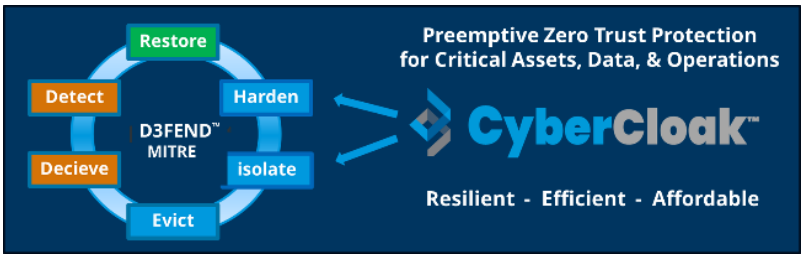
CyberCloak™

PREEMPTIVE ZERO TRUST PROTECTION FOR CRITICAL ASSETS, OPERATIONS, AND DATA

BLUERIDGE NETWORKS

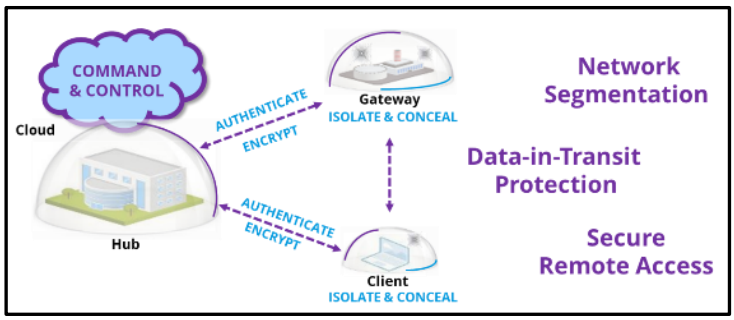
Hide Your Network Assets, Operations, and Data – CyberCloak™

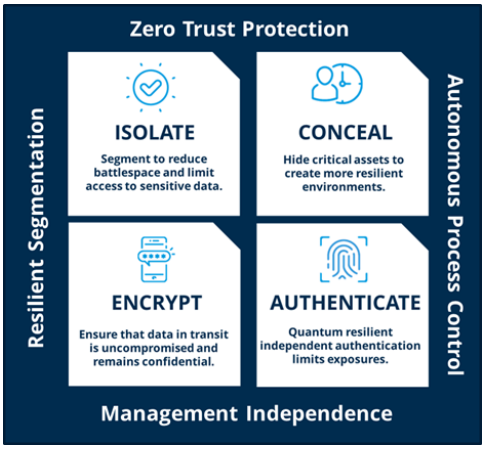
Defensive zero trust cybersecurity frameworks such as MITRE D3FEND™ the have evolved to promote preemptive hardening of network operations to protect mission critical assets, operations, and data with assurance. Achieving this objective has been challenging, particularly given the complexities of integrating Operational Technology (OT) with Information Technology (IT) frameworks. Blue Ridge Networks CyberCloak solution delivers a resilient, efficient, and affordable approach to harden networks.



CyberCloak seamlessly conceals network assets and distributed operations, protects data-in-transit, and reduces attack surface to preemptively prevent external discovery, unauthorized access, or data exfiltration. It is designed to "overlay" existing OT and IT infrastructure to minimize integration and operational complexity. It operates independently and autonomously with negligible latency or overhead to reduce sustainment requirements and increase operational performance. It delivers actionable intelligence to maximize mission performance.

CyberCloak solutions enable **high assurance segmentation, containment, encryption, authentication, and process control** simplify deployment and operations, that reduce battlespace, and reduce overhead for resilient, seamless, and affordable preemptive protection of OT/IT network assets, operations, and data = delivers an effective resilient, efficient, and affordable approach to harden networks. It seamlessly conceals your critical network assets and operations, protects your data-in-transit, and reduces your attack surface to preemptively prevent attackers from gaining access or exfiltrating critical data. It provides a preemptive **zero trust "overlay"** solution within existing infrastructure to segment and conceal, verify identity, authenticate and authorize access, and obfuscate protected systems and operations from unintended access. Its Data Privacy Facility (DPF) patented protocols and methodologies deliver protection from known and unknown threats and vulnerabilities within virtual private networks. Solutions utilizing CyberCloak capabilities have been heavily tested, certified, and deployed to protect U.S. national security and critical infrastructure industry assets and operations for over 20 years with no confirmed security breaches.





DPF is the Difference

Blue Ridge Networks **Data Privacy Facility (DPF)** patented protocols and methodologies create a self-contained, autonomously authenticated cryptographic networking fabric that extends across LAN, WAN, IoT, and private cloud environments. DPF protects the conventional layered network stack at the packet level against the inherent vulnerabilities of open source, open access protocols (IPSEC, TLS, SSL-VPN, etc.). 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 of data-in-transit. Segments are autonomously isolated, contained, encrypted, and authenticated independent of management plane dependency to eliminate

third-party vulnerabilities and complexities that plague alternative approaches. These segments can support all classes of provisioned networks and address space isolated from the underlying infrastructure and from each other to deliver protection from known and unknown attack surfaces and vulnerabilities within virtual private networks. This enables secure cross-domain interoperability and data transit integrity within OT/IT network operations.

