WHITE PAPER

Zero Breach for Zero Trust

Breach Prevention Solutions to Protect Distributed Critical Operations for the Department of Defense

LinkGuard™ Zero Trust Network Access Overview

Synopsis

Blue Ridge Networks, Inc. has been a pioneer for developing and deploying high assurance cyber-security network capabilities for over 20 years to protect distributed critical network operations for IC, Army, Navy including NELO, USCG, Financial, and Infrastructure/Energy Operational Technology (OT) markets. With the launch of its initial BorderGuard™ products in 1995, Blue Ridge Networks, Inc. introduced the first commercial cryptographic component accredited by the NSA for a variety of use cases within the US Government. Many of the current products' unique features evolved based upon feedback from our most demanding customers. Its solutions are designed to deliver high assurance breach prevention in an un-trustable network ecosystem – – Zero Breach for Zero Trust

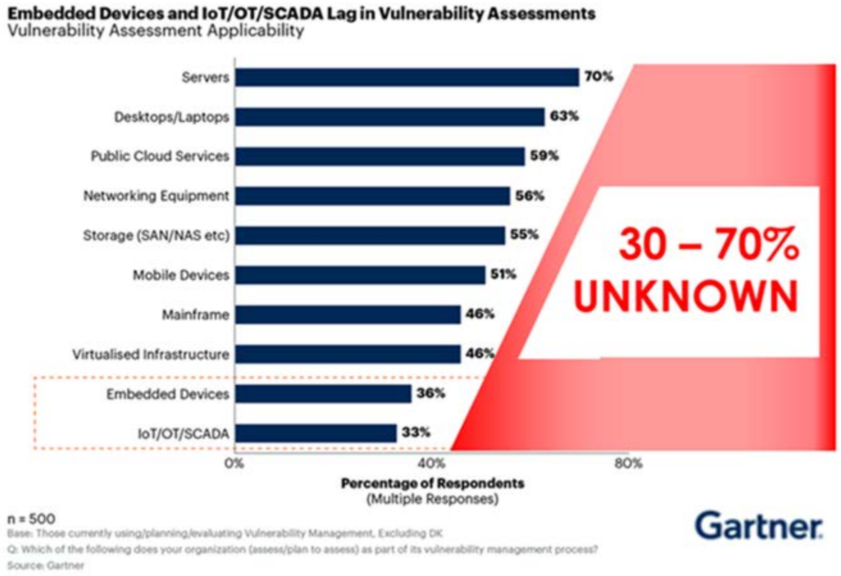
LinkGuard is the cybersecurity solution designed to isolate and contain network sessions within a zero trust architecture. It is the evolution built from the foundation of the company's cyber components. Blue Ridge Networks, Inc. has recently been recognized in several key areas within the 2023 Gartner Hype Cycle report for Operational Technology (OT) security expertise.

We are featured as a top OT security vendor within specific industries and for overall OT security management when applied, for example, to the protection of industrial controls systems (ICS). Unlike firewalls, VPNs or SDN products, LinkGuard is well suited to address threats to Industrial Internet of Things (IIoT) and Critical Infrastructure environments. It delivers the ability to autonomously segment, authenticate, and protect network sessions to prevent breaches with operational efficiency, deployment ease, and minimal sustainment overhead or complexity. Our LinkGuard solution enables you to secure the management plane.

Visibility Gap - Protection Lag

- **Threat Landscape**
  Reports identifying prime threats, trending attack techniques and approaches to threat mitigation, show growing vulnerabilities of IIOT and Critical Infrastructure deployments. In fact, these systems represent almost uncontrolled growth of an attack surface that is both complex and unwieldy to maintain.

- **Common Response**
  Most Cyber Security companies have focused on Detect and Respond methodologies that promise expanded coverage and reduced lag between breach contact and breach response. The statistics shown below indicate that this approach is failing.



