BYOS

# Protect Remote Wi-Fi Users with the Byos Secure Endpoint Edge Solution


## Trust every remote network connection, while isolating devices from dirty networks and foreign devices

**The Key Requirements of Secure Connectivity for the Remote Workforce**

To satisfy a modern security team's need to have the proper controls for a completely remote workforce, our *Secure Endpoint Edge* was built to meet five key requirements:

- **Micro-Segmentation:** Endpoints should have zero-trust access to all Wi-Fi networks, while remaining completely cloaked from other devices and threats
- **Secure Roaming:** Security should travel with endpoints and not be static to a particular environment
- **Plug & Play:** Solutions need to support both corporate and BYOD devices quickly and easily
- **Direct Connections:** Traffic should take the shortest distance between two points, with no traffic backhauling, rerouting, or proxies to inhibit connection speeds
- **Cloud Managed:** Administrators should have a control plane for quick (de)provisioning, centralized policy enforcement, and solutions need to integrate with existing security infrastructure (SSO/IAM, SIEM)

### Easily Deploy, Manage, and Secure Every Remote Network Connection

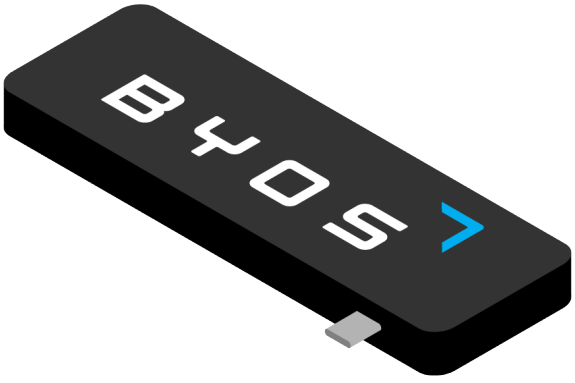
Byos™ simplifies the protection of remote users and devices through the Byos µGateway™ and the Byos Management Console.

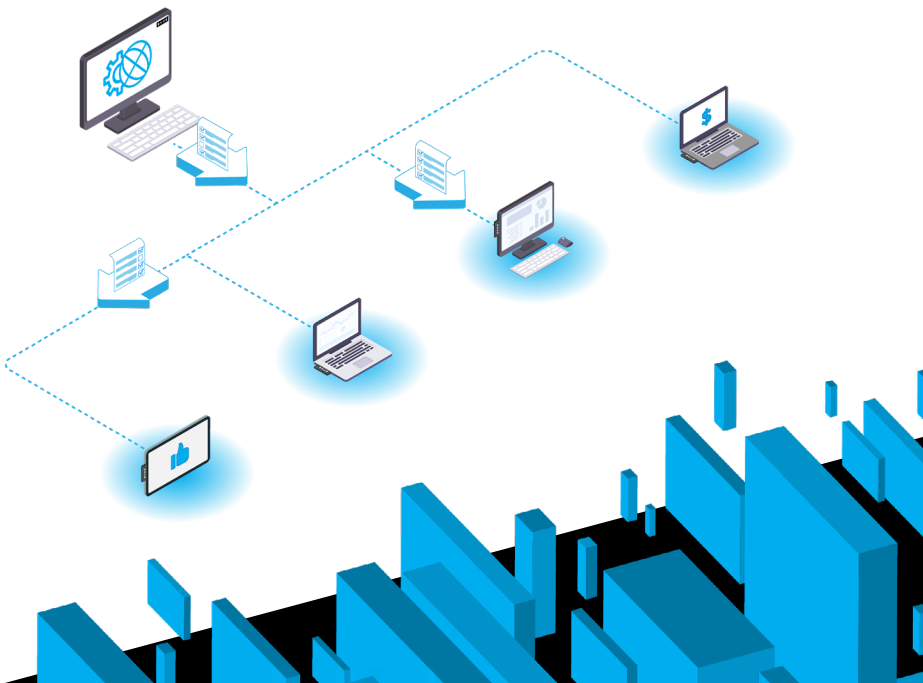
### Byos µGateway

A plug-and-play, USB-based *Secure Endpoint Edge*, built to provide secure connectivity for the remote/roaming workforce and connected devices. 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 Wi-Fi network.

