SOLUTIONS OVERVIEW

Protecting the Power and Utilities Industry

Integrated, Automated Threat Protection Using the Fortinet Security Fabric

Executive Summary

With critical vulnerabilities in both operational technology (OT) and information technology (IT) systems, power and utilities companies must adopt defense-in-depth strategies. The Fortinet Security Fabric provides broad, integrated, and automated threat protection that is specifically geared to security related to power generation, transmission, distribution, corporate infrastructure, and the customer experience.

13% of top-tier organizations leverage orchestration and automation to enhance and keep up with their cybersecurity posture and maturity.[1]

Convergence with IT Heightens OT Risk

As power and utility companies modernize their critical infrastructures, they integrate their OT and IT networks to encourage operational efficiency and grid reliability. However, eliminating the physical separation, the air gap, between the IT and OT environments is a significant opportunity for cybercriminals.

A relatively new challenge to utilities is the shift in the electrical generation portfolio. Renewable energy continues to grow in volume, and as the industry matures, it becomes more vulnerable to cyberattacks. Experts predict that the number of cyberthreats will only increase in the coming years, especially as the clean energy transition gains momentum. Both large-scale and small-scale renewable energy resources are likely to be targeted. The U.S. utilities sector reportedly saw a 46% year-over-year increase in cyberattacks in 2021.[2]

Modernizing OT networks that control critical infrastructure is an enabler of this growing threat. With the dissolution of the air gap, which once separated OT systems from the IT network and public internet, the risk of malicious attacks or even accidental exposure has never been greater. Approximately 70% of transmission lines have been in service for at least three decades and are nearing the end of their operational lifespan. Meanwhile, 60% of circuit breakers have been in use for over 35 years, despite having a recommended lifespan of only 20 years.[3]

Key Power and Utilities Cybersecurity Challenges

Cyberattacks against power and utility systems can have both digital and physical impacts. Poorly secured electronic communications can expose sensitive business and customer personal data. In December 2016, the Ukrainian power grid experienced a second attack that caused a power grid outage in Kyiv. This incident affected 250,000 Ukrainians and resulted in a portion of the city's electricity being unavailable for approximately an hour. It was a significant event in ELECTRUM's history designed to manipulate electric transmission equipment.[4]

Service interruptions caused by cyberthreats can also have financial impacts on the provider and potentially more serious impacts on customers reliant on critical infrastructure. Sabotage operations carried out over the network can cause physical harm to on-site employees and even nearby residents. Failure to protect against these types of attacks can also damage brand reputation and result in fines and loss of compliant status with the numerous regulations governing the industry.

Securing the networks of power and utility companies against cyberattack grows more complex as the integration of newer forms of power like solar and wind result in more distributed infrastructures. Failure to centralize visibility and risk management across the network results in operational inefficiencies due to the need to manually manage security workflows and compliance reporting. These inefficiencies slow threat detection and response rates and create redundancy, increasing operational expenses (OpEx).