Embedded Devices and IoT/OT/SCADA Lag in Vulnerability Assessments
Vulnerability Assessment Applicability

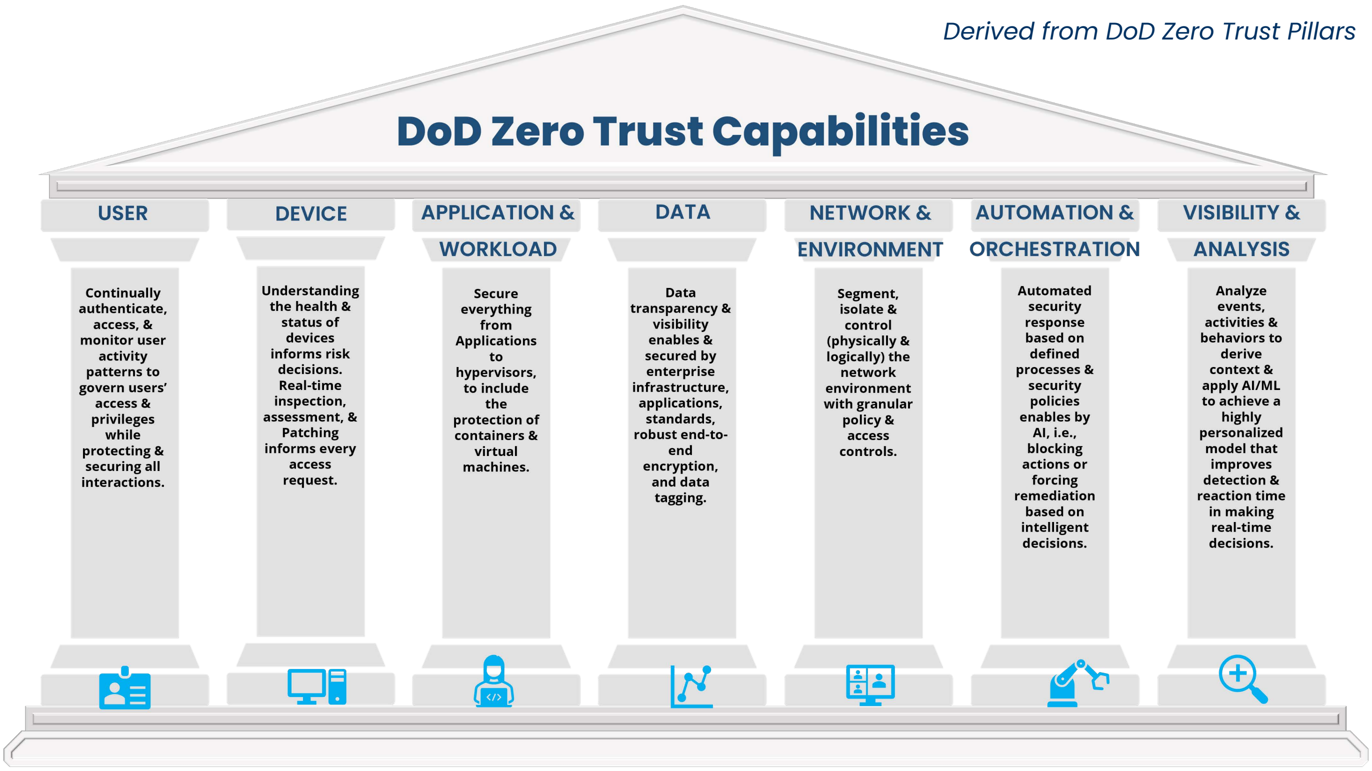
n = 500
Base: Those currently using/planning/evaluating Vulnerability Management, Excluding DK
Q: Which of the following does your organization (assess/plan to assess) as part of its vulnerability management process?
Source: Gartner

> *“The goal is to prevent unauthorized access to data and services and make access control enforcement as granular as possible.”*
> - CISA | Zero Trust Maturity Model Version 2.0

LinkGuard is a complementary breach prevention, zero-trust cybersecurity solution that delivers defense-in-depth without operational complexity to Users, Devices, Networks/Environments, Applications & Workload, and Data.