Undiscoverable Externally – No Data Exfiltration – Reduce Battlespace

CyberCloak preemptively creates isolated, **self-contained segments** for networks, systems, applications, and dataflows in encrypted enclaves. 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. CyberCloak is natively unresponsive to all reconnaissance or scanning activities from inside or outside the protected segments. Enclaved segments are only able to respond to such efforts when specifically provisioned and authorized to do so. This **drastically reduces the attack surface** of the network, including sensitive management traffic. CyberCloak defined secure zones and conduits restrict routing and **prevent the lateral movement of threats** across the enclosed network segments. 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. CyberCloak 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. Malicious and accidental actors are prevented from discovering or accessing the enclaved systems - **what cannot be discovered, cannot be targeted**.

Preemptive Authentication and Data-in-Transit Control

Cryptographic identities and mutual autonomous authentication define the CyberCloak protected network segments utilizing a **built-in public key infrastructure (PKI)** resident in every CyberCloak installation. CyberCloak employs a unique simultaneous public/private key authentication process between all affected devices. Session trust is defined by cryptographic identities that are never transferred to any third party. Private keys are never shared with any other authority, even within the solution, and public keys are only shared with trusted nodes inside the system. Authentication processes support utilization of off-the-shelf (TPM 2.0) and proprietary (integrated) **hardware roots of trust**. All session authentication exchanges are therefore fully **protected from the very first transmitted packet**. This self-contained key management system **operates independently** from its management system eliminating the risks inherent in key exchange approaches dependent on management plane interfaces or third-party certificate methodologies. 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 for connections..

> CyberCloak enforces mutual autonomous authentication, constructs trusted connections, and simply ignores all other unknown or unapproved access.

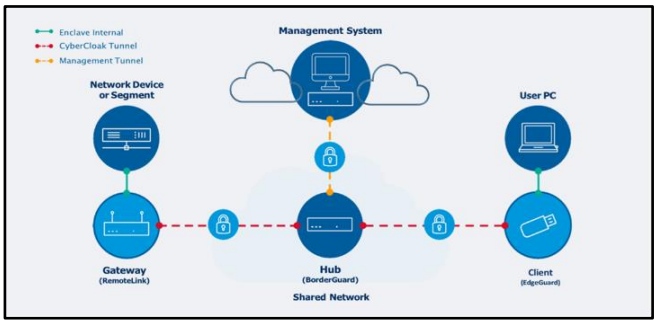
CyberCloak supports standards-based, FIPS 140-**compliant cryptographic functions**, ensuring confidentiality via 256-bit AES (and other post-quantum) encryption methodologies and integrity using uniquely modified SHA-256 authenticated data protection, nonrepudiation, and replay prevention. **Perfect 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. Integration with a supplied or resident hardware root of trust provides tamper protection for the trusted execution environment in which the cryptographic systems and management plane operate. CyberCloak utilizes streamlined DPF packet encryption methodologies with lower overhead and latency compared to other conventional packet encryption methods that **eliminates packet discovery in transit**. This solution is enabled using dedicated systems that are independent of all other resources and establish single trust authorities for authentication and access management.

Secure Remote Access

CyberCloak allows organizations to provide access to isolated network enclaves or segments without the inherent security risks of **access from un-trustable endpoints**. Access can be granted from un-controlled endpoints and personal PCs for remote monitoring, management, and general access. CyberCloak's secure virtual desktop software and systems prevent potential malicious code from entering the network and any critical information from exiting the network. Third parties can use their virtual private network tools operating within CyberCloak protected enclaves to access only those systems and operations within your network that you authorize for interface. This reduces or eliminates the impediments and complexities of coordinating material changes in IT network tools or procedures of third parties while ensuring authorized access remains under the control of your network administration. **Third parties can operate** within their CyberCloak protected enclaves without introducing lateral attack vulnerabilities to your enterprise control of systems and operations.

Seamless Compatibility, Deployment, and Operation

CyberCloak is **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.x and is configurable to exist within and over any existing or new networking architecture(s), including remote and high-latency geographic locations. Implementation of autonomous security and networking controls at the Open Systems Interconnection (OSI) Network Model – Layer 2 provides a 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. 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 CyberCloak system for added flexibility and security. CyberCloak is compatible with a wide range of Operational Technology (OT) assets (ICS, SCADA, sensors) and Information Technology (IT) architectures and systems (firewalls, switches, VPN, XDR).