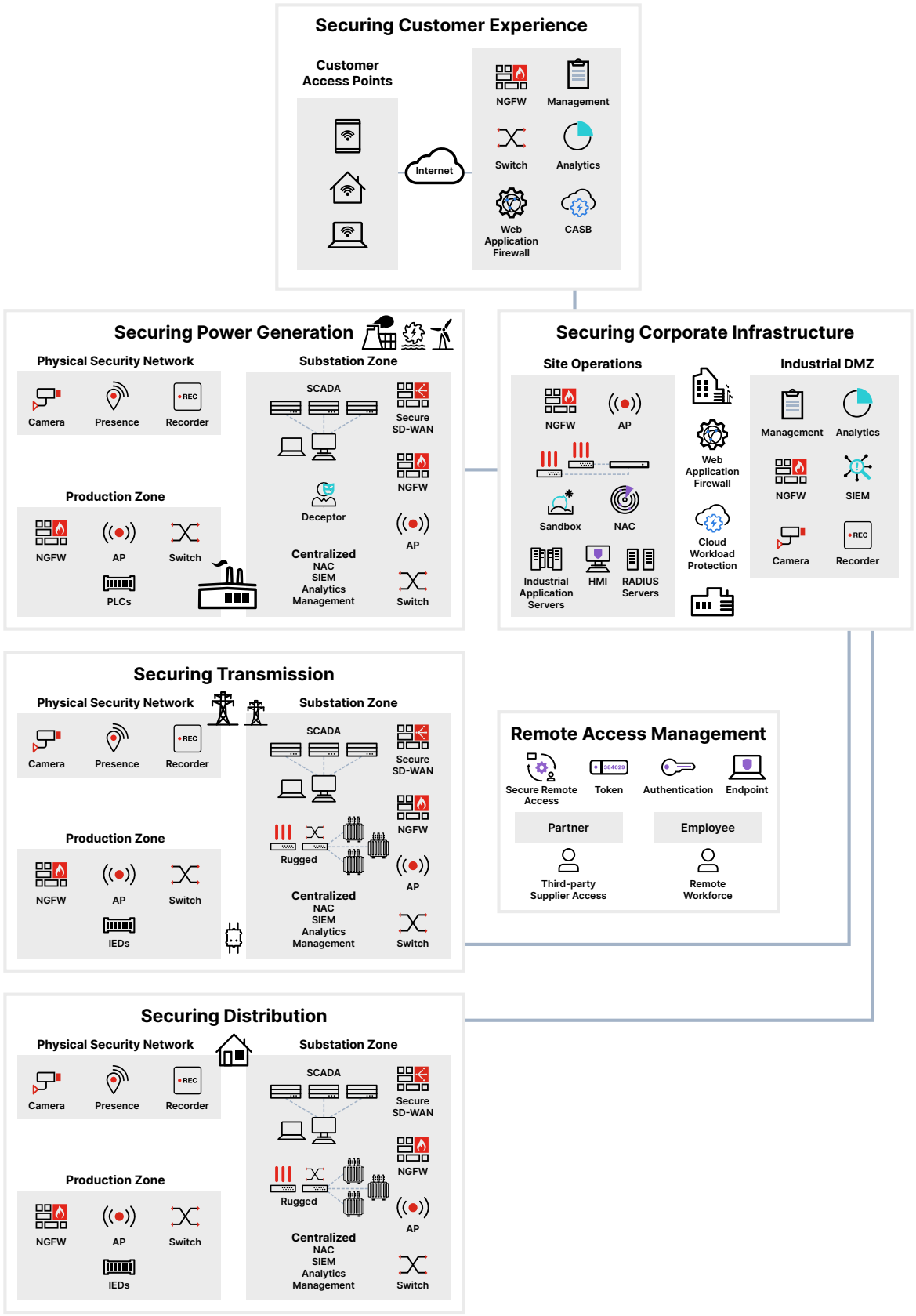


Figure 1: Protecting power and utilities from cyberattacks and insider threats requires a comprehensive security approach across the broad attack surface.

Power and Utilities Cybersecurity Use Cases

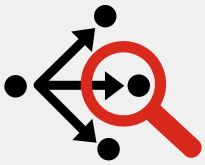
The capabilities found in Fortinet solutions can be used in several different areas in the power and utilities sector.

Securing generation

Cyberattacks against power generation facilities are deployed to cause service interruptions, which can lead to dangerous physical and economic damage. Network managers at these facilities can leverage Fortinet Security Fabric solutions like their peers at the corporate office. The difference is that there often is a larger attack surface in OT, such as numerous headless devices that are inherently vulnerable. There also may be critical infrastructure equipment that highly sophisticated threat actors target in addition to more contractors and other nonemployees operating near or in power generation facilities. These situations have security requirements that can be efficiently met through the Fortinet Security Fabric:

- **Provide security-driven connectivity between the various OT and IT devices.** FortiGate Next-Generation Firewalls (NGFWs) provide internal intent-based segmentation in the OT network and visibility of the applications and protocols on the OT network. When activated within FortiGate, Secure SD-WAN delivers high-performance network connectivity that prioritizes business traffic. FortiSwitch secures access switches, and FortiAP protects access points, and then they extend that protection to the rest of the network infrastructure.
- **Control network access without encumbering authorized users.** Network access requires a well-orchestrated mix of authentication and authorization. The Fortinet Security Fabric seamlessly integrates capabilities for user identity management (FortiAuthenticator), two-factor authentication (FortiToken), and network access control (FortiNAC). FortiNAC is especially important for auditing OT devices, which can lead to productive discussions about upgrading or replacing vulnerable equipment.