Zero Trust 7 Pillars

Derived from DoD Zero Trust Pillars



DoD Zero Trust Capabilities

USER
Continually authenticate, access, & monitor user activity patterns to govern users’ access & privileges while protecting & securing all interactions.

DEVICE
Understanding the health & status of devices informs risk decisions. Real-time inspection, assessment, & Patching informs every access request.

APPLICATION & WORKLOAD
Secure everything from Applications to hypervisors, to include the protection of containers & virtual machines.

DATA
Data transparency & visibility enables & secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

NETWORK & ENVIRONMENT
Segment, isolate & control (physically & logically) the network environment with granular policy & access controls.

AUTOMATION & ORCHESTRATION
Automated security response based on defined processes & security policies enables by AI, i.e., blocking actions or forcing remediation based on intelligent decisions.

VISIBILITY & ANALYSIS
Analyze events, activities & behaviors to derive context & apply AI/ML to achieve a highly personalized model that improves detection & reaction time in making real-time decisions.

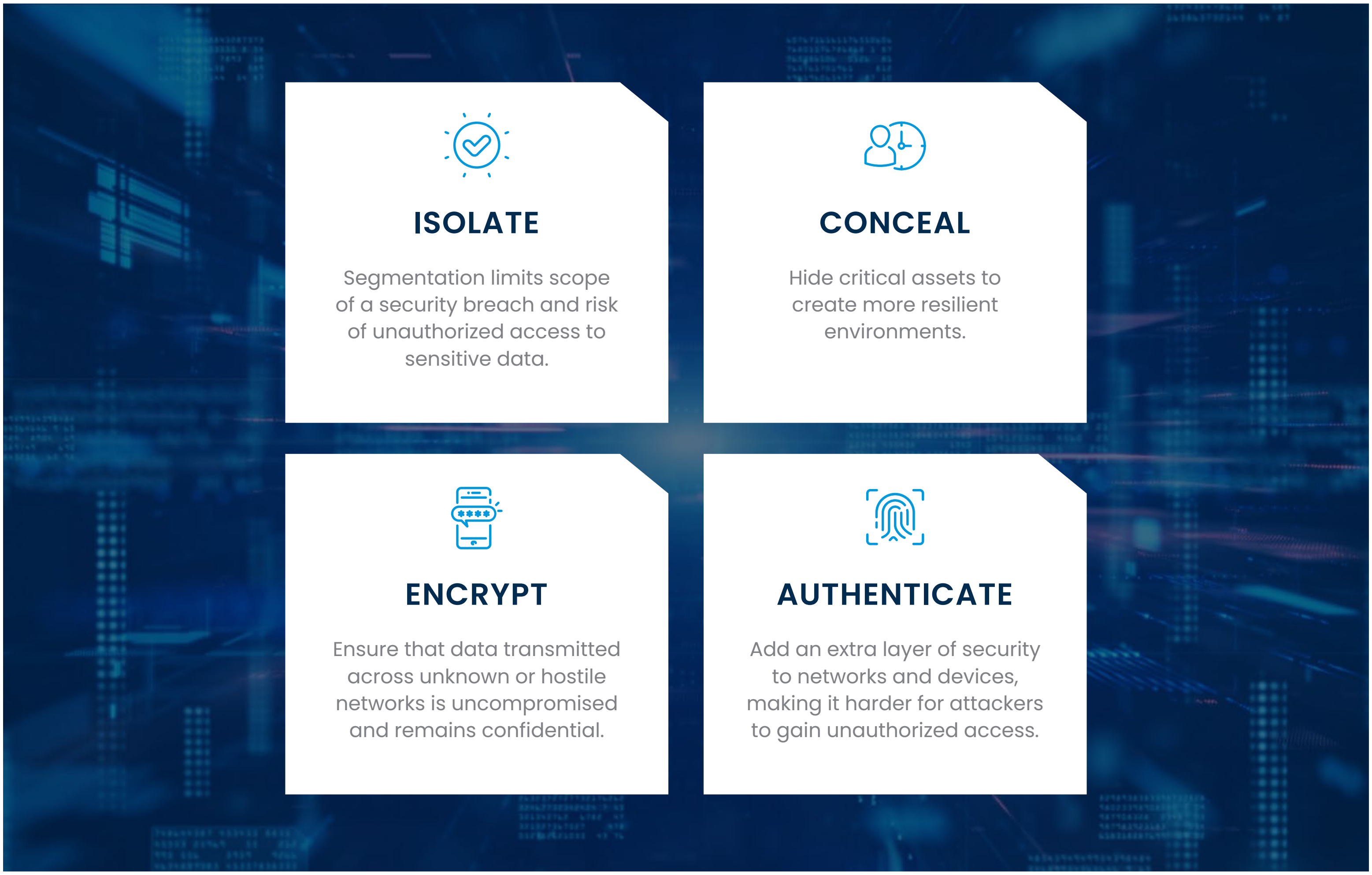
LinkGuard Pedigree

Blue Ridge Networks software, hardware, and operational architecture of its legacy BorderGuard-RemoteLink-Wyse thin-client systems are still in use today, providing secure high-over-high, cross domain interoperability with no reported breach of critical operations in untrustable, uncontrolled, distributed IT/OT digital ecosystems in Government, Financial and Infrastructure/Energy OT markets.

After 9/11, BorderGuard solutions were accredited for tactical deployments. Because the solutions did not use classified cryptography, and because they provided a secure, remote means of deactivating any deployed components, they were suitable for use in hostile territory where devices might be captured.

The Blue Ridge Networks LinkGuard product suite extends these proven solutions to support additional use cases at wider scale for networks and endpoints. LinkGuard solutions are designed to be utilized with minimal integration complexity and maximum compatibility with IT/OT systems and tools, providing the least disruptive deployment and lowest cost of operation for high