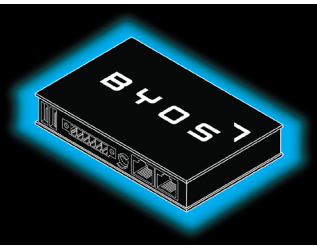
BYOS

Protecting, Managing, and Accessing IoT Devices through Edge Microsegmentation

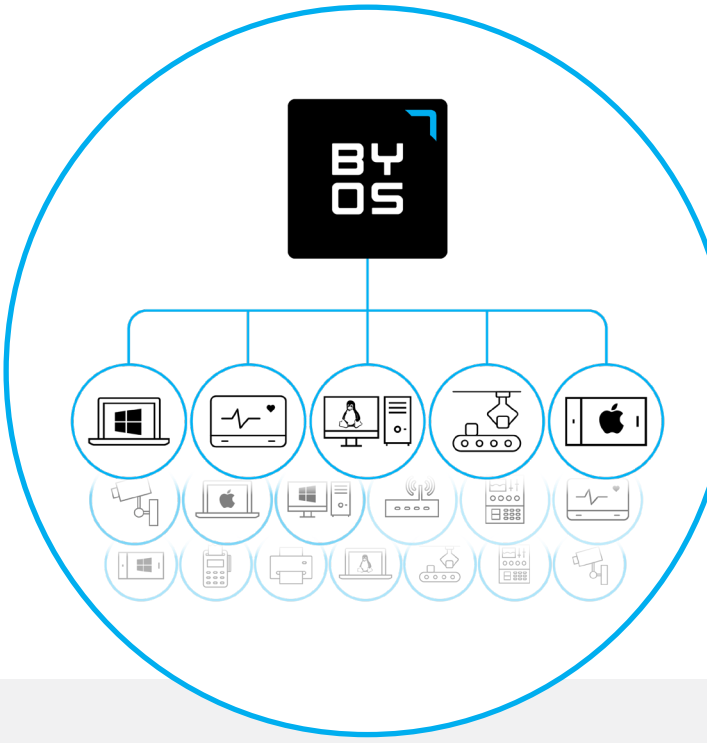


Byos Secure Gateway Edge for Zero Trust Networking

As IoT Continues to Grow, So Do System Vulnerabilities

Corporate network security has evolved to protect conventional networking devices, such as laptops, desktops, and servers, but with this proliferation of connected devices, attackers are now targeting the weakest link—IoT devices. The sheer number of new IoT connections over the next 5 years, the increased digitization capabilities of certain IoT markets (e.g., healthcare, utilities, industrial, infrastructure, and smart cities), and the increase in connected users and assets is increasing the need for security in IoT devices.[1]

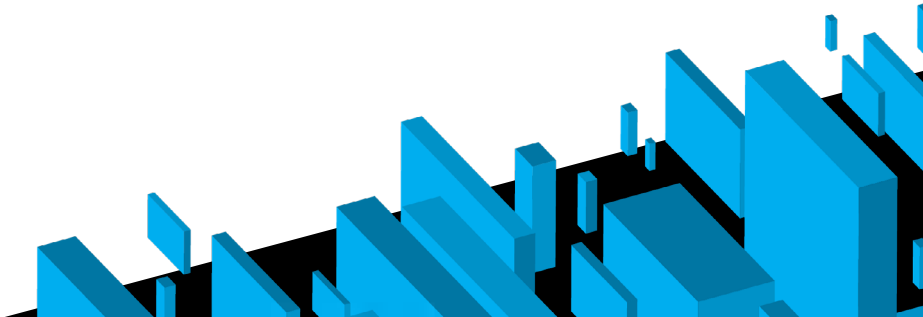
Medium and high security requirement IoT devices like healthcare monitoring devices, intelligent transportation, fleet management, smart grid, etc. are used as an entry point into the larger corporate networks, where the most valuable data resides. Legacy IoT devices such as servers, modems, PLCs, controllers, and networked medical devices are especially vulnerable as attack methods increase in sophistication. The lack of IoT device management capabilities also contributes to challenges, including the absence of built-in security monitoring and update management capabilities.



Common Challenges When Securing IoT Devices

One of the biggest risks associated with IoT is that security measures and systems are not incorporated into the core design of devices.[2] Malicious attackers see this as an opportunity, which led to a 300% increase in cyber attacks on IoT devices last year.[3]

- 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



1. ABI Research, "Connected & Protected: The vulnerabilities and opportunities of IoT Security" 2021
2. Deloitte, "How Much Do Organizations Understand the Risk Exposure of IoT Devices?" 2019
3. Forbes, September 2019

What does the Byos microsegmentation solution offer?

