FORTINET

SOLUTION BRIEF

Protecting Public Utilities’ Smart Infrastructure with the Fortinet OT Security Platform

EXECUTIVE SUMMARY

From 2020-2022, the number of cyberattacks on utilities increased by 118%, according to an International Energy Agency commentary.[1] A growing number of utility providers are implementing smart infrastructure, which offers significant benefits to both providers and consumers, such as reduced consumption, less environmental impact, improved reliability of supply, and cost-savings opportunities. However, smart infrastructure for utilities also requires digital connections, giving bad actors a larger attack surface. At the same time, a growing skills gap has made recruiting and retaining expert cybersecurity personnel a critical challenge.

The Fortinet OT Security Platform offers smart utility providers the industry’s highest-performing cybersecurity platform. It provides full visibility, controlled access, and robust threat detection and response—while still achieving all the benefits that smart utility technology delivers to utilities and consumers. The combination of proven, scalable security equipment, deep knowledge, and skilled personnel creates a comprehensive, manageable security environment from RFP, design, and deployment through the entire lifecycle.

In an industry survey of senior US utility professionals, 83% of respondents said the need for ‘proven security and reliability’ for smart utility networks was ‘very important’.[2]

The Distinct Vulnerabilities of Smart Utilities

A smart utility network connects smart meters and other intelligent devices, the industrial communication network, unique communication protocols, and advanced applications to deliver safer gas, more dependable power, more efficient public lighting, and cleaner water. However, smart infrastructure like smart grids and smart water treatment systems also present a unique, expanded set of cybersecurity challenges that must be solved.

When physical meets cyber. Transforming typical utility infrastructure into smart infrastructure requires removing the barrier between the physical and cyber. There is no longer protection via air gaps or “security by obscurity.” OT and IT systems have an interdependence that improves the service, but creates new risks with serious consequences.

A larger attack surface. With the digital transformation that drives smart utilities, the intersection between the physical and cyber increases the size of the attack surface. Connected components on a network—such as smart meters, sensors, and even smart appliances become new potential entry points for bad actors. Supply chain security and secure-by-design are crucial tissues when dealing with smart technologies employed in the national critical infrastructure.

Increased external threats. Because smart infrastructure such as smart grids and smart water management systems are required for the normal functioning of a society, they are particularly attractive targets to nation-states and hacktivists wanting to cause socio-political disruption, as well as cybercriminals looking to profit by disrupting an essential service.

According to the International Energy Agency, the utilities sector faced an average of 1,101 cyberattacks *per week* in 2022.[3] With infrastructure such as utilities continuing to evolve through digital transformation and become smart infrastructure, Fortinet can help utility providers overcome these unique security challenges by providing protection at scale, legacy-system protection, enhanced compliance, and security as a service. The Fortinet OT Security Platform also offers future-proofing for organizations that intend to continue modernizing and innovating.

Cybersecurity for Smart Utilities

To thrive throughout digital transformation, the smart utilities industry needs to rethink its security posture and move toward a seamless, comprehensive, and zero-trust cybersecurity strategy for its smart infrastructure. The Fortinet cybersecurity platform unifies the best of current IT network security capabilities with an in-depth understanding of the OT security requirements including applications and protocols and offers:

- **Visibility:** FortiNAC network access control (NAC) and FortiGate next-generation firewall (NGFW) provide comprehensive visibility into the network by continuously monitoring and analyzing traffic, user behavior, and device activities. This visibility helps identify potential security threats and vulnerabilities in real-time, ensuring proactive threat mitigation. FortiNDR network detection and response (NDR) offers deep visibility into network vulnerabilities, threats, and malicious network behavior through its patented artificial intelligence and machine learning (AI/ML) techniques. FortiNDR can integrate with Fortinet or third-party security solutions to support response and remediation actions for any detected network anomalies.
- **Secure Networking:** FortiGate serves as the cornerstone of the network infrastructure, offering advanced firewall, intrusion prevention system (IPS), virtual private network (VPN), and secure software-defined wide area network (SD-WAN) capabilities. FortiAP access point and FortiSwitch secure network switch provide secure wired and wireless connectivity while FortiManager, a central management and policy orchestration platform, centralizes network management—making it easier to configure, monitor, and maintain the network infrastructure. FortiAnalyzer, a centralized network analysis and troubleshooting solution, offers centralized logging, monitoring, and reporting capabilities and includes tailored compliance reports mapped to well-known cybersecurity frameworks.
- **Zero Trust Network Access:** Zero trust network access (ZTNA) ensures secure access to applications or devices hosted anywhere, whether users are working remotely or in the offices. FortiNAC, FortiAuthenticator, and FortiPAM play vital roles in ZTNA implementation. FortiNAC enforces strict access policies based on user and device identities, ensuring that only authorized users and devices can access network resources. For enhanced security, FortiToken provides multi-factor authentication (MFA) and can integrate with FortiAuthenticator for single sign-on. FortiPAM combined with FortiClient provides role-based access control and privileged access management capabilities to roll out zero-trust across internal and external users and critical systems at scale so that the users are restricted based on their roles and can perform their activities securely and safely.
- **Endpoint Detection and Response:** A smart infrastructure has an increased number of endpoints and securing these endpoints is critical to ensure end-to-end security. FortiEDR, an endpoint detection and response solution, is an essential part of the Fortinet Security Fabric that can detect and respond to suspicious behavior or threats across a large number of endpoints, minimizing the risk of security breaches in the smart infrastructure.

