SOLUTION BRIEF

Fortinet and Ribbon Security Solution

Protecting Critical Infrastructure from Cyberattacks

Executive Summary

Comprehensive protection of CI internal communication networks and operational technologies to prevent hacking and provide alerts of attacks.

Challenges

Critical infrastructure (CI) companies and industrial control/SCADA systems are basic components of a nation's infrastructure. This makes CI a prime target for cyberattacks. Threats against CI and industrial control/SCADA systems are persistently growing more sophisticated and targeted, as cyber terrorists are becoming smarter and more calculated.

Proper protection of CI is a particularly complex matter. You must secure multiple locations against cyberattacks that are increasing in frequency and sophistication. These are not just clever hackers out for a thrill. Attacks against CI facilities are focused, complex efforts by attackers with funding and resources, backed by unfriendly governments and other deep-pocket organizations. They are creating attacks that trigger immediate damage and/or leave the way open for future infiltration.

As high-profile targets, CI facilities are particularly vulnerable to these risks. Cyberattacks have become a weapon of war, and CI is the main target in the crosshairs.

Utilities and CI sectors face multiple cybersecurity challenges:

- **Aging infrastructure:** Utilities and many CI networks operate legacy equipment filled with well-known security vulnerabilities. The hardware and proprietary protocols often do not address security at all. These protocols are easily corrupted, whether by malicious intent or by accident, leaving the network particularly exposed. Old systems, aging technology, and limited awareness of basic enterprise cybersecurity place these networks in an especially vulnerable state.
- **Inefficient segmentation:** Failure to effectively segment the enterprise network from the operational network allows cyber threats to reach the operational networks via the enterprise. Furthermore, if an attacker successfully penetrates a site, he can easily impersonate a legitimate entity to use valid ports and to propagate the attack to a neighboring site. Therefore, efficient segregation of substations from each other is highly essential.
- **Cybersecurity regulation compliance:** NERC CIP V6 and the Cybersecurity National Action Plan (CNAP) are setting regulations to enhance utility and CI security and resilience. Soon, all of the relevant players will have to comply. Utilities are of great concern in particular, and are now being highly regulated.
- **Budget:** These cybersecurity challenges must usually be met within the constraints of resources, staff, and budget.

Joint Solution Benefits

- Integrates NFV-based distributed attack mitigation with centralized administration and SCADA anomaly and threat detection
- Automates discovery, presentation, and validation of the network topology of all SCADA devices
- Combines multiple security functions to protect against man-in-the-middle, lateral, and zero-day attacks
- Consolidates connectivity with security, creating a streamlined, low-cost, high-reliability architecture
- Consolidates multiple pre-certified best-of-breed security functions on a single form factor, covering SCADA anomaly detection, encryption, and a next-generation firewall
- Leverages the award-winning FortiGate enterprise firewall platform to provide unparalleled network security protection

FORTINET Fabric-Ready

Protecting critical infrastructure from cyberattacks is particularly challenging. It must provide comprehensive protection of the CI's internal communication network and operational technologies, preventing hacking and providing alerts of attacks. It must discern tangible threats from a multitude of reported events. Ribbon's Muse™ Cyber Security is a scalable and flexible network functions virtualization (NFV)-based solution that hosts several "best-of-breed" security virtual network functions (VNFs) on a single Ribbon Mercury™ NFV appliance, orchestrating them to protect against all of the above-mentioned challenges.

Joint Solution

Ribbon's Muse Cyber Security Suite addresses these challenges by providing a holistic cyber security solution for critical infrastructure and operational networks. The solution combines encryption to block man-in-the-middle attacks, Fortinet virtual network functions to segregate substations from each other to prevent lateral attacks, and a SCADA anomaly detection system to identify threats, rate risks, and alert of zero-day attacks.

Joint Solution Components

Ribbon's Muse Cyber Security Suite includes Mercury NFV platform, Cyber Security VNFs, Muse Orchestrator, and SCADA Anomaly Detection engine.

The Fortinet FortiGate VM is a virtual appliance version of the market-leading, high-performance FortiGate next-generation firewall (NGFW). FortiGate VM shares the same advanced features of the FortiGate NGFW, enabling and enforcing security policies across all environments and providing single-pane-of-glass management. FortiGate VM ensures complete application security and secure connectivity by augmenting microsegmentation with advanced L7 security. FortiGate VM offers a consistent security posture and protects connectivity across public and private clouds, while high-speed virtual private network (VPN) connections protect data.

