SOLUTION BRIEF

Fortinet and RAD Security Solution

Securing industrial control systems with Fortinet at level 0 and 1 using built-in Edge Computing and ruggedized gateways

The IoT revolution in businesses goes hand-in-hand with digital transformation. The complexity of networks and infrastructure has never been higher with far-reaching implications for securing safety and production of highly valued assets in Operational Technology (OT) environments. Recent years have brought security to the forefront, especially in the industrial and critical infrastructure sectors.

The top three major challenges IIoT brings to security can be summarized as follows:

- **Cyber Security Threats** - unreliable networks are exposed to malicious attacks. Multiply this by the countless devices that are already – or about to be – deployed and the results can be catastrophic.
- **Operational Complexity** - installing, configuring, maintaining and replacing thousands of edge devices require careful planning, organization, and the right tools and capabilities to avoid costly mistakes and lengthy delays.
- **Data Usability** – thousands, and even millions of IoT devices in the field can process, transmit and receive data. That data is then aggregated, but not necessarily in filtered format. Thee need to transform this data to actionable information requires a cost-effective Edge Computing gateway.

Securing IIoT requires access control, secure access points, visibility into all devices on the network, constant monitoring, unified management, and automated responses to threats. Security solutions also need to meet extreme performance requirements, be available on-demand and be provisioned and de-provisioned in real time while the environment they are protecting is adapting to demands.

Security for today's IIoT network infrastructure must include a smart solution that can provide the combined benefits of cyber security, and cost-effective data usability across all security devices in the OT network for more effective management.

Joint Solution Description

The Fortinet and RAD integrated solution addresses the above challenges, by leveraging the Fortinet Security Fabric's open architecture that connects traditionally disparate security solutions into a unified framework. This allow such solutions to dynamically adapt to evolving infrastructure in order to defend its rapidly changing attack surface. Fortinet's open approach extends the broad visibility, integrated threat detection and automated response of its Security Fabric architecture to RAD's solutions through the Fabric APIs. The integration results in a **flexible, ruggedized and cost-effective joint solution that addresses the growing IIoT visibility and security challenges.**

Joint Solution Benefits

- Highly secure Industrial IoT (IIoT) Edge Computing and ruggedized gateway solutions
- Unrivaled level 0 and 1 security in combination with Fortinet FortiGate and FortiSIEM solutions
- Greater functionality with flexible deployments for distributed and remote locations
- Integrated security aggregation and management for increased security effectiveness of the entire solution
- Lower total cost of ownership with a reduced number of appliances and associated costs

FORTINET Fabric-Ready

Caption: Benefits of the Fortinet-RAD joint solution

Solution Components

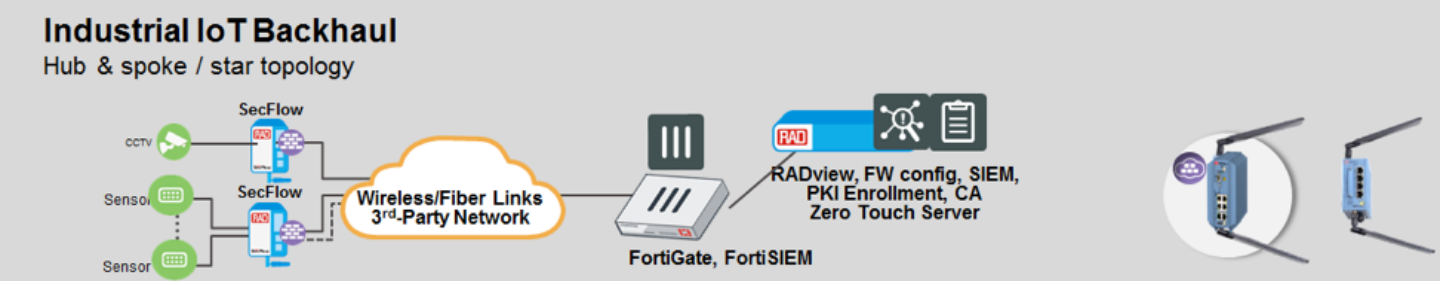
Fortinet FortiSIEM & RAD SecFlow

The integration of FortiSIEM with RAD's SecFlow offers a viable solution to the growing complexity of managing network operations by providing a comprehensive, scalable way of monitoring all OT and IIoT security systems. RAD's SecFlow is able to share threat intelligence and comprehensive event logs with FortiSIEM to correlate security events across protected IIoT devices and all other Fortinet Security Fabric components.

RAD's SecFlow constitutes the level 0 and level 1 ruggedized edge computing solution for Fortinet. Acting as the hub, Fortinet collects data from the remote gateways of RAD.

