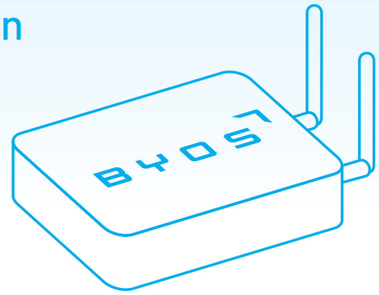
Byos Secure Gateway Edge

Microsegmentation for Critical Infrastructure

SOLUTION OVERVIEW

Introducing Byos: Simpler, Plug-and-Play Security at the Edge, for Maximum Protection



The Byos™ Secure Gateway Edge is a compact, hardware-based security solution that isolates and protects networked devices through zero-trust microsegmentation. Designed for OT, IoT, and IT environments, it prevents lateral movement, secures remote access, and defends against cyber threats—all without requiring major infrastructure changes. By physically isolating endpoints and processing security locally, Byos™ ensures robust, host-independent protection across OSI layers 1-5 against modern attack techniques, making it an ideal solution for securing critical and legacy assets in any network.

The Byos Secure Gateway Edge can be deployed with a number of different types of endpoints, so long as they speak TCP/IP

- Desktops
- Servers
- Injection devices
- Hospital workstations
- ATMs
- PLCs
- RTUs
- Telemetry devices
- Imaging devices
- HMIs
- Industrial PCs
- Security cameras
- UPS systems
- Fire alarms
- Compressors

Greater Connectivity with Tighter Security for OT, IoT & IT

The common key challenges include:

- Legacy operating systems create security risks as unsupported systems can no longer be patched against known vulnerabilities.
- Use of deprecated or insecure software components/libraries increases the likelihood of vulnerabilities
- Network segmentation strategies for limiting malicious lateral movement are inconsistently applied on today's diverse networks.
- Common protocols left open provide uncontrolled access to attackers, leaving the broader network vulnerable.
- Rapid growth and diversity of IoT devices and operating systems make it increasingly difficult to secure networks.

Two Gateway Edge Models for Different Requirements

Byos Gateway Edge 1000 provides secure connectivity for OT, IoT and IT devices including legacy infrastructure in a compact industrial gateway form factor.

Byos Gateway Edge 2000 is the latest version of the hardware. Notable improvements are FIPS 140-2 validated Software, 1GbE ports for faster speeds, and a security rivet for tamper-resistance.

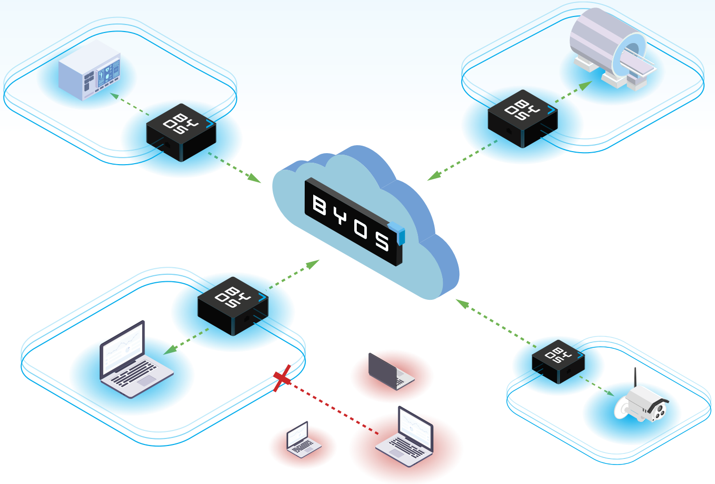
Product Comparison - Technical Specifications

	Model	GW 1000	GW 2000
Details	Customers	Commercial	Defense
	Manufacturing	North America	U.S.A.
	Supply Chain	-	ITAR Compliant
	Operation Mode	Wi-Fi Client Mode | Ethernet Mode	
	Software	-	FIPS 140-2 Validated Cryptographic Module #4964
	Hardware Security	Secure Boot, Encrypted Root Filesystem	Secure Boot, Encrypted Root Filesystem, Anti-tamper security rivet
Network	LAN (downlink)	100Mbps Ethernet Port	1Gbps Ethernet Port
	WAN (uplink)	1x - 1Gbps Ethernet port	
	Wi-Fi	802.11ax Wi-Fi interface	802.11ax Wi-Fi interface/ 2x2 802.11a/b/g/c
	PCIE	-	Expandable PCIE interface
Mechanical Specifications	Dimensions	112 x 84 x 25 mm	112 x 82 x 43 mm
	Enclosure Material	Anodized Aluminium	
	Cooling	Passive, fanless design	
	Weight	250g	200g
	Weight (As Shipped)	450g	400g
Electrical Specifications	Supply Voltage	Unregulated 8V to 36V	
	Power Consumption	2W - 7W	
	Regulatory	CE / FCC	FCC
	EMC	EN 55032/5, EN 61000-6-2, EN 61000-6-3	-
	Safety	EN/UL/IEC 62368-1	-
Reliability and Environmental	MTTF	0° to 60° Ct	
	Warranty	1 Year	
	Operational Temps	Commercial: 0° to 60° C Extended: -20° to 60° C Industrial: -40° to 80° C	
	Storage Temps	- 40° to 85° C	
	Relative Humidity (Operation)	10% to 90%	
	Relative Humidity (Storage)	05% to 95%	

