BYOS

Protect Remote Wi-Fi Users with Byos Endpoint Micro-Segmentation Solution

Remote Access Brings Security Gaps, Business Risks and IT Challenges

Remote access to the corporate network is vital for today's dispersed, always-on workforce. Remote devices create challenges for IT and security admins. Endpoints are targets – and opportunities – for malicious attackers who take advantage of uncontrollable dirty networks that lack the security measures needed to ensure that corporate resources are protected.

As a result, devices are exposed to the risks inherent to the local Wi-Fi network, creating a gap in protection for every remote device. Traditional protection solutions are complex for IT to manage and cumbersome for users. VPNs were not built to protect the endpoint from local W-Fi network threats and leave endpoints exposed, while manually segmenting home Wi-Fi networks to protect work from home is expensive, complex for users, and difficult to audit and enforce.

As CISOs adapt policies and operations to reflect this risk, they are prioritizing the security of remote users and devices. They need to secure and protect remote users quickly and at scale, preferably with a plug-and-play solution that minimizes the need for IT resources and simplifies ongoing management.

Easily Deploy, Manage, and Secure Every Remote Network Connection

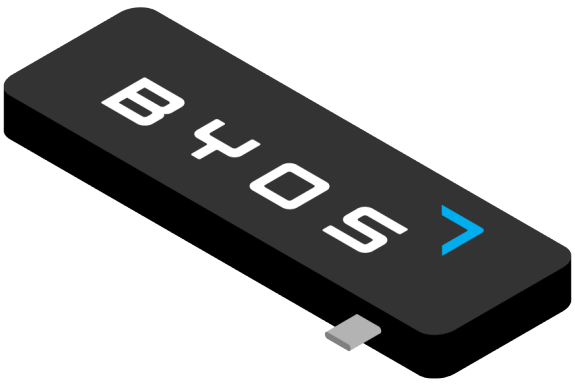
The Byos™ Endpoint Micro-Segmentation Solution simplifies the protection of remote users and devices through the Byos µGateway™ and the Byos Management Console. By leveraging endpoint micro-segmentation, Byos eliminates the need for costly travel device programs, complex home security protocols, and the cellular data expenses incurred when managing remote device security.

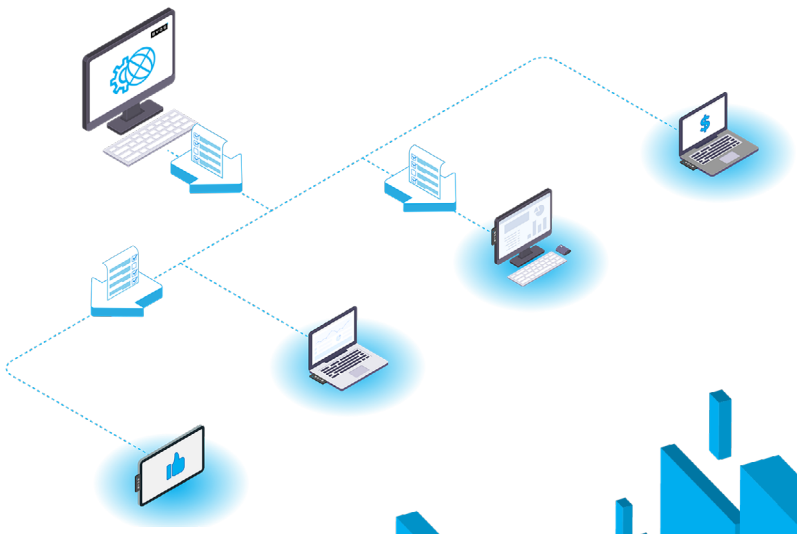
Byos µGateway

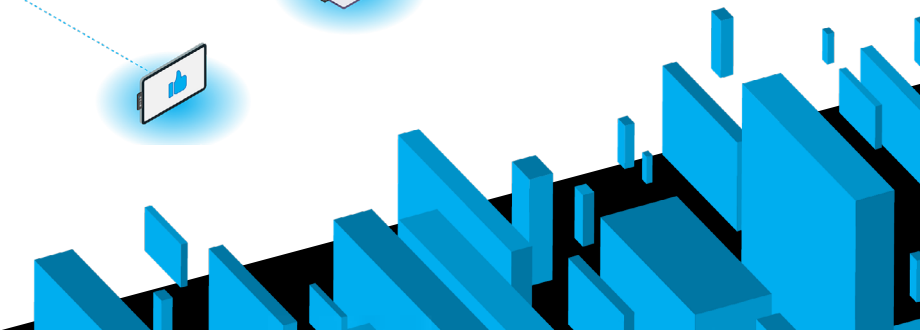
A hardened security stack on a simple plug-and-play USB device, the Byos µGateway provides protection from OSI layers 1 to 5 through hardware-enforced isolation. Each Byos µGateway isolates the connected endpoint onto its own *micro-segment of one* that protects it from compromised networks and other compromised endpoints on the 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.



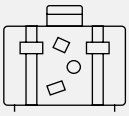




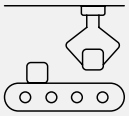
BYOS

Use Cases & Applications:

Work-From-Home



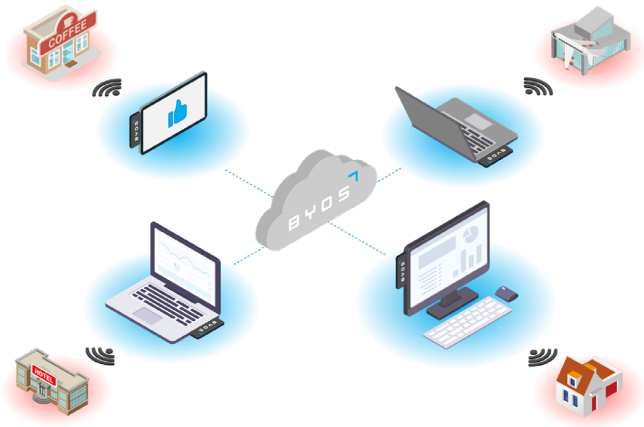
Traveling Employees



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

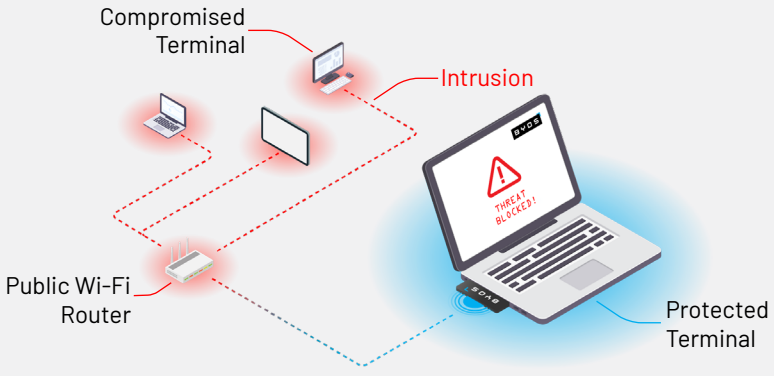
Centralized management gives IT and security teams a simpler, more efficient approach to security policy definition, enforcement, and management for all aspects of device lifecycle management.

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 Endpoint Micro-Segmentation Solution 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