BLUERIDGE® NETWORKS

WHITE PAPER

GAIN BACK THE TRUST IN YOUR NETWORK.

LINKGUARD SEAMLESSLY CONCEALS YOUR NETWORK, REDUCES YOUR ATTACK SURFACE, AND PREVENTS HACKERS FROM GAINING ACCESS TO YOUR CRITICAL ASSETS WHILE EXTENDING TRUSTED COMMUNICATIONS WITH A GRANULAR LEVEL OF CONTROL.

INTRODUCING BLUE RIDGE NETWORKS' TECHNOLOGY

Blue Ridge Networks' LinkGuard platform represents a best-in-class capability to protect the critical assets of commercial and government customers from increasingly destructive and costly cyber-attacks. Able to support a wide range of architectures and technologies, LinkGuard overlays a zero-trust stealth solution at the network perimeter and within existing infrastructure to verify identity, authorize access, and obfuscate the protected systems from unintended access. The solution has been heavily tested, protecting U.S. national security assets for over 20 years with no confirmed security breaches. LinkGuard is highly effective, easy to install, low maintenance and more affordable than any comparable existing combination of cybersecurity solutions on the market.

CAPABILITIES, BENEFITS, FEATURES

The LinkGuard platform takes a proven cybersecurity technology, developed and battle-tested in the Department of Defense and the U.S. Intelligence Community, and applies it to critical assets that need robust security.

Blue Ridge Networks understands that disruptive cyber-attacks directly drive financial losses, and the degradation of safety standards have potentially catastrophic implications for an organization's brand reputation. We have created a solution that is especially relevant to sensitive safety and compliance standards and provides pragmatic protection against those risks.

Most cybersecurity solutions are not focused on preventing attacks - they are designed to respond to cyber threats. Our solution prevents threats at the edge of your protected network, where the initial connection to the Internet occurs, utilizing a standalone hardware root of trust platform that is flexible enough to work with any existing network or infrastructure. LinkGuard provides an invisible protective border that is hidden and inaccessible to outside perpetrators and unauthorized observers, which enables the flow of day-to-day business without disruption or security risks.

As a defense-in-depth solution, LinkGuard enforces mutual autonomous authentication, constructs trusted connections, and simply ignores all other unknown or unapproved access. Once a verified connection is established, LinkGuard creates isolated, self-contained segments for networks, systems, applications, and dataflows in encrypted enclaves as primary or secondary security measures. These protected segments can be used to protect secure communications from remote sites or individual users and provide extensive vulnerability masking, limiting the available attack surface from attempted compromise. This solution is also critical for high-impact networks with distributed systems and limited issue remediation capabilities, such as industrial control systems and Internet of Things (IoT).

LinkGuard can be deployed in stages, requiring no system upgrades or additional operation requirements, regardless of protocol or transport mechanism. The current system operates as a combined hardware and software solution that provides unbreachable encryption to address both legacy and next generation networks.

LinkGuard protected enclaves and network segments are created transparently, rendering them invisible to each other and the rest of the network, forcing all communications through carefully-defined ingress and egress paths that can be tightly controlled and easily managed. Operating at the Open Systems Interconnection (OSI) Network Model – Layer 2, LinkGuard stands apart from its competitors by providing an autonomous security and networking solution that is quickly adaptable and easily integrable with existing network infrastructure or Software Defined Wide Area Network (SD-WAN) architecture to provide additional fault tolerance and environmental resilience.

LinkGuard offers the following benefits:

- Simplicity – No tunnels, no overlays, no more hardware centric networking, all with dynamic provisioning
- Agility – Faster fire-and-forget deployment, application resiliency, better responsiveness
- Security – Zero Trust layered defense model: Deny-all Routing + Authentication + Encryption + Segmentation = cloaked network, reduced attack surface, and thwarted threat actors
- Performance – Less overhead, more scalability, dynamic optimization
- Savings – Reduces bandwidth, connectivity costs and third-party point tools; turns CapEx into OpEx; enables reallocation of engineering resources; provides optionality when considering renewing or purchasing other security tools

A TECHNICAL DESCRIPTION OF LINKGUARD

LinkGuard creates a self-contained, autonomously authenticated cryptographic networking fabric that extends across LAN, WAN, IoT, and private cloud environments by leveraging a dedicated hardware-based root of trust on pre-provisioned modules.

The solution creates a fabric of secure Layer 2 network channels, which protect end-to-end or point-to-point communications by creating new network segments; extending existing networks (LAN and WAN); and enabling rapid, self-contained micro-segmentation for traffic shaping and data protection. These segments can support all classes of provisioned networks and are address space isolated from the underlying infrastructure and from each other.

SEAMLESS INTEGRATION AND COMPATIBILITY

The LinkGuard platform is truly agnostic to existing or emerging technology regardless of architecture, including communication protocols, device placement, or most other environmental constraints. The platform supports all protocols compatible with IEEE 802.3 and is configurable to exist within and over any existing or new networking architecture(s), including remote and/or high-latency geographic locations. The packet-based Layer 2 encryption networking supports legacy and end-of-life systems even if they are not natively routable. Standard privileged access control systems such as jump servers, firewalls, and authentication servers are also easily integrated with the LinkGuard system for added flexibility and security.

