

LinkGuard™ SUCCESS STORY

Operational Technology Security for Secure Continuous Operations

Protecting Cyber Physical Systems for
a Major Urban Water–Wastewater Facility





Overview

Schneider Electric (SE), one of the world's largest industrial automation companies, has chosen Blue Ridge Networks (BRN) to implement the LinkGuard™ zero trust breach prevention solution. This initiative aims to enhance the security of Operational Technology (OT) and Cyber-Physical Systems (CPS) interoperability with Information Technology (IT) network operations for SE's customers. Specifically, LinkGuard has been deployed by a major U.S. city's urban water/wastewater authority to safeguard network command and control for its water treatment operations.

Customer Use Case

The water utility selected LinkGuard to establish secure interoperability of its SCADA networks and cyber physical 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. LinkGuard has a low and predictable latency even on the slowest and most geographically dispersed systems. The overlay deployment of LinkGuard software and systems is fully compatible with OT systems and IT operations. Its autonomous operation minimizes integration and sustainment complexity, delivering an order of magnitude or more in 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

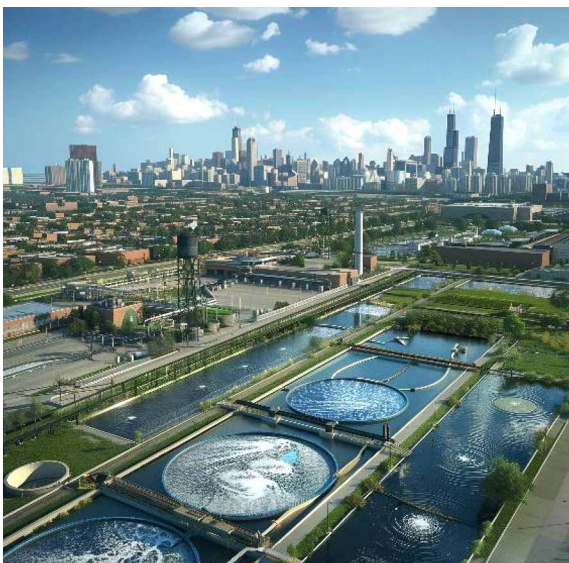
Operational Efficiency

- Ability to securely operate autonomously around the clock (24x7x365)

Increased production rates and efficiency for the multinational company

High ROI

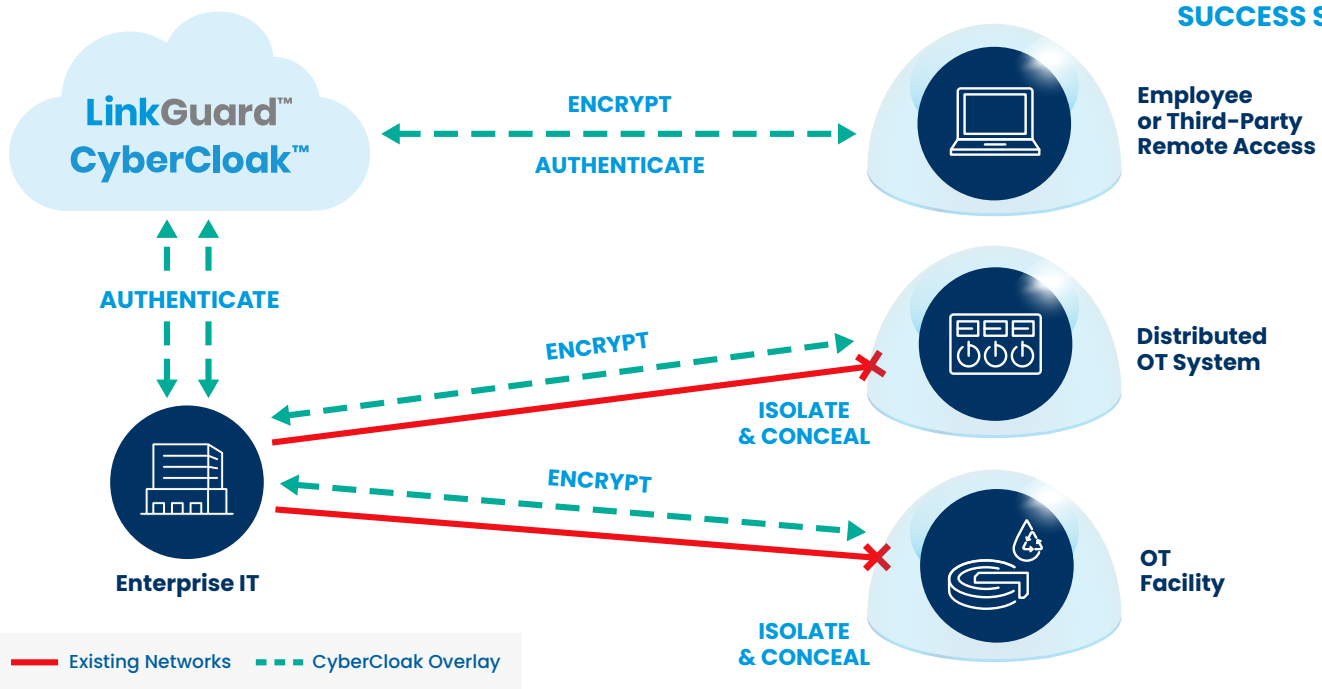
- Easy deployment and operation efficiency delivers an order of magnitude or more cost savings to customers for secure network operations



Customer Need

Secure Continuous Operations to Ensure 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, and seriously compromise public safety.



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 paycheck compared to other alternatives

About Us

Blue Ridge Networks is a proven and trusted provider of cybersecurity breach prevention 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.



1-800-704-5234

sales@blueridgenetworks.com

[BlueridgeNetworks.com](https://www.BlueridgeNetworks.com)

