ribbon ECI THE ELASTIC NETWORK

MUSE™

CYBER SECURITY SUITE

COMPREHENSIVE PROTECTION FOR CRITICAL INFRASTRUCTURE

Protecting critical infrastructure from cyber-attacks 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.

The Muse Cyber Security Suite meets these challenges, and enables geographically-distributed critical infrastructures to easily deploy, manage, and update cyber protection solutions. It protects against multiple attack vectors on OT and SCADA networks, including man-in-the-middle, lateral, and zero-day attacks.

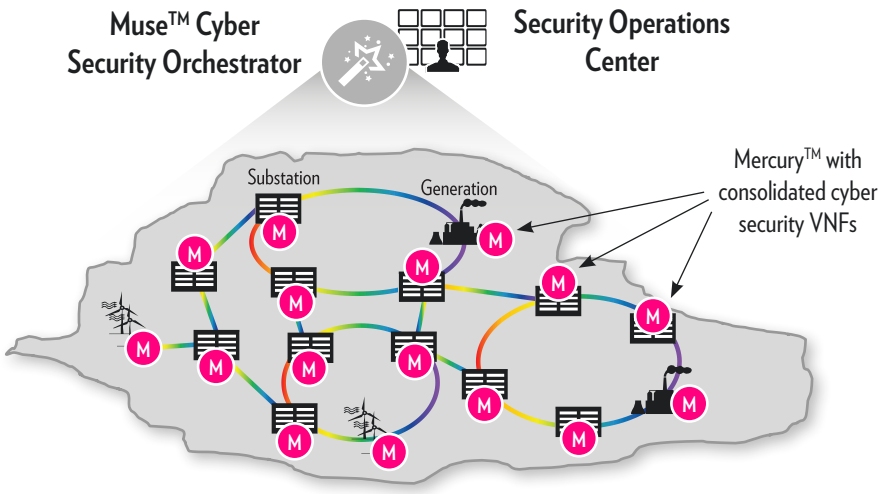
Economical run-time platforms deployable at any CI facility consolidate multiple cyber-security functions, preventing cyber-attacks before they can cause harm. The platforms and their functions are managed centrally and provide SOC personnel with early warnings of anomalies and impending attacks.