ROBUST SESSION AUTHENTICATION AND ENCRYPTION

Cryptographic identities and mutual autonomous authentication define the protected networks and are part of a built-in public key infrastructure (PKI) resident in every LinkGuard installation. Private keys are never shared with any other authority, even within the LinkGuard solution, and public keys are only shared with trusted nodes inside the system. The self-contained key management system and pre-provisioned public keys enable the implementation of Zero Trust environments, operating independently of all third-party systems and ensuring that all communications are fully protected from the very first transmitted packet.

Mutual authentication between systems is a security industry best practice. LinkGuard exceeds this by using a simultaneous public key authentication process between all affected devices. Tunnels are built with dual encryption from the first packet using shared public key infrastructure credentials, autonomously authenticating both the sender and receiver without in-the-clear challenge responses of VPN connections. The solution is not vulnerable to common X.509 PKI vulnerabilities resulting from compromised certificate authorities with trust defined by cryptographic identities that are never transferred to any certificate authority or external certificate revocation list.

PREVENT LATERAL MOVEMENT OF ATTACKS

To further increase the layered security aspects that define defense-in-depth protection, LinkGuard defined secure zones and conduits restrict routing and prevent the lateral movement of threats across the enclosed network. The creation of these secure enclave segments separates them from general networking activity, protects those systems from compromise, and allows continued use of common infrastructure. By nesting these enclave segments or supporting multi-layer encryptions (Layer 3 within Layer 2 or vice versa), the solution can further secure and isolate mission critical devices and networks without resorting to extensive network redesign, further breaking the kill chain and greatly increasing network and environmental resiliency.

UNDISCOVERABLE FROM UNAUTHORIZED ACCESS

LinkGuard appliances are natively unresponsive to all reconnaissance or vulnerability scanning activities from inside or outside the protected segments, and the enclaved systems are only able to respond to such efforts when specifically provisioned to do so. This drastically reduces the attack surface of the network, including sensitive management traffic, and provides a layer of obfuscation similar to, and which can be used in combination with, active firewalling technologies. Malicious and accidental actors are prevented from enumerating and attempting to compromise the enclaved systems - what cannot be addressed cannot be targeted.

TRUSTED THIRD PARTY ACCESS

LinkGuard allows organizations to provide access to isolated network enclaves or segments without the inherent security risks from untrustable endpoints. Service providers and other third parties can use their personal PCs for remote monitoring, management, and general access using a secure virtual desktop that prevents potential malicious code from entering the network and any critical information from exiting the network. This enables organizations to increase their security posture for non-owned and non-controlled vendor and third party endpoints.

MASK THE VISIBILITY OF SYSTEM VULNERABILITIES

LinkGuard uses standards-based, FIPS 140-compliant cryptographic functions, ensuring confidentiality via 256-bit AES encryption and establishing integrity using SHA-256 authenticated data protection, nonrepudiation, and replay prevention. Perfect forward secrecy is ensured by preventing exposure of the private key portion of the cryptographic identity, even on the management plane, and keys are rotated at user-defined intervals, preventing the compromise activities that led to the Heartbleed and SecurID breaches. A hardware root of trust provides tamper protection for the trusted execution environment in which the cryptographic systems and management plane operate. This provides a self-enclosed platform that operates independently from all supporting or supported systems, becoming effectively invulnerable to common software or operating system-level attacks. This solution is enabled using dedicated systems that are independent of all other resources and establish single trust authorities for authentication and access management.

©2018 Blue Ridge Networks. All Rights Reserved

LINKGUARD: HIDE YOUR NETWORK. END CYBER ATTACKS.

Organizations also benefit because of the self-contained nature of LinkGuard's cryptographic overlay fabric which has a minimal impact on IT or security team operations and budget. The solution does not require manual rule setting and complex configuration, is easily deployed by unskilled technicians, is highly competitive in cost, and broadly complements existing security solutions while introducing only a negligible administrative overhead or network performance degradation. Utilizing future capabilities such as zero-touch provisioning prevents the need to install or maintain software at remote sites and auto-failover/failback options easily handle high availability requirements. In addition, the mobile and modular networking capabilities allow organizations the ability to obscure and protect end-of-life or highly vulnerable systems, buying time for more efficient application of compensating controls or other risk management solutions.

CONCLUSION

Organizations face a continual battle striking an effective balance between applying appropriate levels of operational security to their networks, establishing enough autonomy and segregation of responsibilities, and addressing compliance and risk management obligations to minimize exposure to reputational and financial losses. By providing an industry-vetted and time-tested network segmentation and data protection approach, LinkGuard enables granular communication, effective and resilient security, and a broad range of tools to assist companies in their efforts to manage and minimize the scope and scale of these issues. The LinkGuard platform for network extension and segmentation provides a quickly deployed, easily maintained, and highly complementary security solution that provides enhanced capabilities while addressing needs in a foundational and efficient fashion.

We look forward to the opportunity to provide you with further information about this field-tested solution and discuss how it can provide impenetrable protection for your most critical assets. Our customers gain access to a highly trained operations and cybersecurity specialists for consultation upon deployment. We fully enable your organization's mission with negligible impacts on the operational performance of your network.

BLUERIDGE®
NETWORKS

sales@blueridgenetworks.com
1-800-722-1168
BlueRidgeNetworks.com
linkedin.com/company/blue-ridge-networks
@BlueRidge