

SOLUTION BRIEF

Fortinet and Schweitzer Engineering Laboratories Security Solution

Rugged Computing Platform for Substation, Industrial, and Harsh Environments

Executive Summary

Energy utilities face a rapidly evolving cybersecurity threat landscape that requires the modernization of their infrastructures to enhance their security posture. In particular, utilities need to implement new technologies designed to ensure both high reliability and resiliency. To better manage the extensive and increasingly diverse data streams handled by grid control systems, many utilities are now working to bring more processing capability, efficient automation, and enhanced cybersecurity into their substations.

To effectively implement real-time processing, analysis, and the prevention of cybersecurity threats, however, protections and interventions need to be placed closer to where industrial processes occur. Placing virtual cyber services on edge computing platforms can significantly increase cybersecurity responsiveness while reducing cost and minimizing managerial overhead.

Joint Solution

Integrating the SEL-3355 with Fortinet’s virtual FortiGate NGFW, FortiAnalyzer, and FortiManager—enabled through Fortinet’s Fabric-Ready Program—provides organizations with an industrial-grade solution that simplifies operations, reduces managerial inefficiencies, and enables practitioners to deliver excellent responsiveness. The SEL-3355 offers a ruggedized computing platform based on Intel’s industry-leading Xeon processors and no moving parts, enabling SEL to achieve a mean time between failures (MTBF) of over 300 years. Fortinet FortiGate solutions provide zone isolation and granular policy control, while FortiManager enables the rapid scaling of large firewall environments. FortiAnalyzer then delivers Fortinet Security Fabric analytics and automation to better detect and respond to cyber risks.

SEL-3355 and Fortinet Use Cases

Energy utilities are facing complex challenges in today’s rapidly changing energy landscape. Some of these critical complexities include:

- **Decentralization:** The increasing adoption of renewable energy sources such as solar and wind power, as well as the growth of distributed energy resources (DERs) such as batteries and microgrids, are decentralizing the energy grid and making it more complex to manage.
- **Cybersecurity:** Energy utilities face significant cybersecurity risks as they increasingly adopt digital technologies, including the threat of cyberattacks targeting critical infrastructure.
- **Aging infrastructure:** Many energy utilities are dealing with aging infrastructure that needs to be upgraded or replaced to meet the demands of a modern energy grid.

Solution Components

- Schweitzer Engineering Laboratories SEL-3355 Computing Platform
- Fortinet FortiGate Next-Generation Firewalls (NGFWs)
- Fortinet FortiManager
- Fortinet FortiAnalyzer

Solution Benefits

- Complete automation control and operator station functionality in a single package directly on the plant floor without the concern of environmental conditions
- Processing power and rugged hardware necessary for operating in critical infrastructure environments
- Log management, analytics, and reporting with a single management console and the ability to proactively identify and remediate risks for the entire attack landscape
- Convergence of networking and security into a single, integrated system that can expand to any edge
- Centrally manage network and security policies for thousands of FortiGate NGFWs



- **Integration of renewable energy:** Integrating renewable energy sources into the energy grid can be challenging, requiring new technologies and processes to manage the intermittency of these resources.
- **Regulation:** Energy utilities are subject to a complex regulatory environment, with many different regulations and standards with which they must comply.
- **Integration of new technologies:** Energy utilities must navigate the integration of new technologies, such as artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT), into their operations while ensuring that these technologies are secure and reliable.
- **Grid resilience:** Ensuring the resilience of the energy grid in the face of natural disasters, cyberattacks, and other threats are becoming increasingly important and requires new approaches and technologies.

Meeting these challenges will require innovative solutions, including collaboration between stakeholders and investment in new technologies and infrastructure. In this new environment, the SEL-3355's critical role becomes even more significant as it hosts virtual instances of Fortinet Security Fabric solutions, including Fortinet FortiGate Next-Generation Firewalls, FortiManager, and FortiAnalyzer. The FortiGate provides network segmentation and zone separation to protect critical business processes. FortiManager can then manage and operate multiple FortiGates, while FortiAnalyzer offers device visibility and anomaly detection to deliver automated incident response. By combining the SEL-3355 with Fortinet's virtual cybersecurity solutions, organizations can realize a localized, consolidated, and highly secure edge computing platform that can ensure data integrity and meet business objectives to simplify the modernization of all energy utility applications.