assurance cybersecurity protection of critical operations. LinkGuard includes a proprietary cryptosystem based on FIPS 140-2 compliant cryptographic transforms, and LinkGuard solutions have never failed an accreditation nor suffered a red-team penetration. Today LinkGuard systems are in service within the US Army, Navy, Coast Guard, the IC, and Financial and Infrastructure/Energy Operational Technology (OT) markets.

LinkGuard addresses the requirements of the Zero Trust Pillars in the following ways.



ISOLATE

Segmentation limits scope of a security breach and risk of unauthorized access to sensitive data.

CONCEAL

Hide critical assets to create more resilient environments.

ENCRYPT

Ensure that data transmitted across unknown or hostile networks is uncompromised and remains confidential.

AUTHENTICATE

Add an extra layer of security to networks and devices, making it harder for attackers to gain unauthorized access.

LinkGuard Boasts the Following System Features:

- **Resilient Cybersecurity** – field-proven value to government customers; no reported breaches in over 20 years of service
- **Zero Trust Protection** – conceals protected network operations and processes to prevent hackers from gaining access or control; built-in PKI authentication eliminates risk of third-party intrusion
- **Autonomous** - "out-of-band" operations; secure remote management; no management plane operational dependency; no third-party vulnerability
- **Ease of Integration** – integrates seamlessly with existing network infrastructure; exports system syslog data; compatible with legacy and future IT/OT infrastructure
- **Lower Cost** – prevents remediation costs of exploits from potential adversaries; minimal overhead; reduces attack surface

> "A key tenet of a zero trust architecture is that no network is implicitly considered trusted—a principle that may be at odds with some agencies' current approach to securing networks and associated systems." - Executive Order 14028 | Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

LINKGUARD™

Robust Technology Foundation

Blue Ridge cybersecurity solutions incorporate technologies that enable the efficacy of its current products, as well as provide a foundation to effectively evolve capabilities that can address future cybersecurity challenges.

