

**SOLUTION BRIEF**

# Fortinet and Phoenix Contact Security Solution

## Industrial Switching Platform for Enhanced Security and Simplified Deployments

### Executive Summary

Phoenix Contact and Fortinet have established a strategic technology partnership to address the challenges of cyberthreats by integrating the Fortinet FortiGate Next-Generation Firewall (NGFW) into Phoenix Contact’s leading-edge Raptor models, which support module co-processors. This partnership enables customers to deploy a single appliance for OT applications to manage and secure their field devices and network communications remotely.

### The Challenge

As IT and OT networks converge, increasing cyberthreats within OT applications are a growing concern. Security controls against these new and existing cyberthreats must be tightly integrated within the communications architecture of these connected systems. Mission-critical networks (OT environments) such as power utility, nuclear, water utilities, oil and gas, and more must deploy security measures to protect against intrusions. Additionally, OT environments typically operate in harsh, remote, and inaccessible environments. Thus, mission-critical infrastructures require reliable, high-performing communications, which can be challenging due to cybersecurity concerns.

### Joint Solution

Phoenix Contact and Fortinet have partnered to deliver an industry-leading security solution to address these unique OT challenges. The integration of Phoenix Contact Raptor EP series switches and Fortinet FortiGate delivers high-performance networking and cybersecurity functionality in a single, highly hardened package that may be deployed to the very edge of industrial networks.

### Solution Components

The Raptor is an intelligent cybersecurity hardware with 64 Gb/s full line speed and 4 × 10Gb/s + 24 1Gb/s ports running a feature-rich embedded OS. The Raptor’s embedded OS is an all-encompassing operating system that supports L2/L3 switching and routing on a single platform. Its modular system of field-replaceable modules, redundant hot-swappable power supplies, and ability to run third-party software applications make it a very flexible platform for today and the future.

FortiGate NGFWs protect data, assets, and users across today’s hybrid environments. Built on patented Fortinet security processors, FortiGate NGFWs accelerate security and networking performance to effectively secure the growing volume of data-rich traffic and cloud-based applications. FortiGate NGFWs, backed by the threat intelligence of FortiGuard AI-Powered Security Services, help you prevent cyberattacks and mitigate security risks with consistent, real-time protection and responses against even the newest and most sophisticated threats.

### Solution Integration

The Phoenix Contact Raptor series switches support an optional co-processor (CoPro) module, which allows third-party software to be embedded within the switching fabric. For this integration, the CoPro is connected between the switch’s WAN and LAN interfaces, where it runs the FortiGate software.



### Solution Components

- Fortinet FortiGate NGFW and FortiManager
- Phoenix Contact Raptor

### Solution Benefits

- Singular multiservice platform solution
- High-performance, high-reliability NGFW for harsh OT environments
- Robust industrial design, compliant with IEC 61850 and IEEE 1613 standards
- Ease of implementation
- Simplified GUI management, smaller footprint, single power source, simple integration

Combined with the FortiGate NGFW, Raptor enables industrial applications to have “best-in-breed” security solutions for their OT applications. This includes firewall functionality and Fortinet advanced threat intelligence capabilities, such as IPS, application control, vulnerability management, and malware protection, specific to OT environments.

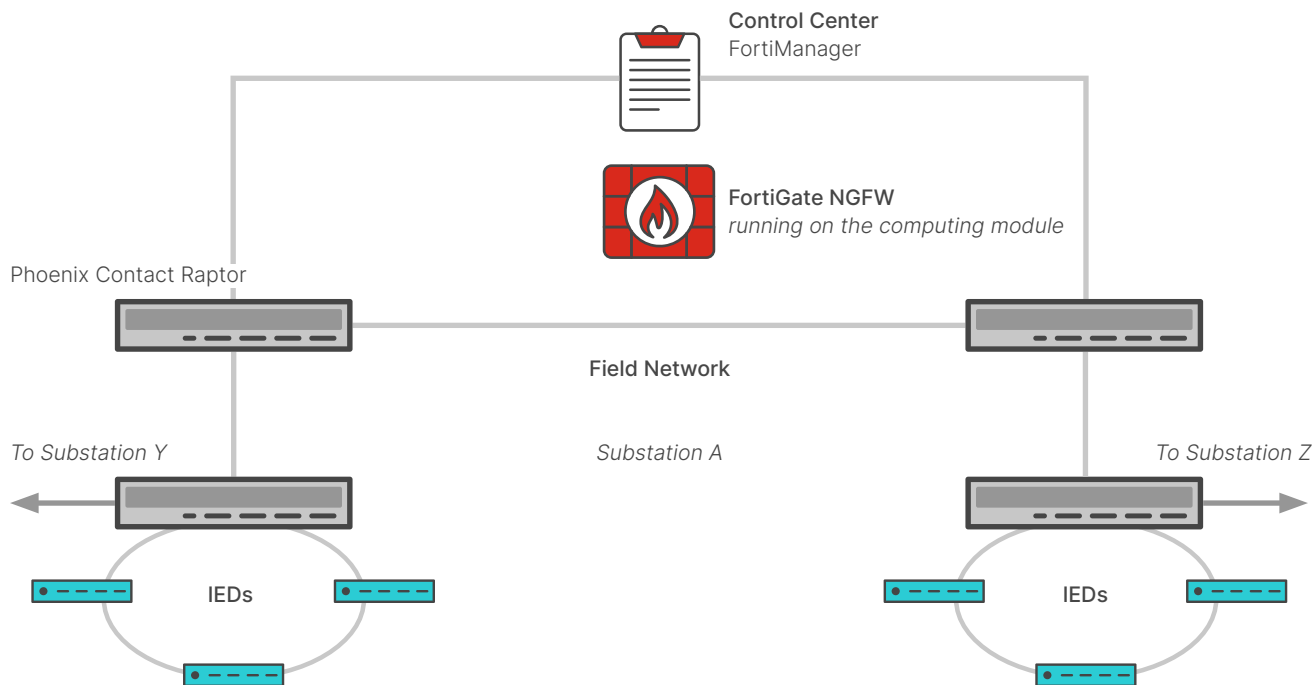


Figure 1: Fortinet and Phoenix Contact Integration

### Joint Use Cases

Use case #1: Advanced networking and cybersecurity for electric substations: A modern electric substation demands sophisticated cybersecurity protection and high-speed, high-availability networking infrastructure for the electric grid’s critical OT systems. Deploying FortiGate NGFW on the Raptor creates a single rack unit or DIN rail-mounted system with redundant power supplies that meet the rigorous requirements of IEC 61850-3.

Use case #2: Unified cybersecurity across IT and OT: Critical infrastructure operators need to manage cybersecurity for both IT and OT systems. A unified approach and technology stack across both environments bring numerous benefits but can be challenging because of the harsh environments of many OT systems. The Phoenix Contact Raptor enables Fortinet technology to be extended to the edge of the harshest of environments.

### About Phoenix Contact

Phoenix Contact is a global market leader based in Germany. We are known for producing future-oriented products and solutions for the electrification, networking, and automation of all sectors of the economy and infrastructure. With a global network reaching more than 100 countries with over 22,000 employees, we maintain close relationships with our customers, something we believe is essential for our common success. Our wide range of innovative products makes it easy for our customers to implement the latest technology in various applications and industries. This especially applies to the target markets of energy, infrastructure, industry, and mobility.

