# Invisible by Design: Security at the Edge

Why Trust Us

TRUST OVERVIEW

**Byos is built on the principle that true security starts at the edge. Our Secure Edge™ solutions are built with a security-first mindset, embedding protection, privacy, and resilience into every layer of the architecture. And every product we design reflects this is our commitment to isolation, integrity, and assurance - from cryptographic protections to cloud security.**

## Core Tenets

### Security First, Always

- End-to-end encryption locks all communications between Secure Edge devices and the Management Console admin interface.
- All personnel are North American-based cybersecurity experts, ensuring deep security culture.

### Privacy by Design

- We never inspect or monetize traffic, nor sell or rent personal information to third parties, ensuring data remains strictly private.
- End-to-end encryption locks all communications between Secure Edge devices and the Secure Lobby management console.

### Edge Security

- Each device operates within its own isolated microsegment, severing opportunities for lateral movement.
- All security processing is done locally within the Secure Edge, independent of cloud servers, reducing your exposure and protecting your data.

### Continual Testing

- Testing at all product stages, including **SSDLC**, internal and third-party penetration tests.
- Byos offers an open **Bug Bounty Program** to identify and address potential threats before they can impact anyone.

### Multi-layer Protection

- Secure Edge has multiple layers of protection built in, backed by both Hardware and Software security mechanisms.
- Operates within **High Assurance Network Access (HANA)** frameworks, aligned with **Zero-Trust** mandates.

### Cloud Security

- Our servers are compliant with **Cloud Security Alliance** standards, further protecting you against vulnerabilities.
- Security features include:
  - TLS 1.3 for all data in transit
  - AES-256 encryption for data at rest
  - Per-device, rotating IVs for encryption sessions
  - No DNS logs or traffic inspection
  - No TLS interception - we do not read user session data
  - No storage of personal or Secure Edge™ traffic
  - No data sharing or resale practices - ever

BYOS

### FIPS 140-2 Validated

Byos Cryptographic Module is FIPS 140-2 Validated. U.S. law (and increasingly Canada) mandates FIPS for government and regulated sectors. Visit the NIST CMVP website for more details - Certificate #4964

### Built in the USA

Byos Secure Edge™ hardware has a proprietary hardware board that is manufactured in the USA, with a certified supply chain of components and a certified chain of custody of software - no backdoors, no weak links. Every component undergoes rigorous verification through certified supply chains, meeting stringent security standards.

## Technical Architecture

**Secure Edge** are the hardware retransmission devices that enforce isolation via inline encryption and logical separation.

**Management Console** provides centralized policy management, activator workflow, secure key custody, and secure monitoring and visibility.

**Secure Lobby**, as a **Secure Software-Defined Network (SDN) Overlay** with Layer 2 encrypted tunnels, for isolated communications between Edges.

## Certifications

ITAR Compliant

FIPS 140-2 Validated

CSfC Compliant

CE

FC

# Byos as CSfC Compliant Retransmission Devices

The **NSA's Commercial Solutions for Classified (CSfC)** program defines requirements for **Retransmission Devices (RDs)** that securely bridge unmanaged endpoints with classified networks. Byos Secure Edge™ solutions meet these requirements by delivering hardware-enforced isolation, protocol break, audit and monitoring capabilities among others - empowering mission-ready, Zero Trust connectivity from virtually anywhere.

Byos Secure Edge™ technology was built to comply with the **NSA's CSfC Mobile Access Capability Package (MA-CP) 2.7** requirements, specifically - **11.8 Retransmission** and **11.9 Hardware Isolation**, which describes several enhancements to the hardware isolation requirements for government-owned retransmission devices (RDs). Byos' solutions feature automatic over-the-air updates, keeping security current without requiring manual intervention.

## Advisory Board Oversight

At Byos™, trust starts at the top. Our Advisory Board brings together nationally recognized leaders in cybersecurity, intelligence, military, and enterprise IT—guiding our strategic approach to secure innovation and Zero Trust adoption.

### John S. Pistole

Former Deputy Director of the FBI and TSA Administrator, John brings decades of national security leadership and operational insight to guide high-assurance policy and threat response.

### Lt. Gen. William Bender, USAF (Ret.)

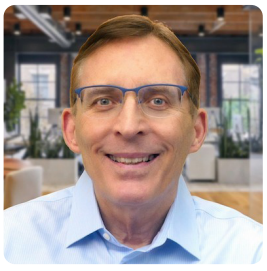
Former CIO of the U.S. Air Force, General Bender provides strategic direction on defense modernization, Zero Trust architecture, and secure digital transformation.


### Dave Lewis

A globally respected CISO and security thought leader, Dave advises Byos on modern threat intelligence, risk mitigation, and enterprise cybersecurity practices.

### Jeff Johnson

Former CTO of the FBI and VP at USPS, Jeff brings deep knowledge of government IT modernization and secure digital service delivery at scale.



### Bob Carver

A pioneer in cyber threat detection and large-scale security operations, Bob contributes guidance on threat monitoring, encryption, and resilience for critical infrastructure.

### Erik Wille

A seasoned CISO and security program builder, Erik offers executive-level expertise on security governance, business-aligned infosec, and high-trust organizational culture.

## Contact Byos Today

For organizations looking to strengthen their security, Byos offers a hardware-backed, FIPS validated microsegmentation platform - protecting everything from remote devices to critical infrastructure. Contact Byos at byos.io/contact-us or engage@byos.io