The percentage of organizations that encountered a ransomware intrusion in this year's survey remained unchanged at 32%, which is the same as the previous year's group.[5]



When Secure SD-WAN is enabled on a FortiGate NGFW, it can automatically optimize the utilization of all available WAN links, while inspecting the traffic traversing any of the links.

- **Monitor the activity and location of users throughout the facility.** Power plant security officers can track smartphones and other mobile devices on the network and analyze their movement with FortiPresence Wi-Fi presence analytics. With network-based video security from FortiCamera, FortiRecorder uses facial recognition to alert the cybersecurity team when employees, contractors, or vendors have ventured into "off-limits" areas.
- **Respond quickly and appropriately to security events at the plant.** FortiSIEM provides automated response and remediation to improve breach detection. FortiSandbox advanced threat detection works in tandem to combat previously unknown threats. Automated deception technology from FortiDeceptor disguises itself to detect and remediate threats from inside and outside the network. FortiManager delivers single-pane-of-glass management, while FortiAnalyzer delivers stronger breach protection with automated reporting capabilities.

Securing transmission

Utilities have transmission infrastructure that includes high-voltage power lines and gas, water, and sewage mains. Infrastructure networks are vulnerable to physical tampering because these components are controlled from substations that are not continuously staffed. Also, a substation's Wi-Fi access points and WAN connections to the corporate office can serve as entry points for cybercriminals to attack the transmission network and even invade the corporate network.

Fortinet security solutions for transmission networks revolve around four activities:

1. **Ensuring high availability:** FortiGates can be configured for active-passive high availability (HA), which provides seamless failover in the event of a network outage or the malicious disabling of an NGFW. When Secure SD-WAN is enabled on a FortiGate NGFW, it can automatically optimize the utilization of all available WAN links, while inspecting the traffic traversing any of the links. In addition, FortiSwitch extends secure access switches out to FortiAP Wi-Fi access points.

2. **Timely incident response:** As part of a comprehensive incident management program, FortiSIEM security information and event management provides the visibility, correlation, automation, and remediation of threats in a unified solution. FortiManager provides centralized management of all Fortinet solutions, and FortiAnalyzer delivers better protection against breaches with powerful automation and log management.
3. **Centralized surveillance:** As in the case of generation systems, FortiCamera and FortiRecorder provide visual surveillance of critical physical locations to ensure infrastructure is protected. In addition, FortiPresence analytics software enables substation managers to discover any unauthorized entry into buildings or areas by tracking devices connected to the substation's Wi-Fi network. FortiPresence also analyzes patterns in a device user's visits by time of day, frequency, and location, which further aids facility security enforcement.

To protect these distributed network assets, the Fortinet Security Fabric provides advanced threat protection through a range of FortiGate NGFWs.

4. **Control the third-party and remote workforce network:** FortiAuthenticator enables authentication and manages users. FortiToken supports two-factor authentication, and FortiNAC provides network access control. In addition, FortiClient provides visibility and control of the endpoint devices that access the network.

Distribution networks

A complex array of smart metering devices, water and sewer mains, and substations form the core of a modernized distribution system. The attack surface associated with distribution networks includes Industrial-Internet-of-Things (IIoTs) devices at virtually every building in a utility's service area and hundreds of substations that may be unstaffed much of the time. It is impossible to eliminate all attacks on these networked IoT devices, but it is important to prevent any compromised devices from infecting the rest of the network.

