USE CASE

BYOS

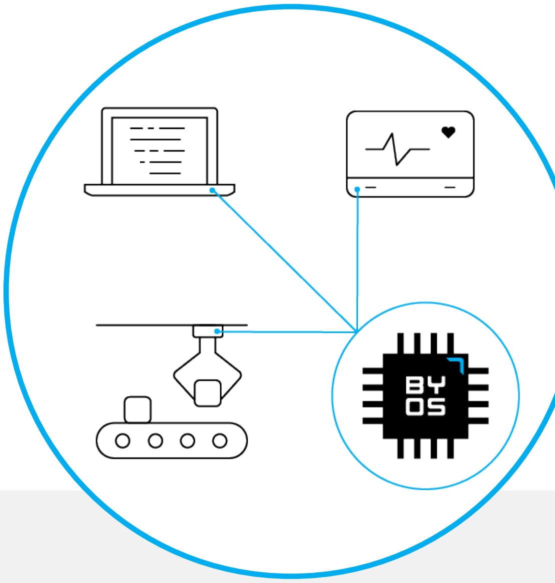
Protecting IoT Devices through Endpoint Micro-Segmentation

Plug-and-Play Security for Legacy and Newly-Designed IoT Devices

As IoT Continues to Grow, So Do System Vulnerabilities

The total number of connected IoT sensors and devices is set to exceed 50 billion by 2022.[1] 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.

IoT devices 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]

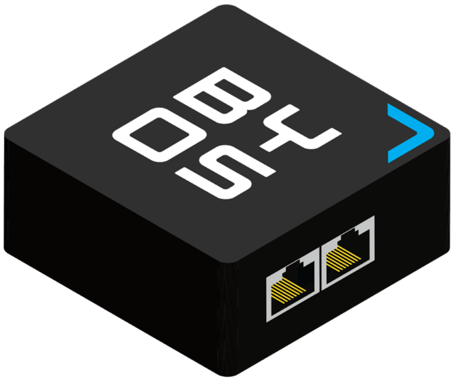
- Legacy operating systems create security risks as unsupported operating systems can no longer be patched against known vulnerabilities
- Network segmentation strategies for limiting malicious lateral movement are inconsistently applied on today's diverse networks
- Use of deprecated or insecure software 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

Byos Endpoint Micro-Segmentation Solution: Trusted and Secure Remote Network Connections for IoT Devices

The Byos™ Endpoint Micro-Segmentation Solution simplifies the protection of each IoT device individually through the Byos µGateway™ and the Byos Management Console. By leveraging endpoint micro-segmentation through hardware-enforced isolation, Byos gives IT and security teams the confidence to protect IoT devices against network threats by minimizing the attack surface and remote code execution exploits.

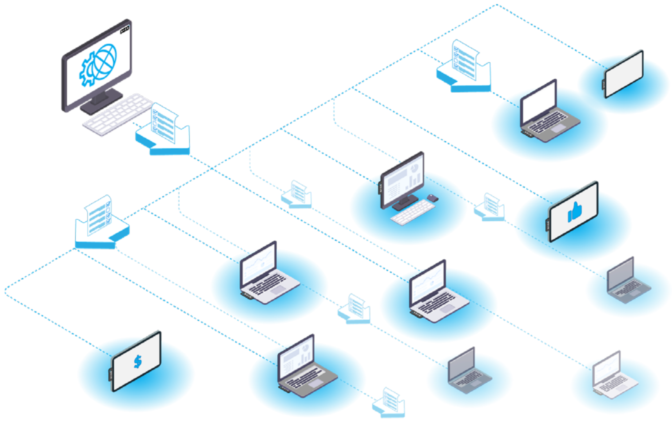
If an alternative attack vector compromises an IoT device, the Byos µGateway provides threat containment within the compromised device, preventing lateral network infections from spreading, and preventing ransomware and Denial-of-Service attacks from rendering devices inoperable.

1. Juniper Research, "IoT – The Internet of Transformation" 2018
2. Deloitte, "How Much Do Organizations Understand the Risk Exposure of IoT Devices?" 2019
3. Forbes, September 2019



Byos µGateway

A plug-and-play, Secure Endpoint Edge, built to provide secure connectivity for IoT devices and legacy infrastructure. The Byos µGateway™ provides protection from OSI layers 1 to 5, isolating the connected endpoint onto its own protected micro-segment of one within the local network.



