BYOS

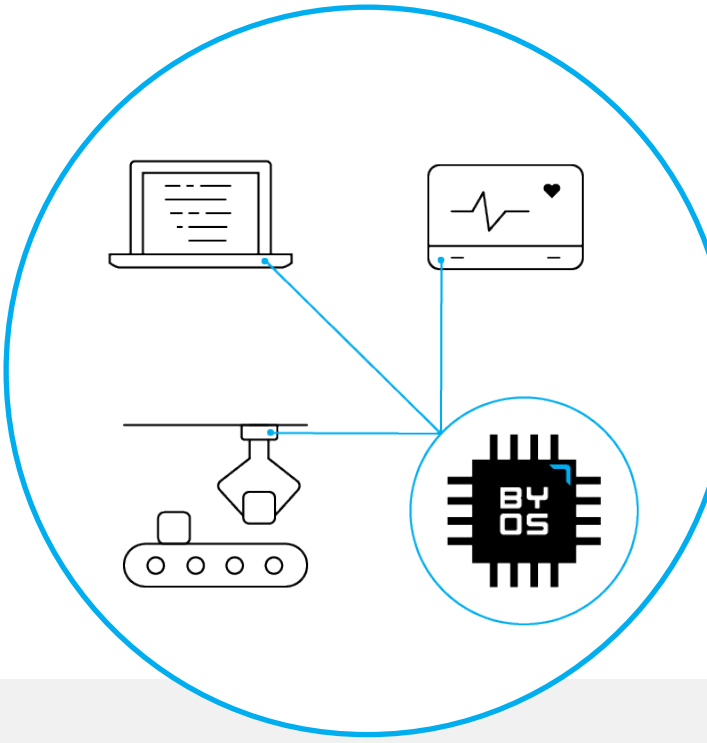
Protecting, Managing, and Accessing IoT Devices through Edge Microsegmentation

Byos Secure Embedded 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]

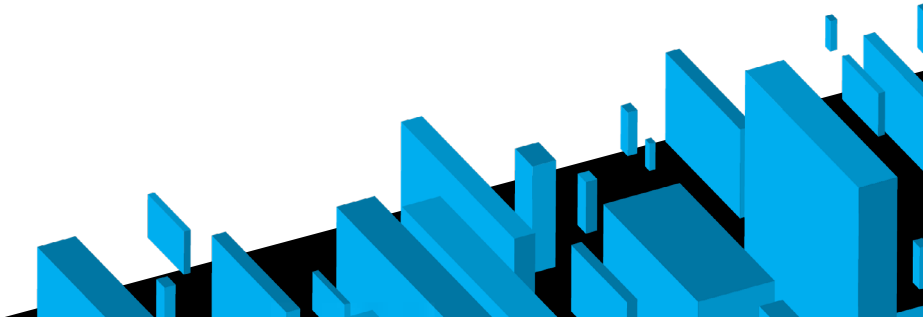
Medium and high security requirement IoT devices like healthcare monitoring devices, intelligent transportation, fleet management, smart grid, etc. are used as an entry point into the larger corporate networks, where the most valuable data resides. Legacy IoT devices such as servers, modems, PLCs, controllers, 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 operating systems can no longer be patched against known vulnerabilities
- Network segmentation strategies for limiting malicious lateral movement are inconsistently applied on today's diverse networks
- Use of deprecated or insecure software components/libraries increases the likelihood of vulnerabilities
- 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 Edge Microsegmentation Solution has three main capabilities, incorporating different components for security, management, and access of IoT devices:

Embedded network security at the edge, independent of the host or the cloud

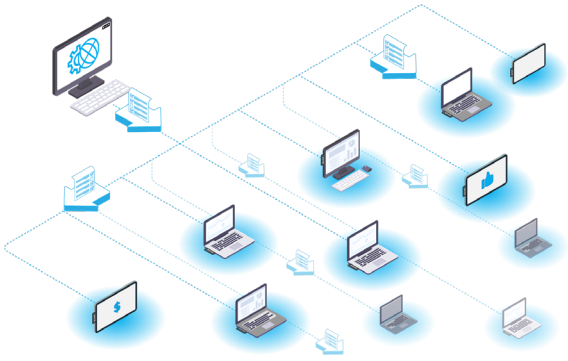
Byos Embedded µGateway™ ("micro gateway") is deployed as a firmware image inside of the host device, on a dedicated microprocessor, at the device's edge, separate from the Host OS. All incoming and outgoing traffic is routed through this core where It provides the Host device with a dedicated network security stack, protecting from OSI layer 1-5, while isolating it from the local network onto its own microsegment.

