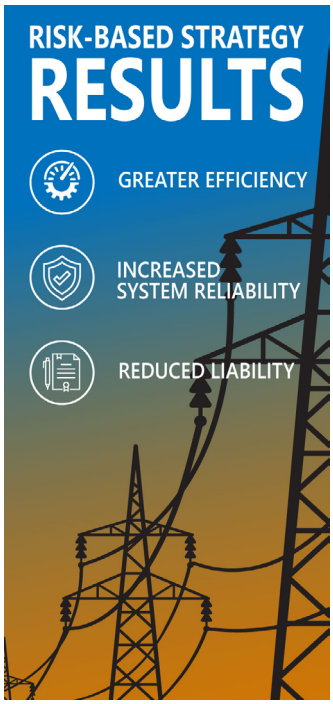
In recent years, it's become clear that security is not just a compliance-driven necessity for utility companies – it's a business imperative. Recent events, such as the cyberattacks that took place against utilities in Ukraine, have proven that large-scale attacks against power grids can succeed, and that organizations must do what they can to protect themselves.

Here in the United States, a number of regulatory agencies are cracking down on utility vulnerabilities. For example, as of July 1, 2016, U.S. utilities must comply with version 6 of the Critical Infrastructure Protection (CIP) standard imposed by the North American Electric Reliability Corporation (NERC), which has an expanded scope and greater emphasis on security compared to previous NERC CIP guidelines.

To respond effectively to an ever-shifting landscape of cyberthreats, including the rise of ransomware, utility companies must act now to adopt a risk-based approach to security that doesn't just meet regulatory requirements – it should exceed them.

## What makes utility security unique

Threats are everywhere in the business world these days, but utilities have become especially popular targets for cyberattacks. According to the Cisco Security Capabilities Benchmark Study, 73% of utility IT security professionals say they have had to deal with at least one security breach. It's true that many U.S. utilities have undertaken substantial cybersecurity measures; however, it's equally important to note that the landscape is constantly changing, and utilities are a particularly difficult sector where security is concerned.




One unique aspect of the utility business is geographic distribution. Very few industries control such a widely distributed infrastructure that connects so directly with consumers. When there is a system failure, the impact is immediate, harsh, and widespread. Along those same lines, fast-growing networks prevent challenges too – with the advent of smart grid and IoT technology, many utility operational technology (OT) departments are now managing networks far larger than their information technology (IT) departments ever had to. Managing the heavy volume of data involved is a considerable leap for many utilities.

There are a couple of other considerations that are not necessarily unique to the utility industry, but are still crucial. For example, consider third-party access – utilities are increasingly reliant on third parties to maintain their equipment, but this can introduce challenges around access control. Additionally, human error is a common problem. Most instances of human-caused utility system downtime result from automobile accidents, not malicious attacks. For all of these reasons, utilities must have sophisticated plans where security is concerned.

## Understanding utility cybersecurity regulations

Because of the challenging landscape that utility organizations face, the federal government has put up a number of cybersecurity regulations on the bulk power grid since 2016. The latest NERC CIP standard is at the center of this conversation. Under version 6, organizations must take a risk assessment-based approach, assigning a risk level to all bulk power system assets and devising a compliance plan based on that metric.

## Risk-based security strategies offer several benefits:

- **Greater efficiency.** With safe automation of processes that were once manual, organizations can save time and money.
- **Increased system reliability (and customer satisfaction).** Security controls not only impede attacks, but they also guard against errors and accidents. This can help minimize damages and speed up recovery after an attack, which makes everyone happier.
- **Reduced liability.** Insurance providers and legal departments are becoming increasingly wary of cybersecurity risks. Proactive, comprehensive cybersecurity can help mitigate their concerns.

Another notable benefit of NERC CIP compliance is that measures implemented for bulk power grid assets can also be voluntarily applied to local distribution grids (minus the cost and labor of regulatory paperwork). Doing this can be beneficial, since hackers and saboteurs probably don't distinguish much between distribution and bulk power systems. Also, within a utility's infrastructure, the line between these systems is blurred, since many substations include both transmission and distribution assets.


## Best practices for utility security

Because threats are evolving constantly, utility organizations must have an agile mindset to mount a response that's both effective and financially savvy. This means responding quickly to potential risks, and it also means having a willingness to change things up. Predictability and homogeneity tend to facilitate, rather than thwart, cyberattacks.

**The following principles would be wise for utilities to consider as they go about enhancing security:**

- **Coordination.** This should include cross-departmental leadership and collaboration.
- **A big-picture view.** Physical and digital security are no longer separate – utilities should address both at once.
- **Identity management.** Context is key here; utilities must know who is accessing their systems, how, and why.
- **Situational awareness.** Utilities should use the network as a sensor to better understand the environment around them.
- **Education.** All relevant personnel must understand the importance of security and how best to maintain it.
- **Execution.** Paperwork alone does not necessarily boost security; utilities must follow through completely on their security plans.

