Byos Secure Endpoint Edge™

Invisibility and Hardware-Enforced Security for Remote Worker Wi-Fi Security

SOLUTION OVERVIEW

The Challenge

With remote workforces increasingly connecting from coffee shops, airports, or home offices, every public or home Wi-Fi network becomes an open invitation for attackers. This creates a sprawling attack surface with devices exposed to scanning, eavesdropping, DNS hijacking, and lateral movement.

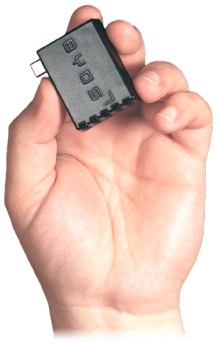
Why existing solutions fall short:

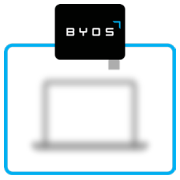
- OS-based endpoint protections like EDR solutions can be bypassed or evaded. Network perimeter protections can't protect endpoints before a compromise.
- Traditional endpoint security tools can't fully protect against untrusted Wi-Fi, making them vulnerable on public and home Wi-Fi networks.
- Centralized visibility into active sessions of distributed endpoints is often fragmented and slow, leaving organizations vulnerable.

The Invisible Shield for Your Endpoints

The Byos Secure Endpoint Edge™ is a thumbdrive-sized USB-C External Retransmission Device (RD) that delivers "first-hop" protection on untrusted Wi-Fi networks. By replacing the endpoint's native Wi-Fi connection with a hardware-enforced microsegment, Byos isolates the endpoint from the local network and makes it completely invisible to attackers. The result: No scanning. No lateral movement. No OS-level bypass.

Key Benefits



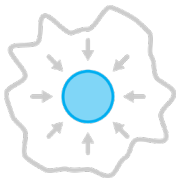


Asset Isolation and Invisibility on Unmanaged Networks

Byos assets are completely invisible on local networks, preventing discovery, fingerprinting, and unauthorized access attempts.

Plug-and-Play Deployment

Byos is agentless, connecting via USB-C, requiring no software or network changes, ensuring fast, non-intrusive deployment within minutes, not weeks.



Reduced Attack Surface

Eliminate exposure for your fleet of endpoints to internal threats like lateral movement and ransomware.

BYOS

Centralized Control with Byos Management Console™

Command your Edges from Anywhere - The Byos Management Console™ is the command center of the Secure Edge platform, giving administrators a single, centralized view of every deployed device. Purpose built for Enterprise manageability, it gives real-time visibility into endpoint activity, along with granular policy enforcement and rapid incident response capabilities. Administrators can securely push policies, monitor threats, and even contain ransomware infections instantly—all without exposing critical assets to the public internet.

Trusted Communications with Byos Secure Lobby™

A Secured Tunnel for Communications - The Byos Secure Lobby™ is a fully encrypted software-defined network (SDN) overlay that ensures private, policy-controlled communications between protected devices - regardless of the network they connect from. By removing exposure to the public internet and enforcing trusted exit nodes, Secure Lobby allows organizations to extend secure connectivity to contractors, employees, and even legacy systems while keeping endpoints isolated from lateral movement risks.

Use Cases

Defense & Government

- CSfC-compliant mobile access for field agents and contractors
- Secure laptop access to private data and classified systems over public and unmanaged Wi-Fi

Enterprise Remote Work

- Isolate executive and employee devices, across OSI layers 1-5, from threats from high-risk Wi-Fi in hotels, conferences, and airports
- Ensure compliant connectivity for remote workers handling sensitive data in regulated industries

Third-Party Access Control

- Provide contractors secure network entry or granular, temporary access for third-parties without exposing internal assets
- Prevent lateral movement between third party devices and corporate networks, and enforce traffic routing to secure cloud services

Designed for CSfC, Ready for Everyone

Designed to meet NSA CSfC Mobile Access Capability Package requirements, it ensures compliance for government and defense use cases, as well as for commercial regulated industries.