### Byos Management Console

All security policy administration is handled centrally through the Management Console, which allows IT teams to deploy and manage Byos µGateways at scale. With the ability to be self-hosted, cloud-based or multi-tenanted, the Byos Management Console can be integrated with existing security environments and customized to meet specific business needs.

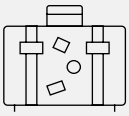


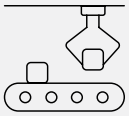
BYOS

## Use Cases & Applications:

Work-From-Home



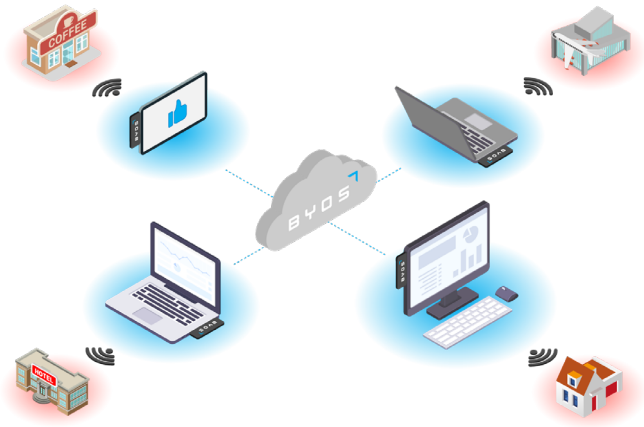
Traveling Employees



IoT Device Protection

BYOD Enforcement

## Extend Zero-Trust Access to any Remote Wi-Fi Connection




With streamlined provisioning for all categories of endpoint devices, Byos enables zero-trust migration and implementation through simple plug-and-play security, including support for:

- Computers, laptops and tablets
- Networked devices such as medical devices, industrial controllers and sensors, payment systems and more

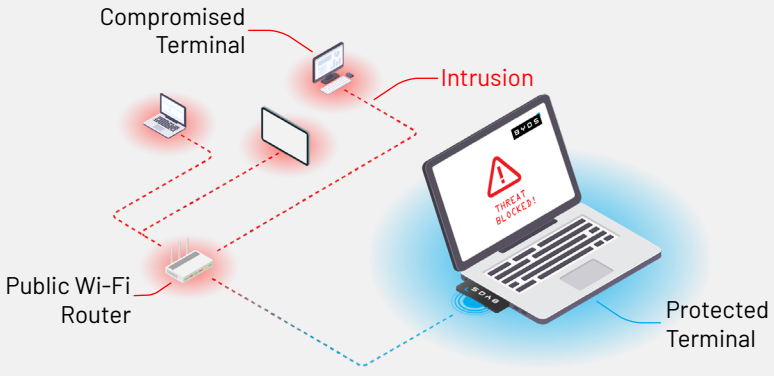
Centralized management gives IT and security teams a simpler, more efficient approach to security policy definition, enforcement, and management for all aspects of device lifecycle management.

The Byos Management Console gives full visibility and control over all remote µGateway network connections with dynamic policy pushing capabilities. At the same time, it supports granular network access control for users and devices, both privileged and non-privileged. And with monitoring and real-time alerting of security incidents, threats can be mitigated before they escalate into business risks.

The increase in remote, on-the-go work environments demands better endpoint protection. The Byos Secure Endpoint Edge improves security through hardware-enforced isolation, giving IT and security teams the confidence to support remote users on any uncontrolled public or home Wi-Fi network.

With the visibility needed to simply deploy and manage at scale, the solution is ideal for organizations that need to deliver more cost-effective security for high risk, high frequency remote workers or networked devices. From healthcare and high tech to financial services and government, with Byos, users are safe to connect and free to work.

## Safe to Connect, Free to Work.




# To get a Business Starter 5-Pack today, visit:

byos.io/get-started