The Byos Secure Gateway Edge Solution has three main capabilities, incorporating different components for security, management, and access of IoT devices:

Plug-and-play network security at the edge, independent of the host or the cloud

Byos Industrial µGateway™ ("microgateway") is a Secure Gateway Edge deployed as a standalone industrialized Gateway. It isolates devices sitting behind it onto their own microsegment within the local network, protecting them from OSI layer 1-5. It has 3 different operation modes:

1. Wi-Fi Hotspot-mode for Wireless-capable Devices
2. Ethernet-mode for Legacy and Wired Devices
3. Client-mode to connect to a pre-existing Wi-Fi Network

This approach provides protection from the attacks that are most commonly seen on Wi-Fi networks: eavesdropping, lateral movement, DNS poisoning, route alteration, Exploiting and DDoS, and rogue AP. Being at the real edge means security isn't dependent on the Host' IoT devices OS nor is delegated to the cloud - all security processing happens locally on the µGateway for maximum protection against typical attacks that rely on evasion techniques.

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

Industrial µGateway Specifications

Network

LAN

- 1000Mbps Ethernet Port
- 100Mbps Ethernet Port

Wi-Fi

- 802.11ax Wi-Fi interface

Mechanical Specifications

- Dimensions - 112 x 8 x 25 mm
- Enclosure Material - Aluminum
- Cooling - Passive, fanless design
- Weight - 450 grams

Electical Specifications

- Supply Voltage - Unrnegulated 8V to 36V
- Power Consumption - 2W - 7W

Compliance

- Regulatory - CE, FCC
- EMC - EN 55032/5, EN 61000-6-2, EN 61000-6-3
- Safety - EN/UL/IEC 62368-1

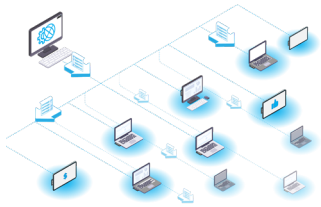
Reliability and Environmental

- MTTF - 200,000 hours
- Warranty - 5 years

- Operating Temperature
  - » Commercial: 0° to 60° C
  - » Extended: -20° to 60° C
  - » Industrial: -40° to 80° C
- Storage Temperature: -40° to 85° C
- Relative Humidity
  10% to 90% (operation)
  5% to 95% (storage)

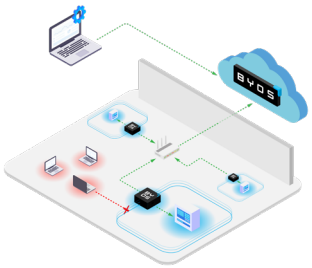
Centralized control for security management and monitoring

The **Byos Management Console (MC)** is the first component of the Byos Cloud Infrastructure. It is used for centrally managing all deployed Byos µGateway 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 µGateway 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 µGateway detects malicious network activity.
- *Security stack integration* - The edge telemetry data of each deployed µGateway is aggregated centrally in the Management Console. Administrators can integrate an number of existing tools including SIEM, IAM, and Asset Management tools

Secure remote access for asset management



The **Byos Secure Lobby** is the second part of the Byos Cloud Infrastructure that is used for secure remote access to devices on 3rd-party networks, without exposing the host to the internet, and without needing changes to the local network configuration or topology. This allows administrators and technicians to perform service, maintenance, and troubleshooting without needing to be physically on site. Secure Lobby is predominantly used for managing multi-party access to endpoints across multi-site networks. Key features include:

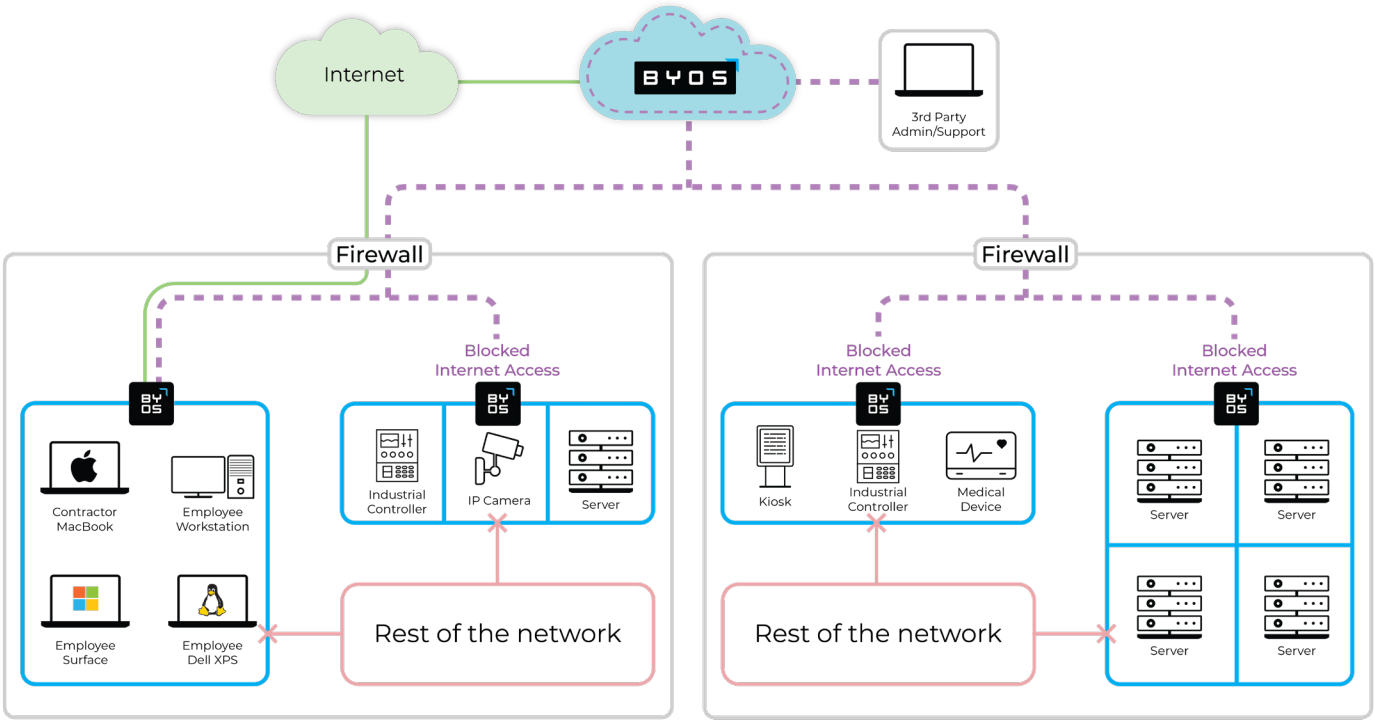
- *Asset Management* - The Byos µGateway can perform a network discovery (IP and Port scans) of all endpoints behind the µGateway, showing endpoint details such as private IP address, MAC, and ports.
- *Private Secure Network* - Endpoints inside of the host that sit behind the µGateway don't need to be exposed to the internet; they can be connected to Secure Lobby and administrators can still have full access to them - this is like a "private cloud". Secure Lobby is also protocol agnostic - any TCP/IP protocol can be used to communicate with the endpoints inside the microsegment
- *Granular Access Control* - There are three levels of access control inside of Secure Lobby: 1) having the Secure Lobby channel turned on/off. and 2) enabling/disabling endpoint visibility inside the Lobby, and 3) as an administrator, having the credentials to access Secure Lobby.

How does edge microsegmentation add value?

Benefits of the Byos solution

- **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.

Deployment Architecture



Byos Secure Edge - The Byos Industrial µGateway can plug into an endpoint directly, or can be connected to a switch, protecting multiple endpoints.

Byos Microsegment - The protected zone created by the µGateway, which the endpoints sit inside, so they remain invisible to fingerprinting, enumeration, or lateral movement attacks on the local network.

Internet Traffic - The µGateway routes clean TLS traffic to the internet for endpoints needing access to resources on the public internet.

Traditional Perimeter - The Byos µGateway device is agentless as nothing needs to be installed on the endpoints and deploys easily without requiring changes to the local network configuration.

Secure Lobby Tunnel - Endpoints connected to a µGateway can have control plane traffic routed through Secure Lobby, to a controlled exit node set by the Administrator, so that Admins and 3rd party support can access these machines, without having access to the entire network.

Blocked Internet Access

Internet access blocked by Byos Policy - Policies can be set by the Admin from the Byos Management Console to block internet access to/from the endpoints inside of a microsegment. However, the µGateway device can still communicate to the Byos MC, and thus Admins remain just one-hop away and can still access the endpoints for efficient incident response.

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

or connect with us at
engage@byos.io

4. For more information about why you should trust Byos, visit byos.io/trust