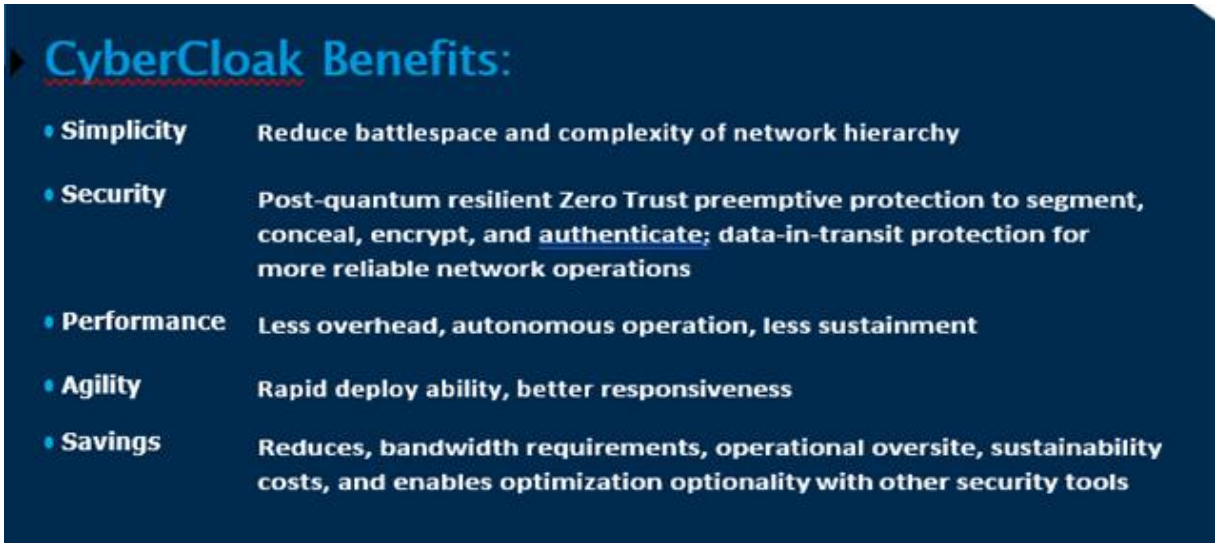


CyberCloak is easy to install and manage, requires low sustainment, and offers **more affordable** high assurance protection than comparable alternatives in the marketplace. It can **deploy in stages**, requiring no system upgrades or additional operation requirements, regardless of protocol or transport mechanism. Deployment configurations can **"mix-and-match"** CyberCloak-enabled hardware hosts and installable/embeddable software/firmware optimized to support a wide range of hub-and-spoke and mesh operations. The **"overlay"** deployment approach enables rapid deployment to protect both legacy and next generation OT/IT networks to streamline and complement existing security systems and tools. It does not require complex configuration processes, constant manual rule setting, and can be easily deployed by unskilled technicians,. CyberCloak can be managed in the field, within an enterprise network, or in the Cloud.

"Actionable" Intelligence

CyberCloak's management system monitors and captures critical operational and performance data to **enhance your visibility (but deny "theirs")**. Enclave configuration and policy management tools provide contextual data to enhance **insight of protected systems**. Access monitoring ensures operational control to streamline operations and enhance the **threat map** external to enclaves. Continuous monitoring of enclave operations enables **performance**

improvements. Management data can be ported to enterprise artificial intelligence (AI), specialized large language models (LLM), and critical resource management (CRM) to deliver **"actionable" intelligence** for high assurance operations.



Summary

CyberCloak delivers a **resilient, efficient, and affordable** approach to harden networks. It seamlessly conceals your critical network assets and operations, protects your data-in-transit, and reduces your attack surface to preemptively prevent attackers from gaining access or exfiltrating critical data. It provides a **preemptive zero trust** solution that "overlays" existing infrastructure with minimal integration requirements, operational complexity, latency, or overhead to segment and conceal, verify identity, authenticate and authorize access, and obfuscate protected systems and operations from unintended access. Its zero-touch provisioning, management plane independence, and autonomous operation materially reduce sustainment requirements for distributed systems and software at remote sites. Its auto-failover/failback geographically independent operations easily handle high availability requirements. It offers organizations a secure way to provide access to isolated network enclaves or segments without the inherent security risks from un-trustable endpoints. Powered by proprietary DPF technology, CyberCloak preemptively **protects against vulnerabilities, known and unknown, now and in the future**.

About Us

Blue Ridge Networks is a proven and trusted provider of highly secure cybersecurity solutions. Our mission is to deliver resilient, seamless, and efficient preemptive zero trust protection for critical assets, data, and operations. Our CyberCloak solutions utilize unique Data Privacy Facility (DPF) technologies with your OT/IT infrastructure and tools to reliably segment and control access for critical network operations. Government and commercial industry 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