Byos Cloud Infrastructure

Consists of the 1) Byos Management Console for centralized provisioning and policy pushing, 2) threat intel API for networking logs collected from the fleet of deployed µGateways, and 3) Byos Secure Lobby for secure remote management of µGateway-protected endpoints. It can be self-hosted or multi-tenanted, and can be integrated with existing security environments.

The Byos Endpoint Micro-Segmentation Solution is applicable for protecting entire fleets of IoT devices, including already deployed legacy devices and new IoT devices in development. The µGateway sits between the device it's protecting and the local network gateway.

- For legacy IoT devices, Byos helps to securely prolong the life of legacy IT infrastructure, without needing to alter the legacy endpoint OS nor changing the local network configuration.
- For newly designed IoT devices, the µGateway can be embedded directly to the motherboard for secure networking.

Features & Benefits

Plug-and-play Implementation
TCP/IP compatible so no agent or software installation is required on the host device

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

Reduced Attack Surface
µGateway has a crypto coprocessor, encrypted filesystem, signed binaries, and secure boot

Legacy OS Protection
Technology-agnostic, working with any device regardless of operating system, model, or age

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

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

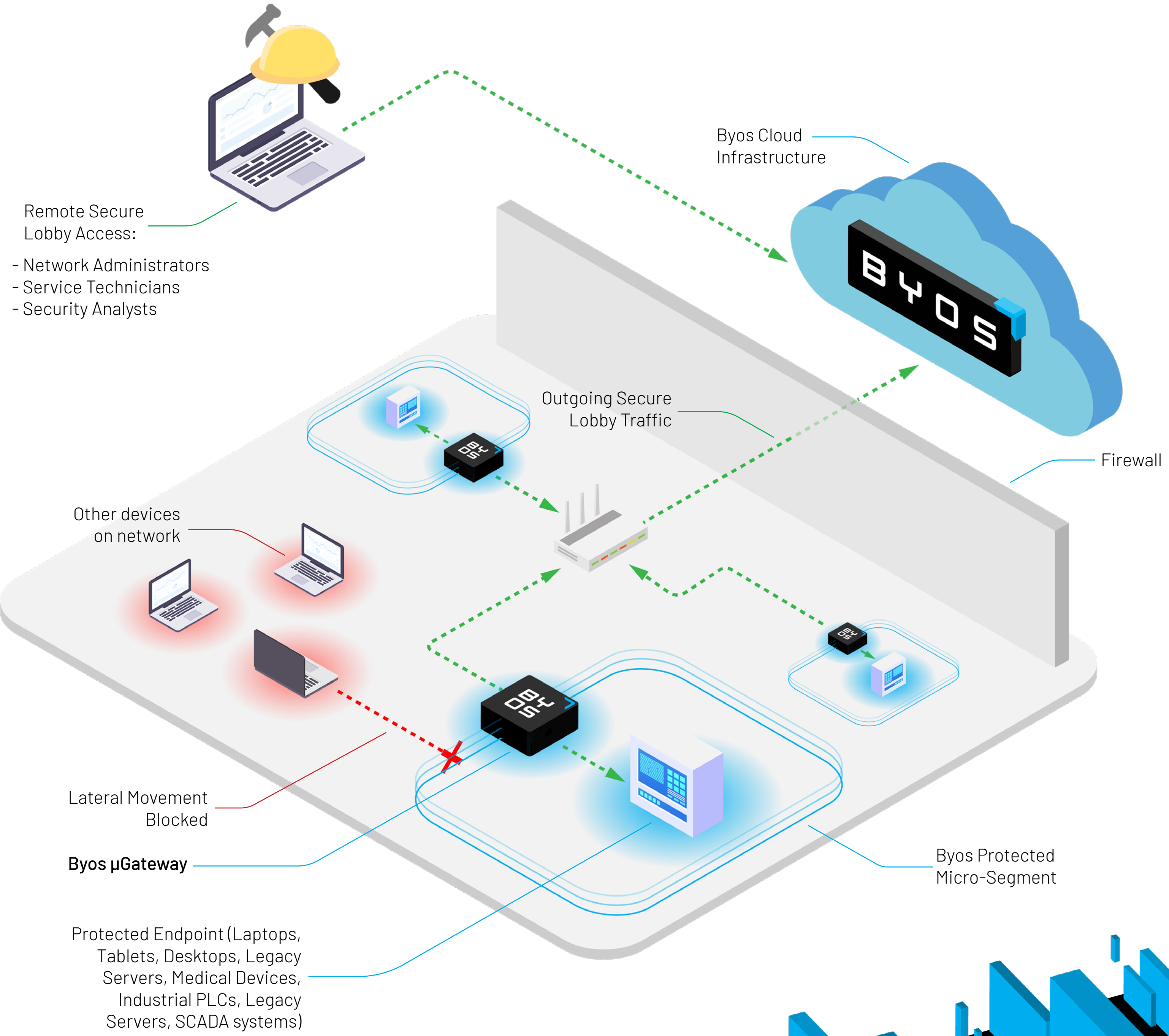
Flexible Implementation
Suitable for both wired and wireless-connected IoT devices - Wi-Fi, Ethernet, Cellular, PCI-E