RAD helps tackle IIoT challenges with -

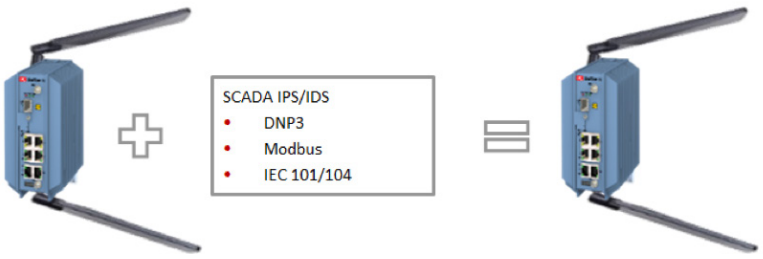
- **Connectivity:** Always-on seamless connectivity over any media with resiliency & redundancy options
- **Security:** End-to-end IPsec VPN tunnels over private and public networks with firewall and encryption
- **Edge computing:** Fog/edge application support to minimize latency and maximizing efficiency
- **Simplified operation:** Secure zero-touch configuration for automated installation and provisioning



Caption: Level 0 and 1 ruggedized Edge Computing solution for Fortinet

Joint Use Cases

- Edge Computing Use Cases
  - IPS\IDS for SCADA– serving DNP3, Modbus, IEC 104 protocols; converting legacy RTU protocols to their IP equivalents and activating IPS\IDS on the converted IP traffic (in the future, this could be the Fortinet containerized IPS\IDS)
  - Protocol conversion gateway
  - ICS software (e.g., open Embedded RTU\PLC) – containerizing PLC capabilities within a secure and ruggedized gateway
  - Sensor aggregation software
  - Store and Forward or periodic broadcast for low speed and infrequent data synch (e.g. metering aggregation)
  - Access Control Software
  - MQTT, Azure, other

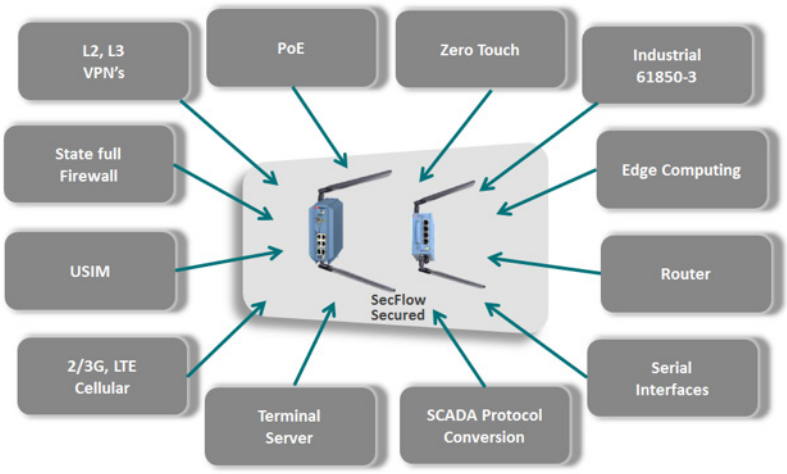


Fortinet Security Fabric

The Fortinet Security Fabric is an architectural approach that unifies the security technologies deployed across the digital network – including multi-cloud, endpoints, email and web applications and network access points – into a single security system integrated through a combination of open standards and a common operating system. These same types of solutions are integrated into the OT environments that are enhanced through the integration of advanced threat protection technologies and a unified correlation, management, orchestration, and analysis system.

RAD SecFlow

RAD's next generation SecFlow industrial IoT (IIoT) gateway hosts third-party applications, such as Fortinet's, using the most advanced, LXD container-based Edge Computing capabilities. In addition, it enables efficient, secure and fast connectivity of IIoT devices over wireless, fiber and even copper networks – either public or private. The SecFlow features a Global SIM, dual SIM and a dual cellular modem supporting flexible connectivity. Advanced Ethernet and IP feature-set provides reliable and secure Layer 2 and Layer 3 communications, while serial protocol handling with transparent tunneling/protocol conversion and terminal servers capabilities support all RTU traffic. In addition, the SecFlow supports the environmental needs of Level 0 and Level 1 of the solution fabric.



About RAD

RAD is a leader in Service Assured Networking (SAN) solutions for critical infrastructure. We address all communication needs of the utilities, transportation and government sectors with always-on reliability and mission-critical protection. We offer best-of-breed SAN solutions that are used for cyber-secure industrial IoT (IIoT) and operational WANs, fog/edge computing, TDM to packet migration, distance Teleprotection and distribution automation, as well as Smart/Safe City deployments.

Founded in 1981, RAD has an installed base of more than 16 million units and is a member of the $1.46 billion RAD Group of companies, a world leader in communications solutions.

August 26, 2019 9:09 AM

478566-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2019:SB-Fortinet-and-RAD:sb-fortinet-and-rad-082619-907am