At the same time, resiliency and total cost of ownership (TCO) of WAN connections can be challenging for unstaffed substations. FortiGate Secure SD-WAN can ensure business-critical traffic and applications are given priority over others that are not as critical. Path awareness intelligence and link remediation enable the best possible application performance and a failback mechanism. Integrated security in the FortiGate Secure SD-WAN extends security to the network edge.

Fortinet security capabilities go beyond Secure SD-WAN. Effective network segmentation with FortiGate NGFWs, supported by FortiNAC network access control and FortiSwitch secure access switches, minimizes the risks posed by vulnerabilities and malicious threats.

The visibility and rapid response enabled by FortiSIEM, FortiManager, and FortiAnalyzer solutions provide a second level of defense. A third layer of defense consists of physical protection of network assets, especially substation buildings and equipment, using FortiCamera and FortiRecorder surveillance solutions and FortiPresence presence analytics. And secure network access can be extended to third parties and remote employees with authentication and use management with FortiAuthenticator and two-factor authentication with FortiToken.

Corporate IT infrastructure

Power and utilities corporate infrastructure consists of IT network services that are critical for the operation of distributed plants and facilities. The corporate network infrastructure supports key business applications, such as enterprise resource planning (ERP), finance, and human resources. It also stores sensitive data about facilities, operations, suppliers, and customers.

The Fortinet Security Fabric provides advanced threat protection through a range of FortiGate NGFWs to protect these distributed network assets. These high-performance NGFWs can be deployed in the corporate data center, at the WAN edges of the corporate office, and in field locations. Virtual versions of the FortiGate NGFWs can be deployed in any public or private cloud that the company uses. And all the FortiGate NGFWs can inspect traffic (even encrypted packets) at near network speed and protect applications and interfaces from a variety of known and zero-day threats. In a secure context, they also perform key network functions, such as software-defined wide area networking (SD-WAN).

This network protection can be extended through FortiSwitch secure access switches out to FortiAP Wi-Fi access points. While providing connectivity to the internet or the corporate network, these access points also act as the first line of defense against intrusion.

Multiple service set identifiers (SSIDs) can be configured in the FortiGate NGFWs to provide different services or privileges to different groups of users, such as employees, customers, and contractors. When users log in to the network through the FortiAP access points, the appropriate firewall policies and authentication mechanisms are automatically enforced. Additionally, security information and event management from FortiSIEM provides automated response and remediation to help prevent breaches before they occur. FortiSandbox uses advanced threat detection to combat previously unknown threats and prevent data loss.

Lean security teams at power and utility companies can proficiently manage their entire FortiGate NGFW deployment from a single dashboard using the FortiManager centralized management and workflow automation solution. When called upon to generate reports for internal stakeholders or compliance audits, staff members can rely on the FortiAnalyzer centralized logging and reporting solution to quickly generate the required reports so they can get back to their network and security management duties.

CEOs view cyberattacks as the most significant danger facing companies in the upcoming years.[6]

When it comes to the use of cloud infrastructure and services, FortiCASB cloud access security broker (CASB), FortiWeb web application firewall (WAF), and FortiCNP cloud-native protection (CNP) help organizations manage risk by breaking down silos across multiple security solutions and cloud environments by providing centralized visibility and policy management across all cloud resources. FortiCASB monitors all Software-as-a-Service (SaaS) activity and configurations, while FortiCNP monitors activity and configuration of multiple cloud resources, including compliance and incident reporting. FortiWeb protects business-critical web applications from cyberattacks that target known and unknown vulnerabilities.

Security teams can easily gain visibility to the devices on their network and designate appropriate access to user devices with network access control from FortiNAC. Teams can also enable user identity management with FortiAuthenticator, and two-factor authentication with FortiToken. Finally, because corporate network security events must often be correlated with physical activity on the premises, the Fortinet Security Fabric also includes FortiCamera and FortiRecorder, which provide network video security and enable surveillance around critical doorways and perimeters of corporate facilities.