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' OS nor is delegated to the cloud - all security processing happens in-device for maximum protection against typical attacks that rely on evasion techniques.

Centralized control for security management

The **Byos Management Console** is the first component of the Byos Cloud Infrastructure. It is used for centrally managing all deployed devices that have the Byos µGateway firmware. 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

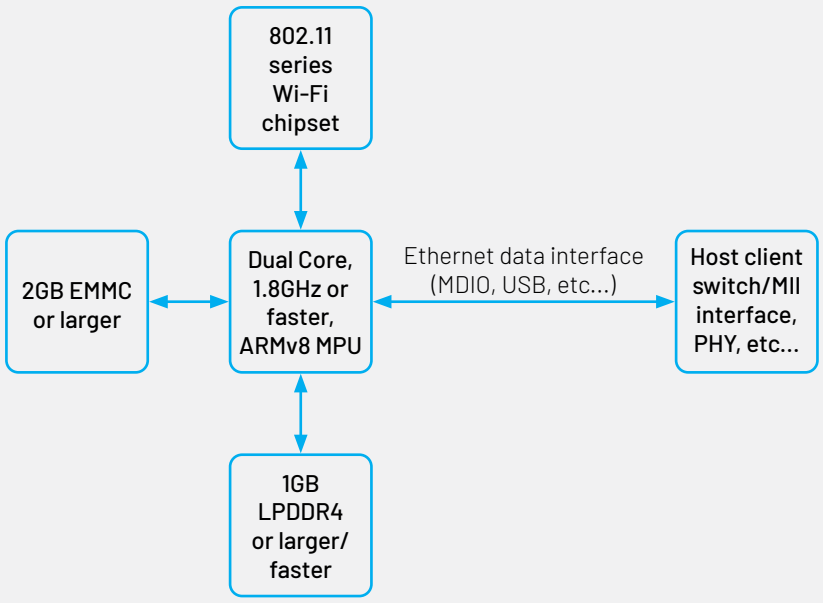
The **Byos Secure Lobby** is the second part of the Byos Cloud Infrastructure that is used for secure remote access to devices on 3rd-party networks, without exposing the host to the internet, and without needing changes to the local network configuration or topology. This allows administrators and technicians 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 Cloud* - 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 is the Byos µGateway Firmware image deployed?

Block Diagram - How to isolate the µGateway from the host OS

The concept of hardware-enforced isolation maintains that all data in and out of the device must first pass through the Byos µGateway before it reaches the device's OS. For this, our embedded firmware must maintain its own microprocessor separate from the main CPU, with the minimum computing requirements that are needed to run embedded linux. Here is the current implementation of how we run the µGateway Firmware on our Hardware:



Specific Functions of Each Block Component:

- **Dual Core 1.8GHz or faster, ARMv8 MPU**
  The MPU processes traffic, hosts a frontend for browser access, provides an API for programmatic or native application access, communicates with the cloud for events and configuration and both manages and executes our security stack. The specific MPU selected by the customer will be dependent on the applications requirements and duty cycles.
- **2GB EMMC or larger**
  Encrypted non-volatile storage of our proprietary source code and configuration.
- **1GB LPDDR4 or better**
  High speed DDR4 allows processes to make extensive use of high speed cached data lookup and avoids unnecessary paging under heavy demand.
- **802.11 series Wi-Fi chipset interface**
  Data transmission to and from the local network happens on this interface. The Byos µGateway Firmware is I/O interface agnostic and works with any TCP/IP traffic. Depending on the data transmission requirements, implementations of the µGateway Firmware can vary, but it will work the same with different network interfaces.
- **Ethernet data interface**
  Data transmission to and from the Host happens on this interface.