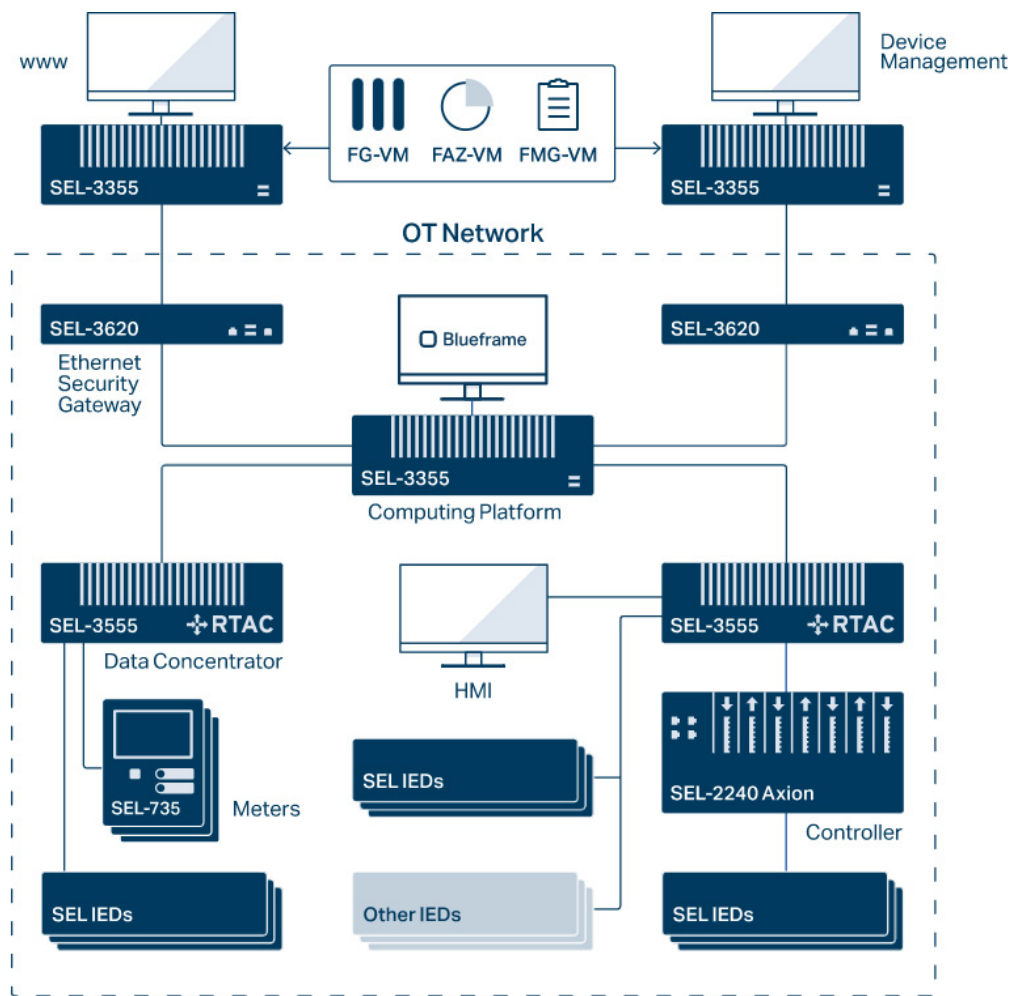


Figure 1. The SEL-3355 Computing Platform integration with FortiGate NGFW, FortiAnalyzer, and FortiManager provides an industrial-grade solution to simplify operations, reduce managerial inefficiencies, and deliver excellent responsiveness.



Solution Components

SEL-3355 Rugged Computing Platform

SEL computing platforms are built to ensure reliable performance in the most demanding utility and industrial applications. These substation-ready platforms feature a solid-state design with an advanced thermal management system—eliminating all fans, vents, and moving parts. They are engineered to withstand extreme events and conditions, ranging from electrical surges and electromagnetic interference to seismic activity and corrosive agents. In addition, SEL computing platforms offer some of the broadest operating temperature ranges in the industry: -40° to $+75^{\circ}\text{C}$ (-40° to $+167^{\circ}\text{F}$) or greater.

All SEL computing platforms are designed and tested to meet the same rigorous standards as SEL's protective relays. As a result, SEL computing platforms have a mean time between failures (MTBF) of over 300 years—a metric based on actual field performance rather than predictive modeling. SEL demonstrates its confidence in these products with a worldwide 10-year warranty, which is unsurpassed in the industry.

Integration with FortiGate

The SEL-3355 and Fortinet FortiGate Next-Generation Firewall are critical in ensuring the cybersecurity of energy substations. Some of the specific use cases for the combined solutions in energy substations include:

- Network segmentation: Segment the substation network into different security zones to reduce the attack surface and prevent unauthorized access.
- Threat detection and prevention: Detect and prevent cyberthreats, including malware, network attacks, and unauthorized access attempts.
- Real-time monitoring: Actively monitor the substation network to detect suspicious activity or anomalies in real time.
- Logging and reporting: Log all network activity and generate reports to allow an operator to review and analyze data to identify potential security threats.
- Remote access control: Control remote access to the substation network, ensuring that only authorized personnel can access critical systems and data.

Integration with FortiAnalyzer

The SEL-3355 and FortiAnalyzer provide centralized logging, reporting, and analytics capabilities for network devices deployed in energy environments in the following ways:

- Collect log data across the environment
- Analyze log data to detect anomalous activity
- Monitor network activity and alert on suspicious behavior
- Automatically create compliance reporting
- Trigger a security response in the event of a cyber incident



Integration with FortiManager

The SEL-3355 and Fortinet FortiManager deliver centralized network management that can be used to manage and secure energy environments, including energy substations and distribution networks. Some of the key ways these solutions can be utilized include:

- Security policy management for consistent distribution and enforcement
- Asset management
- Centralized monitoring and reporting
- Automated compliance reporting
- Automation between systems to streamline operation

About Schweitzer Engineering Laboratories, Inc. (SEL)

In a mission to make electric power safer, more reliable, and more economical, Schweitzer Engineering Laboratories, Inc. (SEL) designs and builds digital products and solutions that protect, monitor, control, and secure power systems worldwide.

SEL is a 100% employee-owned company headquartered in Pullman, Washington, and has been manufacturing products in the United States since 1984. Now serving customers in 168 countries, SEL provides unmatched technical support, customer service, and a 10-year worldwide warranty.



www.fortinet.com