Joint Solution Integration

The Fortinet FortiGate VM, which serves as a gateway for each substation, controls connectivity between authorized elements to and from the substations. It is also capable of analyzing traffic against known attack attempts and viruses, and issues appropriate alerts when detected. The NGFW also provides IPsec encryption when required.

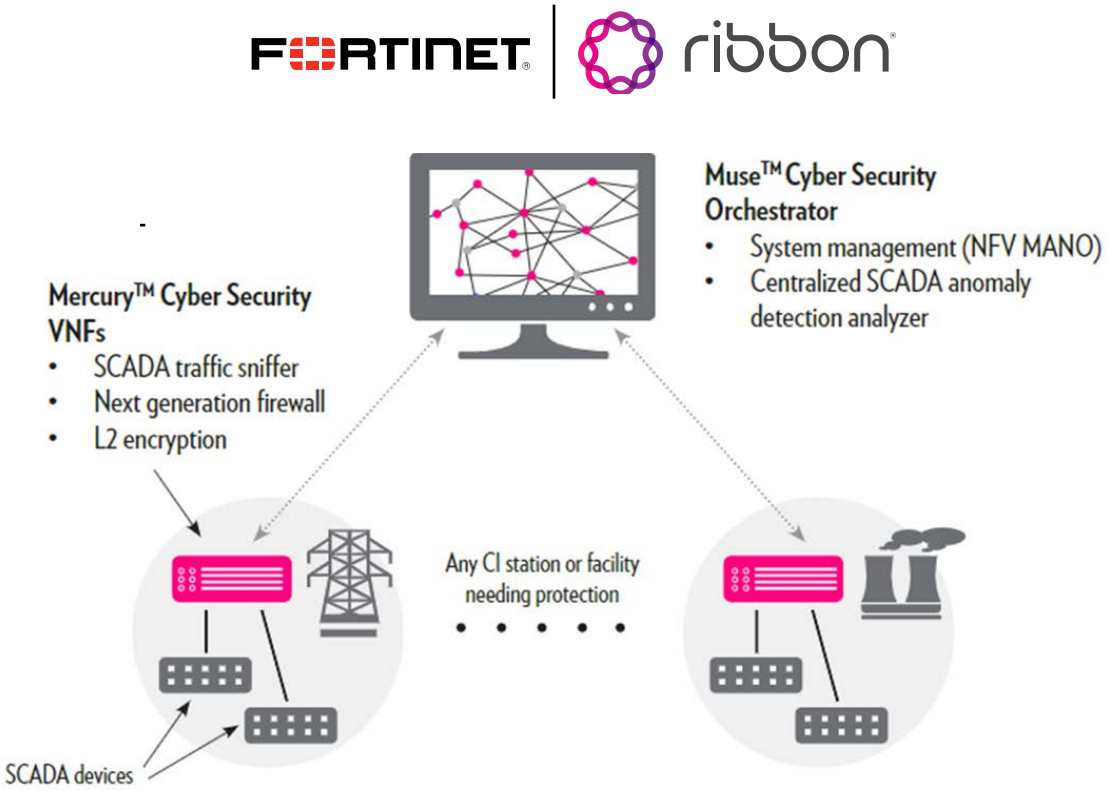

Figure 1: Joint solution.

Representative Use Case

Protection of gas and oil infrastructure systems for conveying gas and oil via pipelines that are deployed across regions, countries, and continents, and through pumping hubs and control points scattered over large distances. These are operated and controlled from a central command office by communicating with remote taps, pumps, and leak detectors, using SCADA-based protocols running on long-distance networks.

The solution includes: the deployment of a Mercury appliance in each of the pumping hubs and at all remote control points and installing VNFs for encryption, FortiGate VM NGFW, and SCADA sniffing on each of the Mercury units. In addition, the Muse NFV Orchestration system, the SCADA Anomaly Detection system, and the FortiGate VM NGFW and encryption management systems are installed at the main site.

About Ribbon Security Solution

Ribbon Communications (Nasdaq: RBBN), which recently merged with ECI Telecom Group, delivers global communications software and network solutions to service providers, enterprises and critical infrastructure sectors. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge IP solutions, UCaaS/ CPaaS cloud offers, leading-edge software security and analytics tools, as well as packet and optical networking. To learn more about Ribbon visit rbbn.com.

October 20, 2020 5:04 AM

814459-A-0-EN

D:\Fortinet\Solution Brief\Grey Solution Brief\Ribbon Communications\sb-fortinet-and-ribbon-security-solution-10202020