Architecture Compatibility

The µGateway Firmware is compatible across multiple architectures including:

- x86_64
- armv7hf
- armv6l
- aarch64

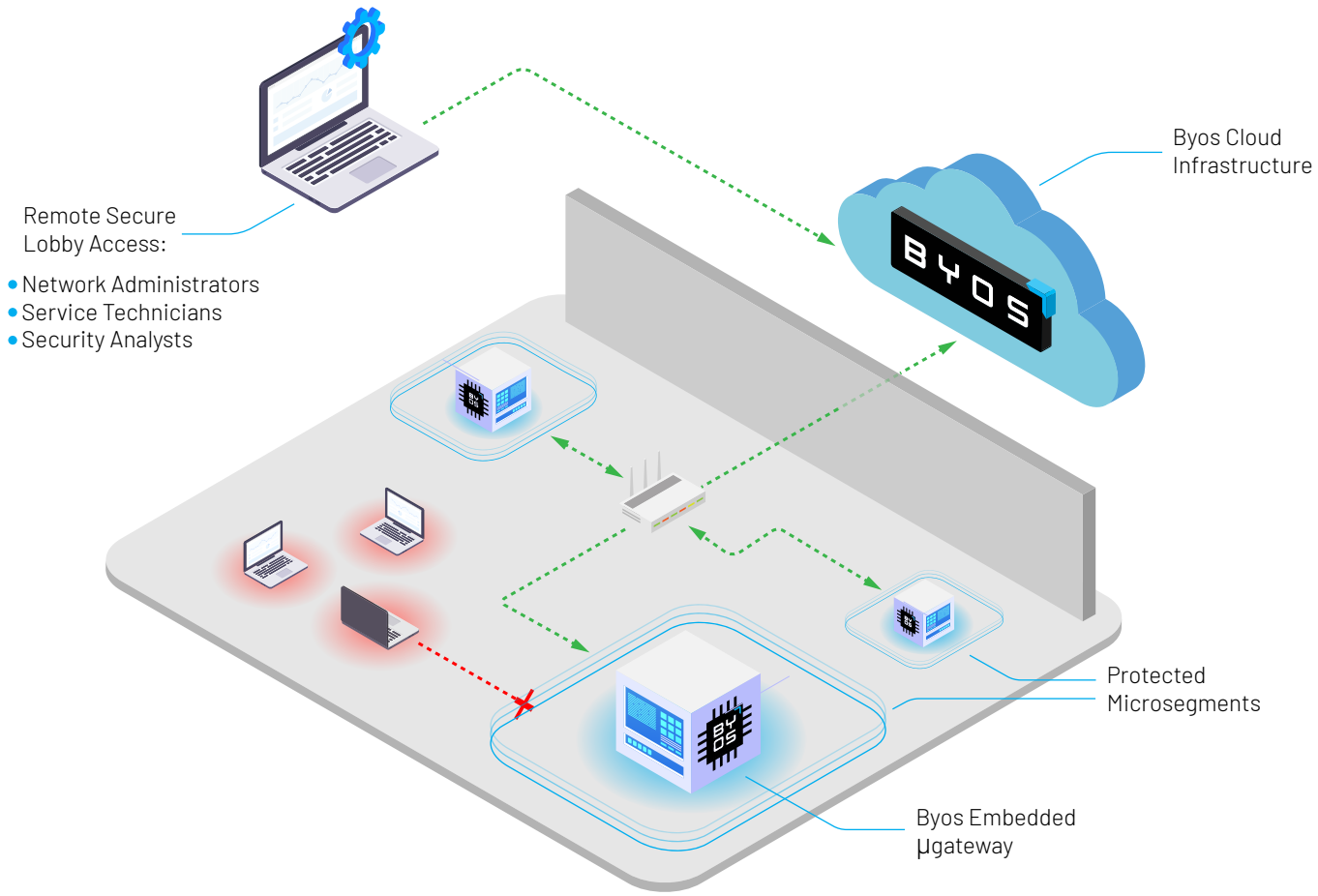
Zero Touch Deployment - µGateways automatically enroll in fleet for immediate security and ease of setup

Developed in North America - Proprietary software that has been developed following secure development best practices and continual testing, recurrent external peer reviews, and active bug bounty program

Improved Security - Multi-layered protection with software security mechanisms across OSI Model layers 1-5

Reduced Attack Surface - has an encrypted filesystem, signed binaries, and secure boot

Reduced Field Service Time - Secure over-the-air updates to both µGateway and host device Firmware and software



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