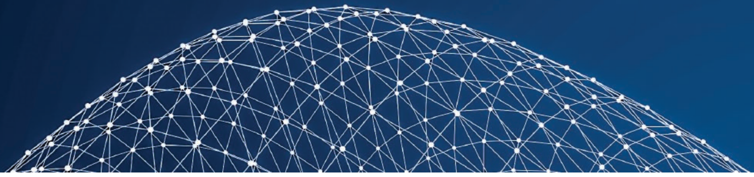
LINKGUARD™ SYSTEM

OVERVIEW AND COMPONENT DESCRIPTION

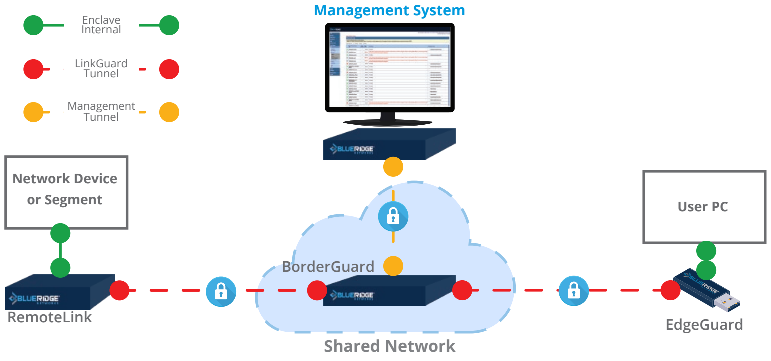


Blue Ridge Networks' LinkGuard system protects critical operations where "good enough" cybersecurity is not good enough. The solution essentially "cloaks" critical Information Technology (IT) network operations (sensitive data transmissions, confidential client communications, network management systems, emergency operations) including networked Operational Technology (OT) assets (industrial control systems, facilities infrastructure, command and control systems) from increasingly destructive and costly cyber-attacks. LinkGuard overlays onto existing network infrastructure with a Zero Trust solution to create and maintain secure network segment "enclaves" immune from external discovery or penetration and from data exfiltration. The patented technology foundation of LinkGuard has been heavily tested, broadly certified, and proven effective in the field protecting government and enterprise critical operations for many years with no reported security breaches.

LinkGuard At A Glance

- **Segments critical operations from external discovery and data exfiltration.**
- **Compatible with both IT and OT infrastructure.**
- **Easy to deploy and manage remotely.**
- **Resilient, scalable and affordable.**

LinkGuard creates secure pre-authenticated Layer 2 network communication channels independent of, yet compatible with, Layer 3 data transfers which protect end-to-end and point-to-point network sessions. The solution enables rapid, self-contained segmentation of network traffic encrypted from the first packet without requiring access to the underlying traffic data. LinkGuard defined enclaves are agnostic to the communications media and isolate network address spaces from the underlying infrastructure and from each other. This network segmentation overlay provides a new layer of cybersecurity defense for non-disruptive secure interoperability compatible with deployed IT systems (SDN, VPN, VDI, applications, IT tools) and OT systems (ICS, SCADA, IP Cameras). It is easy to install, administer and maintain, and has minimal overhead. LinkGuard firmware is also embeddable into future IT and OT devices for easy integration into the LinkGuard protected architecture. In addition to achieving a robust, compliant new standard of resilient and reliable cybersecurity defense, LinkGuard customers typically realize more efficient cybersecurity and network operations with less disruption, less overhead and lower ongoing costs.



The LinkGuard solution consists of a Management System, a BorderGuard cryptographic controller, RemoteLink firmware enabled devices to create multi-endpoint enclaves, and EdgeGuard to provide secure on-demand access to an enclave from an individual endpoint. The Management System can support multiple BorderGuards and each BorderGuard can support up to hundreds of RemoteLink or EdgeGuard instances allowing easy scalability for a wide range of use cases. Enclave access policies are pre-configured and remotely managed eliminating the need for skilled technicians in the field for deployment and easy on-going management and sustainment of enclaves. Ongoing management of LinkGuard is efficient without causing degradation, latency, IP address changes, or cumbersome MACDs (moves, adds, changes, and deletes) to the underlying network segments. The system can be deployed as a fully managed service, co-managed service, or system license with 24x7, 365 Blue Ridge support.

The **Management System** creates, manages, and monitors LinkGuard enclaves as defined by the system administrator. It consists of a Management Console (MC) and a Remote Manager (RM). The MC device implements and maintains administrative policies that define a LinkGuard enclave. The RM establishes the independent management plane connection to deployed BorderGuards for secure policy enforcement and log collection consistent with the MC policies. Separation of the LinkGuard management plane from its data communications plane eliminates vulnerable interdependencies.   This approach provides an effective cybersecurity defense that is highly compliant with increasingly stringent privacy and information assurance, regulations.

BorderGuard® provides the root of trust for controlling secure connection of the LinkGuard data plane and management plane communications. It serves as the backbone of the LinkGuard solution and can handle multiple LinkGuard client connections. BorderGuard systems reliably and resiliently provide total path redundancy for critical operations requiring high assurance continuity.

RemoteLink™ enables deployed plug-and-play devices that creates secure network enclaves in the field. Using crypto-ignition tokens or keys provisioned by the Management System, a RemoteLink securely connects local network segments or devices over any communication medium to the rest of the enterprise via connection to one or more of its designated BorderGuards. RemoteLink devices are inherently unresponsive to cyber-attacks, reconnaissance, or penetration attempts of the LinkGuard enclave. Data within the enclave cannot be exfiltrated.

EdgeGuard® is a virtual machine installed on a PC or laptop or embedded on a bootable device (USB, CAC-PIV reader) to create a LinkGuard enclave to an individual user device (desktop, laptop). EdgeGuard enables secure on-demand remote access to its designated BorderGuard that isolates the secure EdgeGuard session from the host endpoint. This ensures users cannot upload potentially malicious code into the network or download any sensitive data to the endpoint. EdgeGuard provides secure access without the risk of credential theft or malware mediated attacks on the network infrastructure.

About Blue Ridge Networks, Inc.

Blue Ridge Networks is a proven cybersecurity isolation and containment technology innovator delivering network segmentation, remote access, and endpoint cybersecurity solutions that eliminate vulnerabilities to critical network infrastructure and prevent exfiltration of mission critical data. The company has successfully provided resilient, scalable, and affordable cybersecurity systems, software, and managed services for over 20 years, protecting critical operations of its government and enterprise customers with no reported breaches of its technologies - ever.