Industry-leading SCADA security fully covers OT

Prevents attacks at facility points of access

Zeroes in on real threats by combining multiple security VNFs

Combines security with connectivity for low TCO

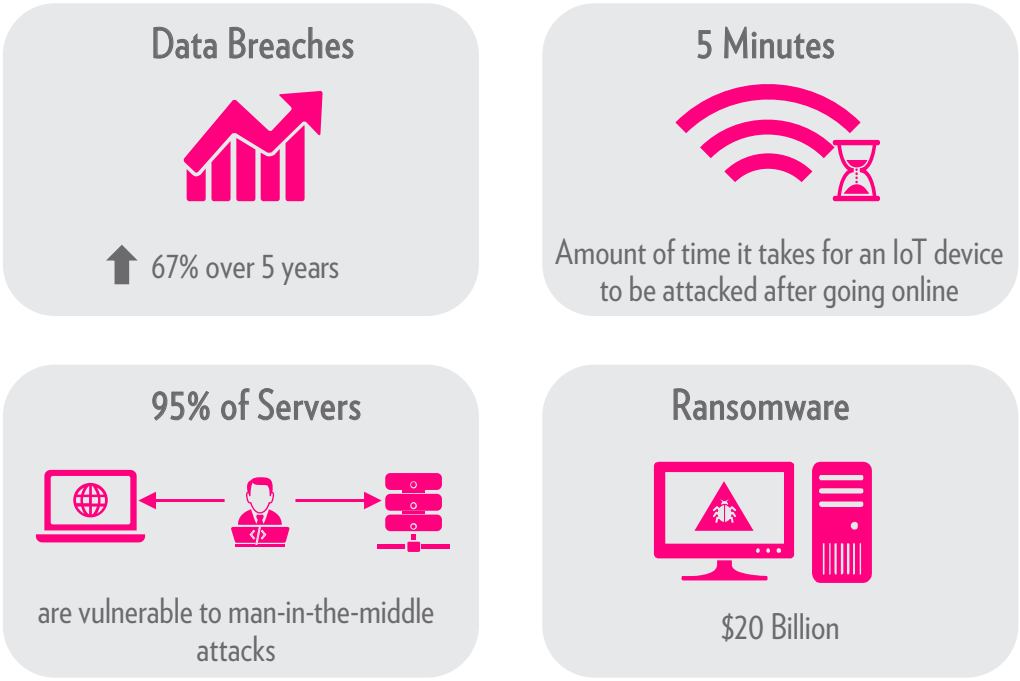


UNIQUE CHALLENGES IN PROTECTING CRITICAL INFRASTRUCTURE

In the past, industrial control systems were separated from corporate networks and the Internet. Gapping, combined with physical security measures, were sufficient for securing these systems. Eventually, organizations connected their SCADA networks with other networks in order to cut costs and share operational information. But eliminating this separation of systems, exposes the control networks to hackers.

A comprehensive cyber security solution is needed to cover a vast distributed infrastructure that inherently has multiple points of vulnerability. Specifically, it should address the following three threat scenarios with a distributed, scalable, and low TCO solution.

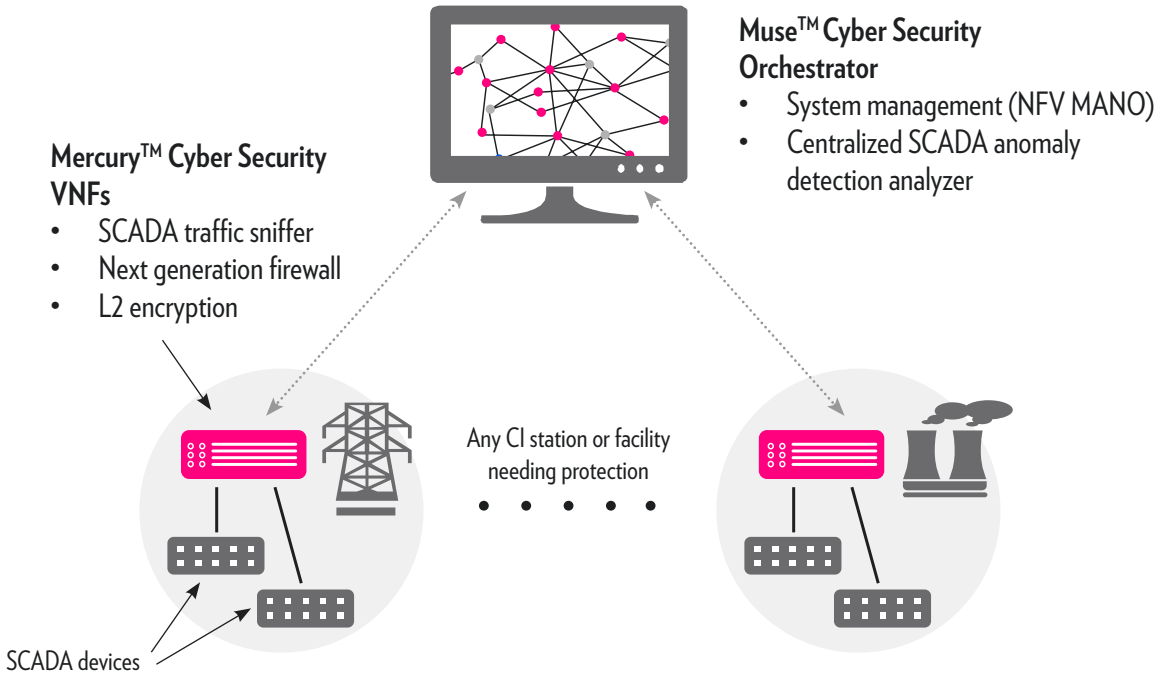
- **Man-in-the-Middle Attack.** The attacker secretly intercepts and changes the communication between operating stations, including falsifying instructions. This can sabotage the proper operation of edge control devices and present a false pretense of "situation normal" to the central command station, even when problems occur.
- **Lateral Attack.** The attacker overcomes the communications protection of an individual substation, and uses this as a launching point to attack neighboring substations. The attack proliferates to edge control devices throughout the network, replicating the situation of the first threat.
- **Unrecognized (zero-day) Attack.** This uses legitimate ports and recognized stations to transmit impostor instructions or to gather information across the network. Through the clever use of legal requests and ordinary commands, attackers can disrupt the operation and cause major losses without being blocked by the prior detection mechanisms of known attacks. Moreover, such attacks can work incrementally, causing only minor impacts at a time, but in a way that the cumulative loss is significant.