"The global rise in cyberattacks means that everything is under scrutiny. As systems become more connected and automated, ensuring security across all network connection points is the first priority during design and implementation."

— **Jeff Scheb,** Director of Product Management at Landis+Gyr, in Smart Energy International

The Fortinet OT Security Platform is tailored to meet the security requirements of the smart utilities. It encompasses a broad portfolio of security solutions, covering detection, prevention, containment, and recovery. Implementation of the Fortinet OT Security Platform assures both providers and users that the cybersecurity requirements for smart infrastructure are met. This includes addressing security audit requirements from regulators and demonstrating compliance. Likewise, the security architecture team can trust that the smart infrastructure adheres to industry-compliant security implementation. Ultimately, the Fortinet OT Security Platform offers an end-to-end security solution.

Enhancing Cyber Resilience Through the Fortinet OT Security Platform

With its breadth and depth, the implementation of the Fortinet OT Security Platform ensures that critical operational resources and data are protected from cyberthreats. As a result of this security implementation, business activities and delivery of services remain uninterrupted, and schedules and resources such as power and water supply are optimized. Fortinet supports the key outcomes that smart utilities industry need most, including:

- **Maintaining Reliability.** Cyberattacks can shut down equipment, expose operational data, and lead to a loss of control over systems. All of this affects the utility's ability to what customers depend upon. Fortinet's commitment to constantly updated threat identification and protection mitigates the risk of service disruptions due to cyberattacks like ransomware and infrastructure takeover.
- **Ensuring Compliance.** As the federal government invests in infrastructure, utilities will need to stay within operational rules to ensure funding. There are also increasingly tough mandates for cybersecurity implementation and penalties on security lapses and negligence. Fortinet both simplifies regulatory reporting and supports standards-based security implementation for smart utilities.
- **Managing Reputational Risk.** Smart utilities providers who don't take security seriously risk severe institutional and personal damage to the reputations of those involved. Partnering with Fortinet, a respected industry leader in cybersecurity, helps mitigate the exposure to reputational risk due to cyber-driven data breaches or disruption of services.

Through a comprehensive and scalable security technology platform, Fortinet can secure smart utilities infrastructure, catering to entities of all sizes—from the smallest independent organizations to the largest public operators. Regardless of the size or extent of smart infrastructure, Fortinet offers cybersecurity for every user, system, and network.

Fortinet for Smart Utilities

Providing power and water is critical to maintaining society as we know it. Utilities are under immense pressure to maintain reliability, keep prices down, serve and protect their biggest industrial customers, and ensure that the public and their employees are kept safe at all times. Smart infrastructure solutions for utilities are an exciting way to conserve consumption while reducing costs—but digital transformation comes with increased security challenges.

The Fortinet OT Security Platform protects modern and legacy systems by scaling to meet all needs through a partnership that provides the equipment, knowledge, and expert personnel to create a comprehensive security environment for smart utilities. It's the only cybersecurity platform rated by Westlands Advisory as a Leader in the 2023 IT/OT Network Protection Platforms Navigator—and delivers broad, integrated, and automated digital security for all infrastructure innovations of smart utility providers.[4]

[1] Ben German, "The Mounting Cyber Threat to Power Infrastructure," Axios, August 3, 2023.

[2] Jennifer Runyon, "Survey: Cybersecurity of IoT is Top-of-Mind for US Smart Utilities and Tech Providers," Smart Energy International, March 17, 2023.

[3] Marc Casanovas and Aloys Nghiem, "Cybersecurity–is the Power System Lagging Behind?," IEA, August 01, 2023.

[4] "Fortinet Recognized as the Sole Leader in the Westlands Advisory 2023 IT/OT Network Protection Platforms Navigator™," Fortinet, July 27, 2023.

FORTINET

www.fortinet.com