LinkGuard™ CASE STUDY

Zero Trust Breach Prevention

Network Command & Control Protection for Multi-National Refinery

Overview

Schneider Electric (SE), one of the world's largest industrial automation companies, has partnered with Blue Ridge Networks (BRN) to deploy the LinkGuard™ zero trust breach prevention solution to secure its customers' critical distributed Operational Technology (OT) and industrial control system (ICS) interoperability with Information Technology (IT) network operations. LinkGuard has been selected by one of SE's major petrochemical customers in Central America to protect network command and control of its refinery operations.

Customer Use Case

The petrochemical company selected LinkGuard to establish secure interoperability of its SCADA networks and industrial control systems with remote command and control from a central site. LinkGuard delivers a solution compatible with industry Safety, Productivity, and Reliability standards.

Solution Summary

LinkGuard is built on a technology foundation that has no reported breach in over 20 years of utilization. It segments, isolates, and contains critical OT/IT systems and network operations with independent, autonomous authentication and control to eliminate external discovery and data exfiltration. Overlay deployment of LinkGuard software and systems fully compatible with OT systems and IT operations coupled with its autonomous operation minimizes integration and sustainment complexity to deliver an order of magnitude or more operational cost savings compared to alternative approaches.

Schneider Electric

Resilient OT/IT Breach Prevention

- Eliminates discovery and data exfiltration of critical OT/IT systems and network operation
- Materially reduces operational and reputational cybersecurity risks for customers

Minimal Disruption & Overhead

- Deploys rapidly, including training and documentation, to protect distributed operations
- Does not require any changes to network infrastructure
- No anticipated down time and maintenance actions

Operational Efficiency

- Ability to securely operate autonomously around the clock (24x7x365)
- Increased production rates and efficiency for the multinational company

High ROI

- Easy deployment and operation efficiency delivers an order of magnitude or more cost savings to customers for secure network operations
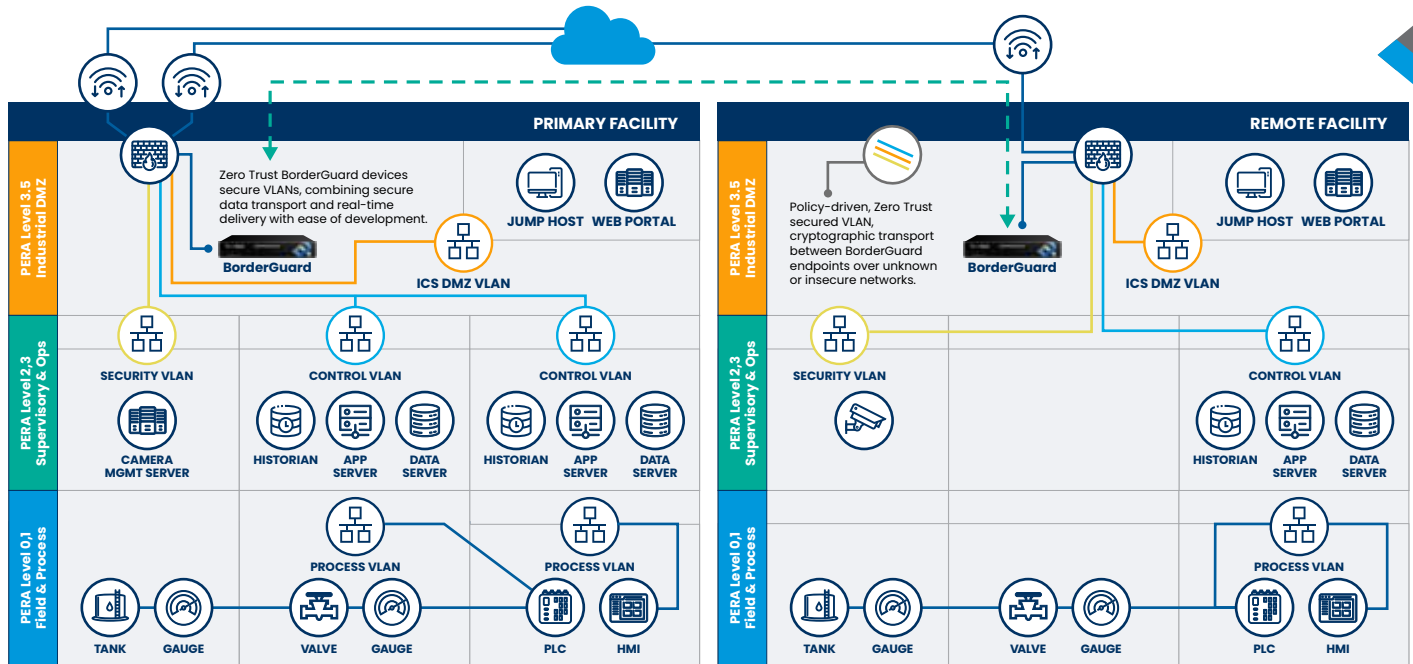
Customer Need
Secure command & control (C&C) of systems ensuring Safety, Productivity, and Reliability