- **Enabling Technology Examples (Current and Near-Term)**

  Tunnel-Lock®: Session isolation methodology; PKI enabled

  DPF virtualization: IoT secure cloud access technology applied to Data Privacy Facility for the LinkGuard crypto system

  Auto-Provisioning: Network session authentication autonomous provisioning technology

  Cryptographic Methodology: Unique model, methods, and algorithms based on FIPS 140-2 compliant cryptographic transforms approved for commercial use

- **Enabling Patents**

Trusted Enclaves (#7,712,143; original BRN patent; perpetual licensee): A trusted enclave for a software computer system of a computer node that provides high assurance protection of a section of the software.

Trustable Communities (#7,809,955; original BRN patent; perpetual licensee): a trustable community for a system that includes multiple software components that have interdependence.

NetTop (#6,922,774; co-invention; NSA licensee): remote access security architecture.

ICS-AutoGuard (#11,096,610): a system to autonomously and securely segment operational technology networks without disruption.

Quantum Resistant Enclaves (#10,630,467): methods and apparatus for network communication resistance to quantum computing brute force attacks.

Unlike firewalls, VPNs or SDN products, LinkGuard is well suited to address the following challenges.

PERFORMING OUT-OF-BAND NETWORK MANAGEMENT

Per NSA guidance[1], a priority step towards zero-trust is to move IT systems management out-of-band. This applies to all seven pillars. Because air gapped management networks are mostly impractical, isolation within encrypted connections allows continued sharing of existing data-plane networks.

This protects against administrator credential theft and pass-the-hash type exploits if attackers have data-plane access. Logically, this requires a completely separate Identity and Access Management system with strong credentials and Two Factor Authentication (2FA).

LinkGuard is an ideal solution for management plane security and separation. Its built-in trust and credentialling system has no external dependencies. Moreover, each LinkGuard system is cryptographically isolated from all others with no possibility of a class break. The network overlay enclave is operationally transparent to all management plane protocols it may be protecting.

LinkGuard, itself, has an out-of-band management plane. The management system provides granular administrator privileges. For example, it is straightforward to prevent a singular LinkGuard administrator from creating new LinkGuard access without the concurrence of another. This protects all systems from insider threats.

SECURING OT INFRASTRUCTURE

The US Department of Defense has the world's largest operational technology infrastructure. Nearly all of this was previously deployed in application and site-specific standalone networks. Until recently, the component elements had only the most rudimentary security features. LinkGuard has been shown to provide a practical and effective solution to secure these systems with little or no impact on their operations.

In 2017, the Blue Ridge products were deployed and tested in the Department of Defense Orlando Florida cyber-range. The DOD red team was unable to penetrate the defenses. Furthermore, existing OT systems continued to operate without change.

LinkGuard offers a practical means of segmenting OT and IT networks as required in the zero-trust initiative. LinkGuard design supports incremental deployments with minimal disruption. It also supports layered segmentation without the operational complexity inherent in firewalls and VPNs.

Most OT systems depend on regular support from vendor support staff. LinkGuard supports secure and granular remote access of these extranet connections. Its independent built-in credentialling system and 2FA avoid the administrative nightmare of issuing enterprise credentials to vendor personnel, thus making the overall system more secure.

RAPID DEPLOYMENT OF TRUSTED COMMUNICATIONS

Ahead of its time in the zero-trust ethos, LinkGuard is operationally self-sufficient with a built-in public-key trust system. Policies relating to system security are mandatory and not subject to administrative errors. Nor are the protected systems and users trusted in any way.

LinkGuard is well-suited to rapid deployment for secure communications. Without prior configuration, it has successfully worked over any combination of public and private communications infrastructure. In addition to expected voice, video and data applications, it is a practical solution for securing remote sensor systems of all types. Simple to configure redundancy delivers up to four nines of availability and no single point of failure including the LinkGuard management plane. Central connection points can be geographically dispersed and pooled for added up-time assurance.

NEAR-TERM LINKGUARD PRODUCT EVOLUTION

Universal Secure Access

Providing zero trust compliant remote access from enterprise managed endpoint devices is relatively straightforward. But, what about extranet connections from business partners, or employee access from smart phones or home computers? Currently, this continues to be a significant cyber business risk.