Additionally, compliance alone does not guarantee security. Regulatory mandates create a useful baseline across an industry, but attackers are constantly seeking, and finding, new vulnerabilities. A narrow focus on regulatory compliance can leave glaring weaknesses in any utility's security framework.

## What our partners have to offer

Utility security is a serious challenge, but fortunately, Zones' portfolio of technology partners cover the range of x86 Data Center (On and Off Prem Cloud), Client Compute, and Network. Below are two examples from our Tier 1 OEM partners:

- **Cisco's Advanced Malware Protection** platform offers an integrated architecture that was developed around a core of shared, bi-directional threat intelligence, thus automatically keeping organizations protected against even the most advanced threats of today. With AMP for Endpoints, you'll be able to prevent threats immediately at the point of entry, then continuously track every file you allow onto your endpoints – including desktops, laptops, mobile devices, and more.
- **Dell Technologies** can also play a key strategic role here. With PowerScale, Dell Technologies' newest offering for network-attached storage (NAS), users can get the power of OneFS from a much smaller, more affordable offering than Isilon or ECS. Additionally, utilities can enjoy cloud and data protection through Power Protect and IDPA appliances, also available through Dell Technologies. The company also offers a complete solution to protect against ransomware attacks in Cyber Recovery Vault.

In a fast-evolving space like utility security, these solutions can come together to provide flexibility and ease of access for organizations that sorely need it.


## Zones has been there before

As for Zones, we have a lengthy track record of working with utility organizations to help them achieve their IT objectives, both security-focused and otherwise. To cite just one example specific to x86 On-Prem Data Center, we recently worked with a large utility client to enhance the security posture of their systems. Within that effort, we also addressed ancillary requirements.

The client migrated from a proprietary legacy system for data warehousing and adopted a modern open-source platform. It became a challenge to keep up with the rapid pace needed to maintain and optimize the performance of the new open-source platform.

Zones identified the areas where the client needed improvement and developed a solution to address them. The solution included system software patching, version upgrades, remote workload monitoring, and technical project management. The outcome of this solution was a more stable and secure environment, predictable performance, and maintenance automation.

This is just one example of the Zones approach, but it shows what we do best – we assess risks and develop solutions to mitigate them, as well as improve the overall state of your environment.

## How you can get started

If you're ready to begin working with Zones to improve the security posture of your utility organization, we have CapEx-friendly solutions available that can help you achieve your desired outcomes. The next step is to schedule a discovery workshop with the Zones account team to identify areas of needed improvement. From this workshop, we'll draw up a plan to not only meet, but exceed your requirements and your criteria for success.

Generally speaking, cyberattackers prefer the path of least resistance – they want to go after the easiest targets. Utilities that invest in security, therefore, are far less likely to be the victims of large-scale attacks. With proper planning, your organization can make such an investment in a way that stays within budgetary constraints and meets all relevant regulatory requirements.

## About the Authors

**Matt Leavitt** is a Senior Account Executive at Zones with 17 years of technology solutions experience, including 12 years specific to utilities. His work spans the domains of x86 Data Center (On and Off Prem), Network Engineering & Construction (Wired/Wireless/Outdoor/Indoor), and Client Compute (Field Force and Campus). Matt has delivered solutions catered to utility infrastructure architectures for Substation Automation, Grid Management, Smart Meter, Field Force, and End User Experience/Productivity.

**Robb Stanton** is the Director of Strategic Solutions at Zones. He has over 25 years of experience supporting complex service delivery and strategy. He has been focused on critical infrastructure and supporting some of the largest utilities in North America over the last 10 years. He has developed and implemented several complex solutions specifically targeting the complexities of utility infrastructure and utility clients needs resulting in increased operational efficiency and cost savings.

### More Information

Visit our website Zones.com
To speak with a solution specialist in the U.S. call toll-free **1-800-408-9663**.


### References

**Cisco, Utility Security:**
Exceeding Mandates to Mitigate Risk.

## About Zones, LLC

For over 30 years, Zones has worked with industry-leading partners to offer comprehensive IT solutions to clients around the world. Our Workplace Modernization, Network Optimization, Data Center Transformation, and Security Fortification solutions lead clients through their digital transformations, and our services offer support every step of the way. That's what makes us the First Choice for IT.™

### Corporate Headquarters

Zones, LLC
1102 15th Street SW, Suite 102
Auburn, WA 98001-6524