Byos Secure Embedded Edge™

Protect, manage, and control laptops with microsegmentation using Byos' internal retransmission device

BYOS

SOLUTION OVERVIEW

Devices connecting to unmanaged networks like public and home Wi-Fi expands the sprawling attack surface.

There is a fundamental gap in protection between endpoints and the networks they connect to: endpoint and network security technologies fail to protect at the ingress/egress point of traffic to and from the endpoint, aka at the edge:

- Software-based endpoint protections installed on the OS can be bypassed/evaded.
- Perimeter-based protections cannot protect individual endpoints on the network before an attacker gains a foothold and propagates.
- Getting centralized runtime visibility into the active sessions of distributed endpoints is cumbersome with current tools.

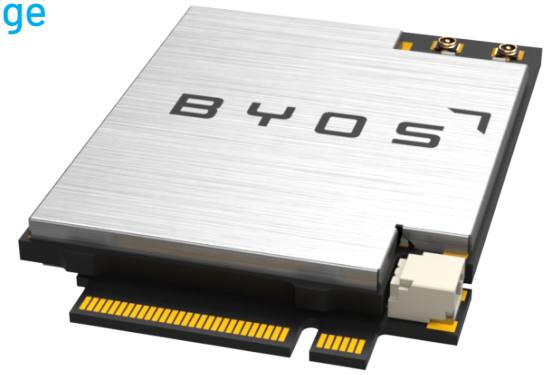
Because of this, attackers leverage a number of tactics that many solutions are unable to protect against: Scanning/ Enumerating/Fingerprinting, Eavesdropping, Remote Access Exploits, Evil-Twin Wi-Fi, Lateral Network Infections, and DNS hijacking to name a few.

Hardware-enforced Security at the Edge

An internal retransmission device providing network security at the edge, independently of the host and cloud.

Byos Secure Embedded Edge™ is a secure networking card that is embedded inside of Laptops, in the WWAN/ WAN port. Connecting to the laptop using an M.2 connector, it draws less than 2 watts of power. It replaces the Laptop's native Wi-Fi module, acting as a retransmission device, providing microsegmentation protection across OSI Layers 1-5 by becoming the gateway.

This device isolates the connected laptop from the network, enhancing security beyond software solutions by acting as the sole entry and exit point for internet traffic, thus preventing bypass attempts and stealth attacks originating within the endpoint's operating system.



Core features include:

- **Network Attack Protection** - Out of the box protections include: eavesdropping, enumerations, spoofing, lateral movement, etc.
- **Retransmission Device (RTD)** - Decoupled from the Asset's OS.
- **Asset Cloaking** - Makes the Asset it's protecting undiscoverable and inaccessible in the local network.
- **Captive Portal Protection** - Allows for greater security on captive portal based networks.
- **Advanced Crypto and Security** - Key features include encrypted filesystems, secure boot, tamper-resistant, etc.
- **Roaming Security Posture** - Mobile form factor that is low power draw, no batteries, plug-and-play, agent-less and driverless.

Byos Secure Embedded Edge Technical Specifications:

- Dimensions: 42mm x 30mm x 4mm
- Type of Device: Embeddable System on Module
- Power Consumption: 1.0W-2.5W, 3.3V
- Connector: M.2
- OS Requirements: Any OS compatible with USB-OTG
- Special Driver Requirements: None
- Manufactured in: USA
- Certified Supply Chain of Hardware components: Yes
- Certified Chain of Custody of Software: Yes
- Software Updates: Automatic, Over-the-air
- Laptop Compatibility: Any Laptop with a WWAN slot.

Compliance with the Highest Security Standards

Byos Cryptographic Module is FIPS 140-2 Validated.
Visit the NIST CMVP website for more details -Certificate #4964

FIPS 140-2 Validated

The Byos Secure Embedded Edge™ meets the NSA's Commercial Solutions for Classified (CSfC) requirement:

6.3.2 ENHANCED HARDWARE ISOLATION REQUIREMENTS FOR RETRANSMISSION DEVICE, 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 Embedded 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.	There is no native Wi-Fi Interface as Byos Secure Embedded Edge™ replaces it.
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 Embedded 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 Embedded Edge™ processor and Wi-Fi module are physically separate.
The RD must implement a protocol break between the RD and the EUD.	The Byos Embedded Edge has its own DHCP, DNS, NAT, and thus isolates RD and EUD traffic so that they can be independently managed.
The RD must be managed over a wired connection.	The Byos Secure Embedded Edge™ was developed to be a hardened "Bastion Host" on behalf of the EUD. It provides protections against wired and wireless attacks like spoofing, enumeration, fingerprinting, exploiting, etc.

Byos Management Console and Secure Lobby SDN Overlay

The **Byos Management Console** is a cloud-cased control plane to manage Secure Embedded Edge™ devices centrally. **Byos Secure Lobby™** is a secure Software Defined Network (SDN) Overlay for private secure communications between Byos-protected laptops. Combined they offer a simple way for network security admins to manage a distributed fleet of Edges with ease:

- **Centralized Management** of assets across multi-network environments (ie. remote workers across the world and critical infrastructure devices in the same fleet).
- **Real-time policy pushing** for instant control over remote devices.
- **Remote Lock capabilities** for immediate incident response.
- **Asset Discovery and Management** to find the ports and services that are running on your managed laptops.
- **Secure remote access** from Asset to Asset is facilitated through Secure Lobby™.
- **Multi-Layer Access Control Zones** - OSI Layer 2, 3, and 4 controls for proper segmentation within the Overlay.
- **Secure Lobby™ Guest access** with granular permissions and controls for letting 3rd-parties access.

Safe to Connect, Free to Work.

The increase in remote, on-the-go work environments demands better endpoint protection.The Byos Secure Embedded Edge improves 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.

Get Started

Contact us at engage@byos.io, or byos.io/request-demo to schedule your demo today!