The Blue Ridge roadmap for its RemoteLink and Micro RemoteLink products will offer the following cybersecurity protections:

- Secure access from any and all endpoint devices including smartphones and un-managed PCs.
- No need for endpoint software installation.
- True 2FA, a non-replicable possession factor and a user entered PIN.
- Highly secure connections over any type of public or private networks.
- Compatibility with all remote access applications based on the use of browsers and RDP clients.
- Immunity to credential theft, social engineering like phishing attacks, and MITM exploits.
- Instantly revocable access for lost or stolen RL devices.
- Compatibility with all enterprise identity and access management systems.
- Wired and wireless WAN connectivity.

This is an ideal means of securing the enterprise management plane.

Trusted Cloud Access

One or more BorderGuard appliances in the LinkGuard system act as the hardware root of trust for the extended LinkGuard network enclave. Currently, cloud access requires egress from the LinkGuard enclave to an SDN node which in turn connects with the cloud. Customers have asked for the simplicity and added security of extending LinkGuard directly to the cloud.

Blue Ridge is developing a virtualized BorderGuard that will operate in a cloud virtual machine. Using the cloud provider's HSM services, it still provides a hardware root of trust for the extended LinkGuard enclave.

Blue Ridge is a licensee of the NSA NetTop patent. This has enabled several generations of LinkGuard and EdgeGuard software clients that include virtual RemoteLink components. Leveraging hardware level protection of these virtual machines preserves the operational independence and security robustness expected from LinkGuard.

Quantum Resistant Secure Connections

LinkGuard includes a proprietary cryptosystem based on FIPS 140-2 compliant cryptographic transforms. Blue Ridge recently received a patent for an extension to this cryptosystem which will prevent brute force quantum computer attacks that will penetrate all currently available commercial VPN products. See note under Securing OT infrastructure about DOD Red team testing earlier in this document.

Auto-Provisioning for OT Networks

Operational Technology networks are often not well documented. Deploying firewalls and VPNs for these networks requires details about the devices, their layer 2 and layer 3 addresses, their protocols, and the policies necessary to protect them but not interrupt continued operations.

Blue Ridge has received a patent for an extension to its LinkGuard system that supports automated provisioning of LinkGuard protection that avoids possibly costly interruptions for the OT network. It may be simultaneously deployed to many sites for which it will provide isolation and containment security. Future further segmentation or extensions will also be automated.

LinkGuard Sample Use Cases:

Secure Remote Site LAN Extension

- Site to Site L2 over L3 LAN Extension, no need to change OP addressing scheme already in place. Fully encrypted communications for all Ethernet connected devices. Extremely useful in SoHO communication needs, as well as over WiFi/Cellular or Wired Internet WAN facilities

Secure Command & Control

- Great use case for Autonomous Vehicles over 4G/5G Cellular WAN or ultra-secure connections between Critical Infrastructure Facilities. Especially useful in securing OT environments which generally use legacy communications methods such as SCADA for verticals in Oil & Gas, Water Treatment, Electrical and other Industrial controls.

Vendor/Function Separation

- Multi-Vendor E-Commence or Infrastructure Partitions allowing outside contractors/vendors access to necessary systems to better fulfill engagements/contracts faster. This applies to verticals such as Consumer Package Goods (CPG) or Financial Companies for example where there is a need to provide access to certain systems but not others.

Secure Distributed Operations

- Communications across varying WAN paths such as single and double hop satellite links. Can be useful for all ship to shore communications as the LinkGuard solution has a very small footprint which is an advantage due to limited space available. Self-contained system for Rapid deployment in temporary use cases.

LinkGuard Questions and Answers

Why Does LinkGuard Integrate Independent Hardware Hosts for Its "Overlay" Architecture?