Securing customer experience

Customers expect easy, immediate, and automated access to their power and utilities providers, with communications using mobile applications, automated bill payments, and real-time metering information. Providers also rely on the same types of electronic channels to communicate with customers and deliver real-time information and updates about system outages or situations that may jeopardize physical safety. A distributed denial-of-service (DDoS) attack on a power and utilities website that prevents customers from getting timely and accurate information can have life-threatening consequences. Ransomware that renders a utility's data and applications inaccessible can bring operations to a standstill.

Power and utility companies can leverage the complete suite of threat protections available in FortiGate NGFWs, FortiWeb web application firewalls, and the FortiCASB cloud access security broker to minimize these risks. When these solutions are deployed at the corporate data center and in the cloud, they can be configured automatically and apply security policies consistently through a central FortiManager console with powerful automation and log management from FortiAnalyzer.

Fortinet Differentiators for Power and Utility Companies

Fortinet solutions offer unique capabilities and a proven track record in the power and utilities sector. Key differentiators include:

- **Broad visibility:** Fortinet solutions provide end-to-end visibility and security integration across IT and OT environments. For example, an industrial control system (ICS) service in all FortiGate NGFWs interfaces with the unique communications protocols used in OT systems. This feature provides contextual awareness of the entire network environment, which helps maintain trust while allowing monitoring of east-west and north-south traffic.
- **Single-pane-of-glass management:** Power and utility networks contain a variety of endpoints, including ICS, IIoT devices such as sensors and gauges, and surveillance devices such as IP-enabled cameras. Fortinet solutions help consolidate network and security infrastructure, eliminate silos, and provide single-pane-of-glass visibility and control.

- **Ruggedized appliances:** Fortinet security solutions can operate in even the harshest environments, including locales of extreme heat, cold, and electrical interference. Ruggedized FortiGate NGFWs and FortiSwitch switches can protect critical infrastructure in any deployment location.
- **Threat prevention:** Intent-based segmentation isolates critical systems to protect against threats within the network, and FortiDeceptor helps identify and respond to threats posed by malicious or compromised user accounts.
- **Proactive threat intelligence:** Securing critical infrastructure requires threat intelligence specific to ICS. Fortinet has years of experience in securing the OT space with unique knowledge and insights. Fortinet combines these insights with OT-specific threats tracked by FortiGuard Labs into OT-specific security threat reports.
- **Industry experts:** The Fortinet team includes industry experts with decades of experience securing OT systems. This deep experience informs the design of industry-leading technologies for OT security and provides relevant insight and analysis in the power and utilities sector.
- **Robust partner ecosystem:** The Fortinet Security Fabric includes integrations with other network and security technology providers. Fortinet has the largest ecosystem of partners specializing in OT cybersecurity and integration of third-party solutions through an open application programming interface (API) ecosystem and built-in Fabric-Ready APIs for solutions by Fortinet Security Fabric-Ready Partners.

Conclusion

State-sponsored threat actors, financially motivated cybercriminals, and amateur hackers will continue to be enticed by the massive impact that can result from an attack on a nation's critical infrastructure. Power and utility company security leaders must relentlessly thwart these malicious attacks with in-depth strategies based on a broad suite of integrated and automated security technologies.

The Fortinet Security Fabric provides a strong foundation and integrates disparate security elements. It unlocks policy management, security workflows, and threat intelligence sharing, which enables lean IT teams to address the full range of security needs. They can do so with minimal training and at a lower cost when compared to deploying the same number of disparate cybersecurity point products or other cybersecurity platform solutions.

[1] "2023 State of Operational Technology and Cybersecurity Report," Fortinet, May 24, 2023.

[2] "2023 renewable energy industry outlook," Deloitte, 2022.

[3] Chuck Brooks, "3 Alarming Threats To The U.S. Energy Grid – Cyber, Physical, And Existential Events," Forbes, February 15, 2023.

[4] "2022 ICS/OT Cybersecurity Year in Review," Dragos, 2022.

[5] "2023 State of Operational Technology and Cybersecurity Report," Fortinet, May 24, 2023.

[6] "Tim Human, "CEOs name cyber-risk as top threat in 2022, according to PwC survey," IR Magazine, January 27, 2022.

November 30, 2023 10:07 AM

1218398-A-0-EN