Automated control of connected operational technology (OT) devices provides a wealth of opportunity for productive, efficient uses. But this interconnection also increases the attack surface introducing weak points within an organization network infrastructure for cyber attackers to exploit inherent vulnerabilities. Once devices are compromised, attackers can bypass typical security defenses to transverse the network, gain control of connected devices, disrupt operations, and steal critical data.

Secure Remote Command & Control

Secure Autonomous Operations Enabled

Diagram labels — PRIMARY FACILITY

- PERA Level 3.5 Industrial DMZ
- Zero Trust BorderGuard devices secure VLANs, combining secure data transport and real-time delivery with ease of development.
- JUMP HOST — WEB PORTAL
- BorderGuard
- ICS DMZ VLAN
- PERA Level 2,3 Supervisory & Ops
- SECURITY VLAN — CONTROL VLAN — CONTROL VLAN
- CAMERA MGMT SERVER
- HISTORIAN — APP SERVER — DATA SERVER
- HISTORIAN — APP SERVER — DATA SERVER
- PERA Level 0,1 Field & Process
- PROCESS VLAN — PROCESS VLAN
- TANK — GAUGE — VALVE — GAUGE — PLC — HMI

Diagram labels — REMOTE FACILITY

- PERA Level 3.5 Industrial DMZ
- Policy-driven, Zero Trust secured VLAN, cryptographic transport between BorderGuard endpoints over unknown or insecure networks.
- JUMP HOST — WEB PORTAL
- BorderGuard
- ICS DMZ VLAN
- PERA Level 2,3 Supervisory & Ops
- SECURITY VLAN — CONTROL VLAN
- HISTORIAN — APP SERVER — DATA SERVER
- PERA Level 0,1 Field & Process
- PROCESS VLAN
- TANK — GAUGE — VALVE — GAUGE — PLC — HMI

Overview
Resilient, efficient, remote C&C

- Protect OT network operations without degrading performance and availability
- Counteract any potential vulnerabilities inherent in other cybersecurity approaches
- Improve networks security management without disruption
- Quickly and easily establish and manage secure site-to-site connections without IP constraints and complexity
- Minimize impact and overhead on infrastructure and users
- Securely provide access to remote workers, contractors, and partners using unknown and untrusted devices
- Cost effective scaling to meet growing network command and control requirements

Solution
LinkGuard secure enclaves

- Isolation and containment of devices, systems, and workgroups using micro segmentation based on cryptographic identities
- "Cloaking" of critical infrastructure OT systems and IT interoperability within LinkGuard enabled secure enclaves
- Encrypted communications between authorized systems within secure enclaves
- Enabled secure communications from authorized devices and users
- Reduced costs - seamless and flexible cybersecurity protection with low configuration sustainability requirements
- Significant deployment and operational costs savings with rapid payback compared to other alternatives

About Us

Blue Ridge Networks is a proven and trusted provider of cybersecurity breachprevention solutions. Our mission is to provide proactive protection of critical infrastructure that eliminates the adverse impacts associated with reactive responses to compromises.

Our unique CyberCloak capabilities secure critical assets and operations in zero-trust IT/OT network architectures. Regulated, Commercial, and Industrial organizations have trusted Blue Ridge Networks for over 20 years to prevent exploits and receive continuous returns on their investments while achieving uninterrupted operational efficiency.

BLUERIDGE®
NETWORKS

1-800-704-5234
sales@blueridgenetworks.com
BlueRidgeNetworks.com