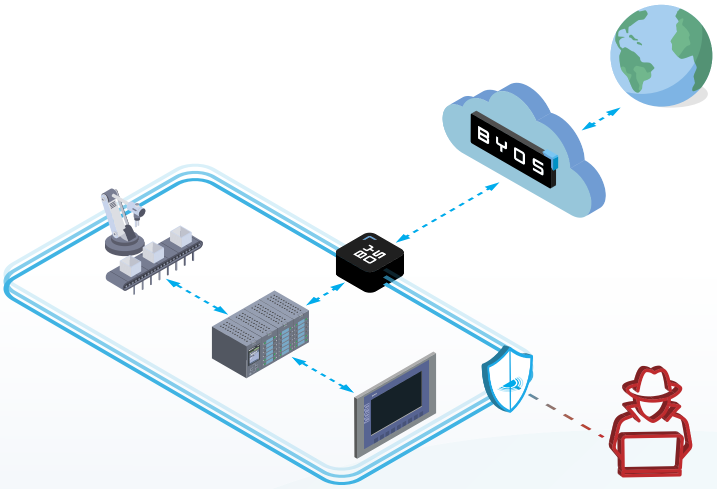
Centralized Control for Security Management and Monitoring

The Byos Management Console (MC) is the first component of the Byos Cloud Infrastructure. It is used for centrally managing all deployed Byos Secure Gateway Edge devices. Key features include:

- **Security policy provisioning** - administrators can provision devices into different "groups" based on their specific characteristics, and can apply granular security policies to those groups at the click of a button.
- **Threat management** - The Byos Secure Gateway Edge collects threat signals and reports them back to the Management Console, and allows the administrator to have a view into the overall security posture of the fleet. Administrators can enable the Ransomware killswitch, which will automatically isolate the device from the internet when the Secure Gateway Edge detects malicious network activity.
- **Security stack integration** - The edge telemetry data of each deployed Secure Gateway Edge is aggregated centrally in the Management Console. Administrators can integrate a number of existing tools including SIEM, IAM, and Asset Management tools.



Software-Defined Network Overlay for internet-isolated communications



As the second part of the Byos Cloud Infrastructure, Byos Secure Lobby™ establishes a Secure Software-defined Network (SDN) Overlay through Layer 2 tunnels, encrypting all traffic and isolating assets in private microsegments. Byos Secure Lobby provides secure remote access to devices on third-party networks without exposing the host to the internet or requiring changes to local network configurations. This enables administrators and technicians to perform service, maintenance, and troubleshooting remotely, eliminating the need for on-site visits. Secure Lobby is especially valuable for managing multi-party access across multi-site networks.

Key Features:

- **Asset Management** - The Byos™ Secure Gateway Edge can discover and map networked endpoints, performing IP and port scans to display critical details such as private IP addresses, MAC addresses, and open ports.
- **Flexible Deployment** - Secure Lobby can be deployed as a Cloud-based SaaS service managed by Byos™ or self-hosted by the customer in their own infrastructure for greater data control and compliance.
- **Granular Access Control** - With granular Layer 3 and 4 access controls, administrators define device permissions, traffic routes, and connection parameters to control device access fully.

BYOS

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

FIPS
140-2 Validated

Why do customers deploy Byos?

The Benefits of Microsegmentaton

- **Legacy OS protection**

Securely prolong the life of IT infrastructure running legacy applications and unsupported OS that are not ready to be retired

- **Secure Connectivity**

Connecting previously air-gapped devices to the network for more efficient and secure remote maintenance and monitoring.

- **Zero Touch Deployment**

Non-intrusive deployment to existing network configurations, without having to expose internal devices to the internet.

- **Reduced Attack Surface**

Eliminated exposure of unpatched legacy networked devices to internal threats like lateral movement and ransomware.

- **Reduced Field Service Time**

Reduced technician trips onsite for service and maintenance saving operational expenses.

If you'd like to learn more about Byos, visit us at byos.io

or connect with us at engage@byos.io