LINKGUARD™

Case Study

Zero Trust Breach Prevention

Command & control network protection for multi-national food & beverage distillery

Summary

Schneider Electric (SE) utilized the LinkGuard™ zero trust breach prevention solution to protect critical command & control operations for one of its marquee global food & beverage distillery customers. LinkGuard secured interoperability of Operational Technology (OT) operations with minimal integration requirements and disruption delivering over $500,000 annual operational savings.

Overview

Schneider Electric (SE), one of the world's largest industrial automation companies, has partnered with Blue Ridge Networks (BRN) to deploy the LinkGuard solution to secure its customers' critical OT/IT infrastructure operations. This SE customer has main distillery sites as well as remote grain storage facilities in the UK. The grain storage sites are frequented by tankers for transfer of materials. When a tanker arrives on site, it is required to show its credentials for approval to proceed. Once approved and in position, release valves are opened to fill the tanker. The process must be tracked and documented for audit records.

Use Case Requirements

The company desired to operate the storage facilities as unmanned sites. In addition to personnel cost savings, remotely managed sites were a necessity during the pandemic with a need to limit physical interactions. The unmanned remote sites are operated using live CCTV feeds and automation combined with manual operations at the central control site. Secure network extension to the storage facility was required to protect operational processes remotely as well as secure live feeds from the CCTV cameras that record when tankers arrive and their documentation to proceed. Release valves are remotely activated and monitored to control the amount of material to be dispensed.

Schneider Electric

Resilient Operational Efficiency

- Enabled unmanned operation of remote grain filling sites
- Ability to securely operate autonomously around the clock (24x7x365), which increased production rates and efficiency for the multinational company

Minimal disruption and overhead

- Rapid deployment, including documentation, in only three (3) weeks
- Did not require any changes to network infrastructure
- No operational issues and no support calls logged for the year it has been deployed.
- No down time and no maintenance actions were required.

Resilient OT Breach Prevention

- Impregnable cybersecurity – LinkGuard has no reported breaches in over 20 years of deployment – avoidance of operational and reputational damage for Schneider Electric and its customer

Over 10x ROI

- Resulted in significant cost savings for the Schneider Electric customer – approximately $500,000 per annum per site with LinkGuard investment recouped within 3 months.

BLUERIDGE NETWORKS

LINKGUARD™

Case Study

Customer Need: Control connected devices with secure network interoperability

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.

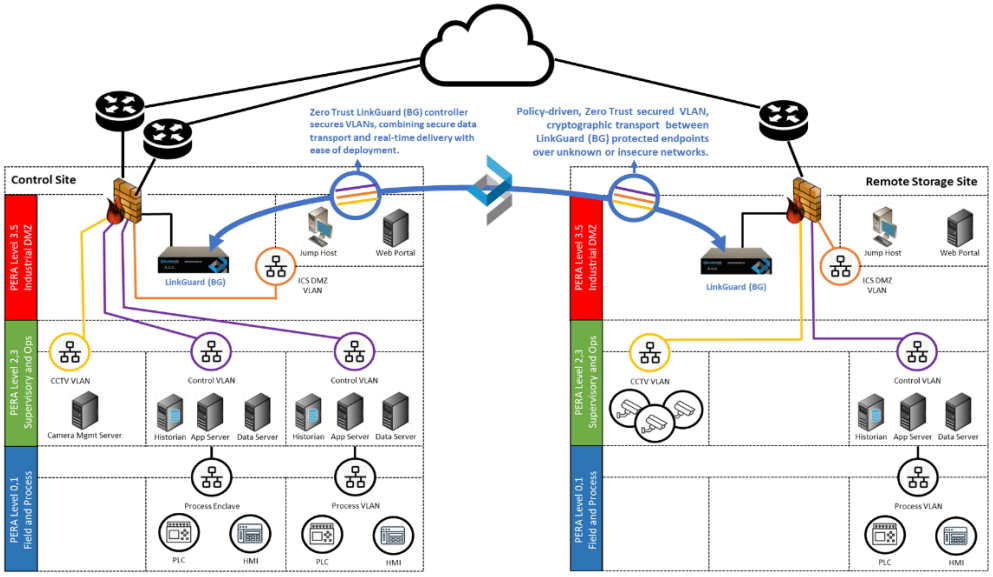
Organizational Objectives

- 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
- Costs savings over $500 thousand per site – payback in 3 months

Secure Remote Command & Control



Secure Autonomous Operations Enabled

About Blue Ridge Networks, Inc.

Blue Ridge Networks is a proven zero trust cybersecurity breach prevention solutions provider for the connected world. The Company's solutions eliminate external discovery and data exfiltration of OT/IT operations from vulnerabilities inherent in modern networks without the dependencies and overhead of threat detection. Blue Ridge solutions have protected critical operations for some of the largest U.S. government, financial, healthcare, and other critical infrastructure customers for more than twenty years with no reported breaches – ever.

Contact
1-800-722-1168
sales@blueridgenetworks.com

Headquarters
14120 Parke Long Court
Suite 103
Chantilly VA, 20151

BLUERIDGE NETWORKS