MUSE CYBER SECURITY SUITE ARCHITECTURE

Muse 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, a secure gateway 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. The Muse Cyber Security Suite consists of the following components:

- **Mercury NFV platform:** Unifies VNF-based cyber security functions into a consolidated run-time form factor, deployed at every substation. It is available as a standalone platform, or as an integrated blade within the Neptune transport system, with both approaches meeting mission-critical performance requirements.
- **Cyber Security VNFs:** These run in Mercury, and include:
  - Traffic sniffing, which gathers critical information on operational traffic flowing among the substations. A centralized SCADA Anomaly Detection engine processes and analyzes this traffic information.
  - Next-Generation Firewall (NGFW), which serves as a gateway for each substation, controlling 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.
  - L2 Encryption, which delivers encryption when traffic is Ethernet rather than IP, using AES 256-bit keys.
- **Muse Cyber Security Orchestrator:** Centrally and securely manages all aspects of Mercury hardware and its cyber security VNF software, via a single pane of glass.
- **SCADA Anomaly Detection engine:** Located alongside Muse Orchestrator in the central SOC, this automatically discovers the assets across the OT networks, employing distributed traffic sniffing. It learns the finite set of connections, conversations, and commands and creates a fine-grain behavioral system baseline that characterizes legitimate traffic behavior for each asset in the network. Advanced algorithms are applied to the baseline to detect anomalies that may indicate an attack or another problem.



PROTECTION WITH LOW TCO

Muse Cyber Security also addresses the customer's goal of low TCO by leveraging the following capabilities:

- Distributed NFV technology controlled centrally by a cloud-based orchestrator, ensures an economical and future-proof solution through its ability to remotely and securely add or modify cyber security applications as risks evolve.
- Mercury runs all required security VNFs on a single platform, eliminating the need to install and manage discrete hardware for each function. Moreover, Mercury is implementable as a blade, integrated within the Neptune packet networking system.

COMPREHENSIVE PROTECTION FOR CRITICAL INFRASTRUCTURE

Muse Cyber Security provides multiple benefits:

CURRENT CHALLENGES	MUSE CYBER SECURITY VALUE
Separate systems for attack mitigation and threat detection	Integrates NFV-based distributed attack mitigation with centralized administration and SCADA anomaly and threat detection.
Limited visibility of the operational technology (OT)	Automatic discovery, presentation, and validation of the network topology of all SCADA devices.
Ensuring system integrity, that all commands and control functions are genuine and correct	Validates OT network on the assumption that it has been breached and that SCADA C&C may be altered by an intruder.
Protection against multiple attack vectors	Combines multiple security functions to protect against man-in-the-middle, lateral, and zero-day attacks.
Network connectivity and network security are detached	Consolidates connectivity with security, creating a streamlined, low-cost, high-reliability architecture.
Multiple security mitigation functions from multiple vendors	Consolidates multiple pre-certified best-of-breed security functions on a single form factor, covering SCADA anomaly detection, encryption, and a next generation firewall.
New cyber security threats drive new security tools on separate solutions	Open cyber security platform capable of implementing additional security functions.

Contact us to discover how Muse™ can secure your critical infrastructure from cyber attacks