Overview

Today, organizations are going through digital transformations to improve business processes by leveraging the internet to connected previously air-gapped systems. But open-protocol information technologies (IT) have also made it easier for adversaries to access and exploit operational technologies (OT) such as physical security and surveillance systems within decentralized offices, medical equipment, remote systems and other network connected devices and systems associated with the Internet of Things (IoT).

The convergence of OT/IT means that organizations are highly susceptible to lateral attacks from these connected systems. This leaves core business functions, critical operations, and sensitive data vulnerable to wide scale disruption.

The Blue Ridge Networks Solution

Blue Ridge Networks’ LinkGuard solution, a part of the BorderGuard cybersecurity ecosystem, protects organizations from vulnerabilities posed by operational technology (OT) and IoT devices and systems. With LinkGuard, organizations can isolate and contain IoT network segments within cryptographic boundaries (secure enclaves) which mitigates the risk of unauthorized access to the devices and prevents data exfiltration.

Based on the Zero Trust methodology, LinkGuard provides the highest level of security autonomously – seamlessly protecting your most critical infrastructure and allowing your IT teams to focus on other tasks. LinkGuard enables secure connectivity across the enterprise – wherever it’s needed, without costly or time-consuming IT overhead.

Organizational Challenges

- Improve network and system security without significant cost and disruption
- Manage internal and third-party threats when opening the network to remote workers, vendors, and support teams using untrustable devices
- Quickly and simply establish and manage secure site-to-site and remote connections
- Simultaneously protect critical assets against external and internal threats
- Cost-effectively scale to meet growing networking requirements

Technical Challenges

- Establish quick and secure connections, without IT intervention and overhead
- Protect IT, IoT, and OT networks without degrading performance and availability
- Counteract the vulnerabilities inherent in software or virtual security solutions
- Minimize impact on existing infrastructure and user experience
- Prevent propagation of malware already on the network
**How it Works**

LinkGuard is an operationally transparent and versatile overlay solution that enables organizations to seamlessly connect, isolate, contain, cloak, and manage any ethernet enabled connected device over any transport, anywhere in the world – with minimal network configuration changes.

The LinkGuard platform is comprised of the BorderGuard hardware appliance that serves as the root of trust for the entire platform, and RemoteLink and EdgeGuard products that extend the proven security architecture to dispersed offices, remote sites and users, devices and more.

LinkGuard’s security architecture has protected critical infrastructure for government and commercial customers for more than 20 years. LinkGuard helps mitigate vulnerabilities and harden systems in three ways:

**Prove** - Mutual mandatory authentication based on cryptographic identities ensures that a connection originates from an authorized and secure device according to the established policies. This eliminates IP spoofing, session hijacking and a variety of other attacks.

**Protect** - Full packet encryption of data in motion is protected and not accessible to anyone other than the authorized parties as established by the policy. This enables secure communications and prevents data theft – even over untrustable means of communication.

**Prevent** - Isolation and containment of systems and devices within the secure enclaves are completely segmented, preventing any attacker or malicious payload from penetrating the cryptographic boundary. Systems are also cloaked and invisible to attackers – drastically reducing the attack surface using obfuscation. Even previously compromised systems are protected because the information with in the enclave is contained and only accessible by another authorized party.

LinkGuard single handedly stops a wide range of attacks on OT and IoT devices by seamless segmenting the network and upholding automatic, robust security policies. With the LinkGuard solutions, workgroups can also remotely access the connected devices for diagnostics, maintenance, and more.

**Key Benefits**

- **Increased Efficiency** – Minimal IT configuration and provisioning plus independence from traditional IT tools increases efficiency of both OT staff and users and drastically decreases operational expenses.
- **Tried and Tested** – Originally developed to protect high value critical operations and assets for the US Government.
- **Reduced Network Complexity** – Protects critical operations autonomously without dependence on complex traditional IT solutions like firewalls, VPNs, Access Control Lists, and VLANs.
- **Seamless Integration with Existing Infrastructure** – Overlays existing IT infrastructure with little to no modification to the underlying network infrastructure.
- **Simple and Cost-Effective** – Eliminates the need for pre-configuration and traditional IT tools that require staff to manage, drastically decreasing CapEx and OpEx.
- **Built-in Two-Factor Authentication** – Mitigates the vulnerability of exposure by not requiring a user to depend on a password, or shared secret, for authentication.
- **Managed Services Option** – Further decreases the complexity of secure networking; deploy LinkGuard as a managed service to allow IT teams to focus on more critical tasks.
**Attack Scenario**

**Challenge:** Secure connected devices and communications  
Connected operational technology (OT) or Internet of Things (IoT) devices provide a wealth of opportunity for productivity and efficiency, but they also increase the attack surface by introducing weak points within an organizations network infrastructure. From these devices, attackers can traverse the network and bypass IT security defenses to steal critical data or gain control of connected devices.

**Solution:** Isolate and contain critical assets  
Deploying Blue Ridge Networks’ LinkGuard solution enables:
- Isolation and containment of devices, systems and workgroups using micro segmentation based on cryptographic identities
- Cloaking of infrastructure within BorderGuard enabled secure enclaves
- Encrypted communications between authorized systems within secure enclaves

**Result:** Protected and cloaked devices with ubiquitous access  
With LinkGuard you can:
- Prevent and contain unauthorized access to connected devices, systems, and data
- Mitigate attacks on IoT devices
- Enable secure communications from authorized devices and users
- Reduce costs with seamless and flexible security and low configuration changes

---

**Want to learn more about how LinkGuard can protect your connected devices?**  
Contact us to talk to a cybersecurity expert today.

---

**About Blue Ridge Networks**  
Based in Northern Virginia, Blue Ridge Networks is a visionary cybersecurity pioneer that provides autonomous cybersecurity for the connected world. Blue Ridge Networks’ Autonomous Cybersecurity Suite protects organizations from vulnerabilities posed by connected devices, endpoints, networks, and people. Blue Ridge solutions have protected critical operations for some of the largest US government, financial, healthcare, and other critical infrastructure customers for more than twenty years with no reported breaches.

---

**Contact Us:**  
1-800-722-1168  
sales@blueridgenetworks.com

**Headquarters:**  
14120 Parke Long Court Suite 103  
Chantilly VA, 20151

©2018 Blue Ridge Networks. All Rights Reserved.