Built in North America
Proprietary hardware board with a certified supply chain of components to ensure no hidden backdoors or malicious spyware

Key Feature: Byos Secure Lobby

The Secure Lobby feature allows for secure remote access to IoT devices protected by the Byos µGateway. Conventional remote access tools require opening up the perimeter, which adds unnecessary exposure risk to entire corporate networks. The Secure Lobby allows for monitoring, troubleshooting, updating, and patching remotely, without exposing internal endpoints to the internet.

The Secure Lobby creates a secure connection between the µGateway and the Byos Management Console using an outbound connection, originating from inside of the corporate network perimeter, as to not interfere with local network configurations. This saves both Network Administrators and Service Technicians time when servicing Byos-protected endpoints remotely.



Remote Secure Lobby Access:

- Network Administrators
- Service Technicians
- Security Analysts

Byos Cloud Infrastructure

Outgoing Secure Lobby Traffic

Firewall

Other devices on network

Lateral Movement Blocked

Byos µGateway

Byos Protected Micro-Segment

Protected Endpoint (Laptops, Tablets, Desktops, Legacy Servers, Medical Devices, Industrial PLCs, Legacy Servers, SCADA systems)

How the Secure Lobby Works:

1. First, the Network Admin or Service Technician initiates the Secure Lobby connection in the Byos Management Console.
2. Upon receiving the command from the Management Console, the Byos µGateway then establishes an outgoing 4096 RSA-encrypted connection with the Secure Lobby, which is not impacted by the corporate network firewall and does not require weakening the perimeter security of the main network.
3. The user then connects their computer to the Secure Lobby using an encrypted connection.
4. Once the user is inside of the Secure Lobby, the Byos µGateway allows traffic to and from the protected endpoint, allowing the user to interact with the endpoint directly.

Benefits

- Securely prolong the life of IT infrastructure running legacy applications and unsupported OS that are not ready to be retired.
- Connecting previously air-gapped devices to the network for more efficient and secure remote maintenance and monitoring.
- Non-intrusive deployment to existing network configurations, without having to expose internal devices to the internet.
- Eliminated exposure of unpatched legacy networked devices to internal threats like lateral movement and ransomware.
- Reduced technician trips onsite for service and maintenance saving operational expenses.

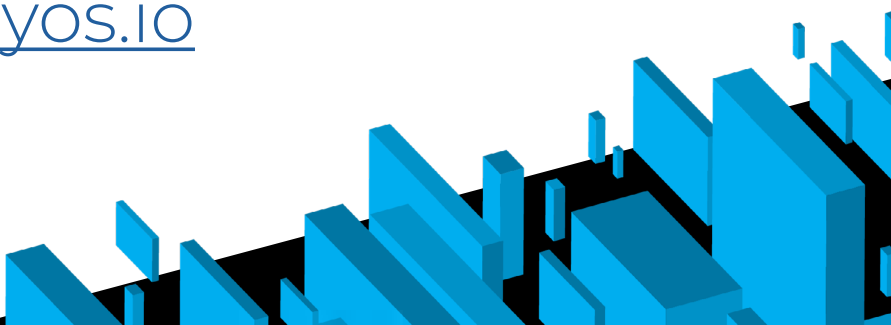
How is Byos µGateway different from standard IoT Gateways?

- The Byos µGateway facilitates secure Remote Monitoring, Updating, Patching, and Troubleshooting through it's Secure Lobby, for improved efficiency without compromising on security.
- Managing IoT gateways is limited, cumbersome, and inefficient. Byos µGateways can be managed centrally, allowing for comprehensive fleet management, simplified policy pushing, provisioning, and threat detection.
- The Byos µGateway provides an entirely independent network security stack on top of providing basic networking functionality.
- The Byos µGateway was built by our team of industry-vetted cybersecurity veterans with security in mind at every stage - secure development and continual testing, recurrent external peer reviews, a certified supply chain of components, and North American manufacturing.[4]

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