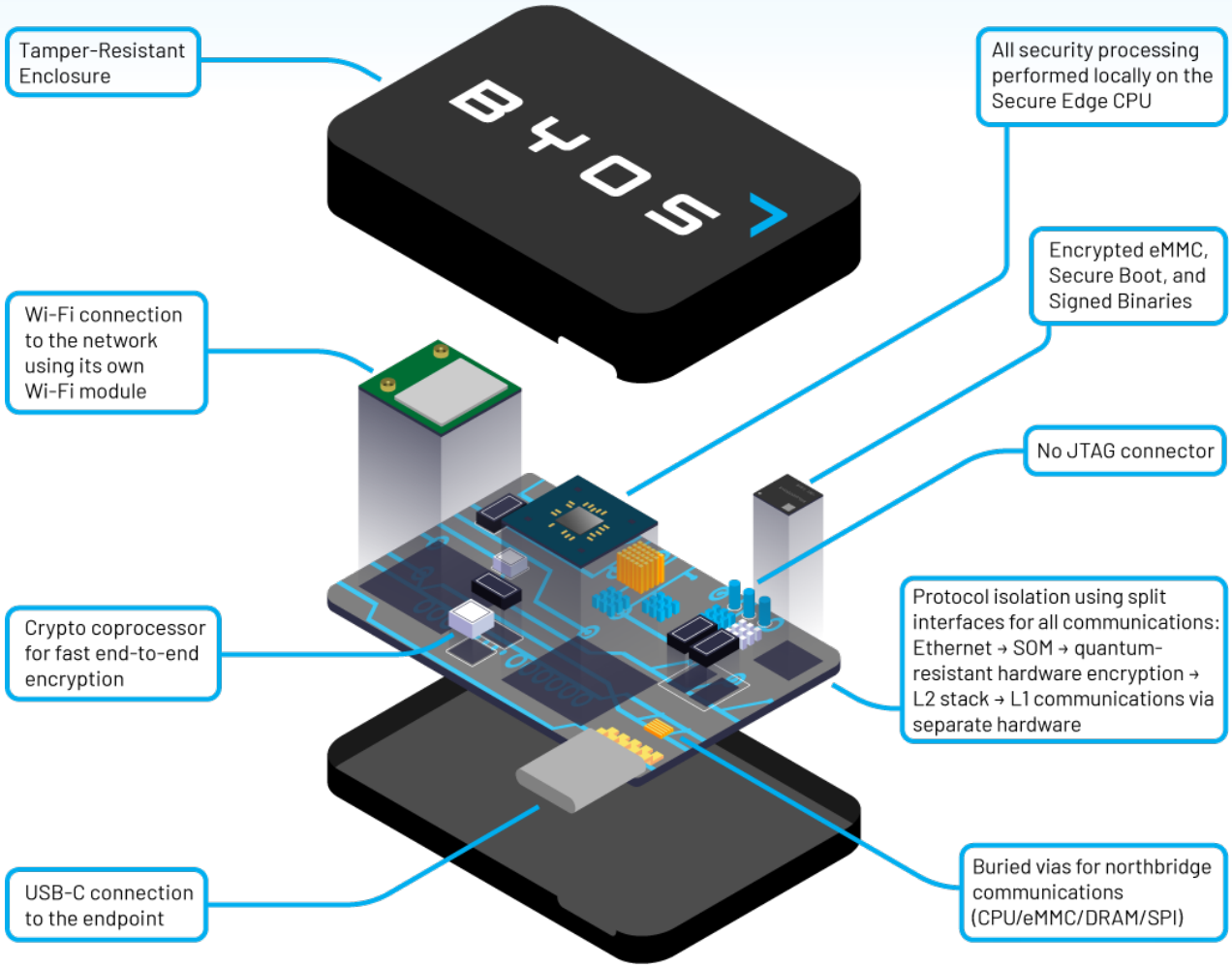
- Fully compliant with MA-CP 2.6 – 11.8 Retransmission / 11.9 Hardware Isolation
- Manufactured in the USA with a certified, auditable supply chain
- Byos Cryptographic Module is FIPS 140-2 validated, ensuring compliance with stringent security standards required by government and regulated industries.

CSfC Compliant

FIPS 140-2 Validated

Security By Design

Unlike traditional tools or software agents, Byos Secure Endpoint Edge™ enforces protection in hardware and replaces the endpoint's native networking module/Wi-Fi, ensuring true isolation on any network. It contains its own processor, encrypted DNS server, NAT/DHCP stack, and FIPS-validated cryptographic module—so threats never reach the host operating system. This dedicated hardware design provides isolation, invisibility, and CSfC-compliance for even the most sensitive environments.



Technical Specifications

- Dimensions: 1.76 x 1.38 x 0.57 in. (4.48 x 3.49 x 1.45 cm)
- Type of Device: Plug-and-Play USB Ethernet Gateway
- Power Consumption: Under 2W
- Connector: USB-C 2.0 (Compatible w/USB-A adapters)
- OS Requirements: Any OS compatible with USB-OTG
- Special Driver Requirements: None
- Manufactured in: Canada/USA
- Certified Supply Chain of Hardware components: Yes
- Certified Chain of Custody of Software: Yes
- Software Updates: Automatic, Over-the-air

Whether protecting private data for defense and government agencies or securing enterprise remote workers, Secure Endpoint Edge brings hardware-enforced trust to any network—without slowing you down.
Connect with us at engage@byos.io or at byos.io/request-demo to see a demo!