Byos Secure Edge as a CSfC Retransmission Device

Wi-Fi Security for Remote Workers

USE CASE

Executive Summary

The increase in remote, on-the-go work environments demand better endpoint protection. The Byos Secure Edge improves Wi-Fi security through hardware-enforced isolation, giving IT and security teams the confidence to support remote users on any uncontrolled public or home Wi-Fi networks.

The Challenge

Organizations face critical security gaps when devices connect to unmanaged networks like public and home Wi-Fi, expanding the attack surface. Current security solutions fall short in several ways:

- Software-based endpoint protections installed on the OS can be bypassed/evaded
- Perimeter-based protections cannot protect individual endpoints before an attacker gains a foothold
- Getting centralized runtime visibility into distributed endpoints' active sessions is cumbersome
- Common attack vectors include scanning/enumeration, eavesdropping, remote access exploits, evil-twin Wi-Fi, lateral network infections, and DNS hijacking

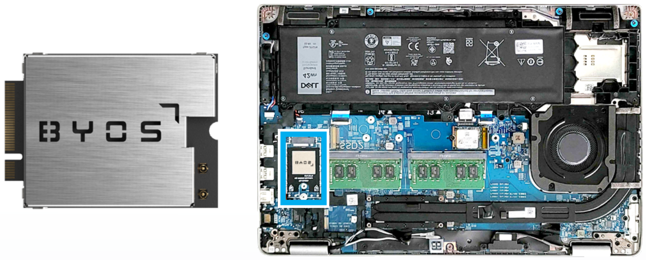
About CSfC Retransmission Devices

Retransmission Devices (RD) are critical components within the NSA's CSfC Mobile Access architecture, serving as secure intermediaries between End User Devices and classified networks. They provide:

- Hardware-based isolation
- Dedicated management interfaces
- Integrated firewall capabilities
- Protocol break implementation
- Comprehensive security controls
- Audit and monitoring capabilities

The Solution: Byos Secure Edge™ Technology

Byos offers two form factors to address these challenges for Remote Laptops:



1. Secure Endpoint Edge™ - External RD

A plug-and-play hardware edge device providing "first hop" protection when connecting to unmanaged networks.

Technical Specifications:

- **Dimensions:** 1.76 x 1.38 x 0.57 in. (4.48 x 3.49 x 1.45 cm)
- **Type:** Plug-and-Play USB Ethernet Gateway
- **Power Consumption:** Under 2W
- **Connector:** USB-C 2.0 (Compatible w/USB-A adapters)

2. Secure Embedded Edge™ - Internal RD

A System on Module (SOM) embedded inside laptops in the WWAN/WAN port.

Technical Specifications:

- **Dimensions:** 42mm x 30mm x 4mm
- **Type:** Embeddable System on Module
- **Power Consumption:** 1.0W-2.5W, 3.3V
- **Connector:** M.2

CSfC Compliance

The Byos Secure Edge™ Technology meets the NSA's Commercial Solutions for Classified (CSfC) requirement: Mobile Access Capability Package (MA-CP) 2.6 - 11.8 Retransmission / 11.9 Hardware Isolation, which describes several enhancements to the hardware isolation requirements for government-owned retransmission devices (RDs).

CSfC Requirement	Byos Capability
The main change is that on the internal side, the RD can only be connected to EUDs through a hard wired connection such as Ethernet or Ethernet over USB.	**The Byos Secure Edge™ connects to the EUD via a hardwired M.2 connection.**
The RD may not use Wi-Fi on the internal side for connection to EUDs. Wi-Fi must be disabled on the EUDs.	**The Byos Secure Edge™ replaces the native Wi-Fi on the EUD.**
The RD must implement a software or hardware firewall to restrict traffic that is allowed to flow through the device.	**Traffic control is enforced by the Byos Secure Edge™ and applied via policy group from the Byos Management Console™**
The chip providing connectivity on the external side must be physically separate from the main processor.	**The Byos Secure Edge™ processor and Wi-Fi module are physically separate.**
The RD must implement a protocol break between the RD and the EUD.	**The Byos Secure Edge™ has its own DHCP, DNS, NAT, and thus isolates RD and EUD traffic so that they can be independently managed.**

Security and Manufacturing Excellence

Both the Secure Endpoint Edge™ and Secure Embedded Edge™ share industry-leading security and manufacturing standards that set them apart in the market. Compatible with any operating system supporting USB-OTG, these devices require no special drivers, enabling seamless deployment across any organization. Proudly designed and manufactured in the USA, they maintain the highest levels of supply chain integrity. Every component undergoes rigorous verification through certified supply chains, meeting stringent security standards. A complete chain of custody certification from design to deployment ensures zero compromise in security. Both solutions feature automatic over-the-air updates, keeping security current without requiring manual intervention. The **Byos Cryptographic Module** is FIPS 140-2 validated, ensuring compliance with stringent security standards required by government and regulated industries.

FIPS
140-2 Validated

Certificate #4969

Management and Control

The Byos Management Console and Secure Lobby SDN Overlay provide comprehensive control and management of remote workers deployed across the world:

Key Features:

- Centralized management across multi-network environments
- Real-time policy deployment
- Remote lock capabilities
- Asset discovery and management
- Secure asset-to-asset remote access
- Multi-layer access control zones

Feature Comparison

Feature	**Byos Secure Edge**	GoSlient Cube	Netgear Nighthawk
Protection			
Network Attack Protections	✓	Partial (Limited prevention)	✗
RTD Decoupled from Asset's OS	✓	✓	✗
Valuable without the Tunnel?	✓	Partial (Only basic firewall)	✗
Asset Cloaking	✓	Partial (Not without tunnel)	✗
Captive Portal Protection	✓	✓	✗
Advanced Crypto and Security	✓	✓	✗
Roaming Security Posture	✓	✗	✗
Usability			
Portability	✓	Partial (Requires extra components)	
Over-the-Air Updates	✓	✓	✓
System Maintenance and Upgrades	Included	✗	✗
Remote Support	Included	✗	✗
Management			
Central Fleet Management	✓	✗	✗
Policies	✓	✗	✗
Activator Identities	✓	✗	✗
Remote Lock	✓	Partial (Cannot remotely disable device)	✗
SDN Overlay (Secure Lobby™)	✓	✗	✗
Asset Discovery + Management	✓	✗	✗
Network Map	✓	✗	✗
Secure Remote Access to Assets	✓	✗	✗
Multi-Layer Access Control Zones	✓	✗	✗
Guest Access	✓	✗	✗

To learn more about how Byos enables government and defense agencies to enhance remote security, aligning with CSfC compliance and protecting against cyber threats, request a demo with our team here: byos.io/demo