The marketplace has and will continue to discover exploitable vulnerabilities at every level of the compute stack including compromises arising within and from system hardware. Ultimately all software, including software defined networks (SDN), is dependent and reliant on the underlying trust architecture of the hardware on which it is running. Virtual approaches (virtual TPM, virtual "switches", blockchain derivatives, etc.) that attempt to create and manage hardware roots-of-trust are only as useful as their compatibility with the underlying hardware ecosystems on which they are dependent.

All networks, particularly OT networks, are composed of multiple generations of systems with a myriad of ever evolving operational protocols that exacerbate attempts to deploy trustable virtual access and authentication controls for high assurance resilience. LinkGuard does not trust the systems and networks which it protects, nor does it trust the networks over which it communicates. It has no external dependencies for its security-related operations thereby eliminating the dependency and sustainment complexity by integrating its firmware and software on independent hardware hosts to deliver a reliable, independent cybersecurity trust architecture. By removing all implicit trust, LinkGuard achieves zero trust.

How Does LinkGuard Expand Protection Based on Firewalls or VPNs?

No External Dependencies
The product includes all the components required to install and operate at full security. For example, LinkGuard has its own public-key trust system with no need of a certificate authority, unlike TLS/SSL based systems which require over the Internet agreement on which Public Certs to use. It provides strong mutual authentication of all connections between LinkGuard gateways. It also includes a very robust two-factor authentication system for remote access. The design and implementation eliminates the possibility of stolen credentials, the most prevalent step in sophisticated cyber-attacks. This also simplifies deployment and significantly reduces the cost of operation.

Mandatory Policies
Unlike any firewall or VPN product, LinkGuard requires very few non-default settings for operation. No settable parameters can reduce or turn off LinkGuard security protection. When LinkGuard is operating, it is providing its full security. If the mandatory settings are not correctly input or overlooked, LinkGuard will not function because the enclave can't be activated. This feature guards against incorrect configurations. This is significant for LinkGuard customers' security. Per AFRL 2, most network security problems are due to human error. But, LinkGuard does not permit human errors that cause the system to operate with reduced protection. Also, its L2/L3 overlay design that decouples interior and exterior address spaces, reduces overall configuration complexity by an order of magnitude.

Protection Not Based on Detection
LinkGuard protects by isolating (segmenting) networks from external access. The isolated network and the LinkGuard gateways are cloaked and undiscoverable by potential attackers. The LinkGuard enclave also contains the protected systems and networks. No external connections can be initiated, thereby neutralizing potential command and control channels from compromised systems.

LINKGUARD™

Conclusion

Attainment of the goals described in the Seven Pillars documents will require significant and ongoing policy changes to network infrastructure including servers and end-user devices. This introduces risk of errors and oversight. LinkGuard can add a completely independent layer of protection to the IT management plane. This will ensure that administrator credentials cannot be stolen by attackers. This is additional value to use-case specific instances of LinkGuard like OT/IT critical infrastructure protection.

LinkGuard's effectiveness is due to its self-contained credentialing and mandatory policy design. It exemplifies "zero trust." It empowers and enables the securing of the management plane.

LinkGuard is a complementary zero breach, zero-trust cybersecurity system that is simple to deploy, but delivers defense-in-depth without adding operational complexity to Users, Devices, Networks/Environments, Data and Orchestration.

Over many thousands of USG deployments, there have been no reported breaches or system failures.

It has never failed an accreditation nor suffered a red-team penetration.

Notes & Resources

1. https://media.defenselgov/2021/Feb/25/200279/-1/-1/0/CSI EMBRACING ZT SECURITY MODEL UOO115131-21.PDF
2. “A Science of Network Configuration” - article in The Journal of Cyber Security, May 2017
3. DoD Zero Trust Strategy - November 22, 2022
4. https://www.cisa.gov/zero-trust-maturity-model
5. https://disa.mil/NewsandEvents/2021/ZeroTrust
6. https://doi.org/10.6028/NIST.SP.800-207A

LinkGuard Product Resources

View the Product Video

Read a Product Implementation Case Study

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

f 𝕏 in