BYOS

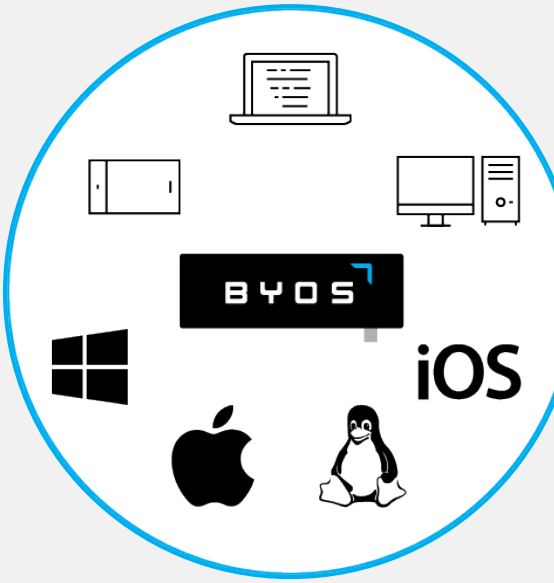
BYOD Enforcement

Extend Zero Trust Access to Unmanaged Devices on Corporate Networks

BYOD Access to Wi-Fi Brings Increased Security Risks

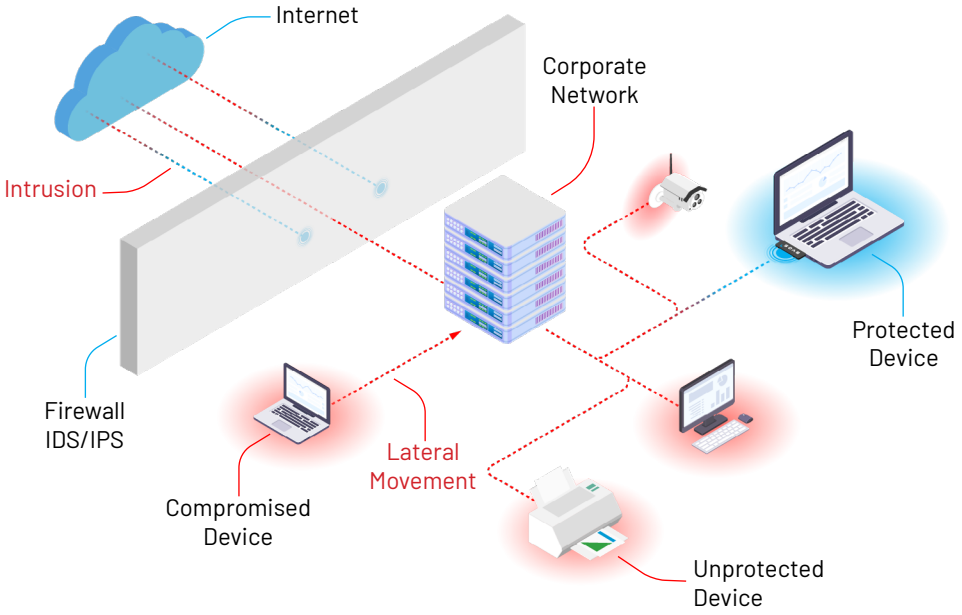
A daily influx of on-site visitors, contractors and external vendors is a reality for today's dynamic business – and so is the need for these visitors to have access to the Internet. Whether it's a vendor who needs to log-in to an ordering system, a contractor fulfilling the needs of a project or a guest who wants to check email, third-party, unmanaged devices on your network bring new and lucrative attack opportunities. Exposing mission-critical trade secrets, intellectual property, customer data, industrial control system data, or private health records costs organizations both financially and reputationally.

Recent high-profile data breaches have put companies in an unwelcome spotlight, highlighting security failures and the resulting financial costs, reputational damage and need for a zero-trust security solution. Unfortunately, preventing vendors and contractors from connecting with their own devices is too restrictive for today's working environments. Often, in an effort to prevent intrusions and information leakage, security postures include a guest Wi-Fi network, segmenting them from the internal network and providing crucial protection of an organization's data. However, a guest network alone isn't enough protection in today's cyber landscape.



Exposed Third-Party Devices are Not Isolated from Internal Corporate Resources

Organizations that offer guest Wi-Fi are vulnerable to a variety of tactics attackers use to gain access to internal devices and resources:



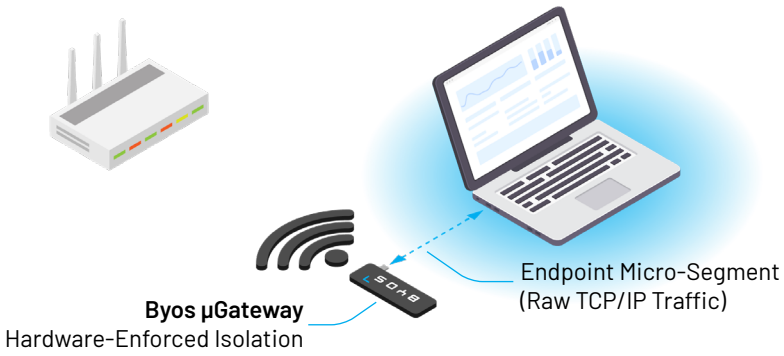
- Man-in-the-Middle
- DNS Hijacking
- Evil-Twin Wi-Fi
- Packet Rerouting
- Eavesdropping
- Scanning and Enumeration
- Fingerprinting and Exploiting
- Lateral Network Infections
- Rogue VPN

An ideal guest access solution will protect an organization's internal corporate network by isolating each unmanaged device onto their own *micro-segment of one*.

Byos Endpoint Micro-Segmentation Solution

Trusted and Secure Remote Network Connections for BYOD Environments

The Byos™ Endpoint Micro-Segmentation Solution simplifies the protection of remote users and devices through Byos µGateways and the Byos Management Console. By leveraging endpoint micro-segmentation, Byos adds a layer of protection between the visitor and the rest of the network, without adding substantial internal networking infrastructure.

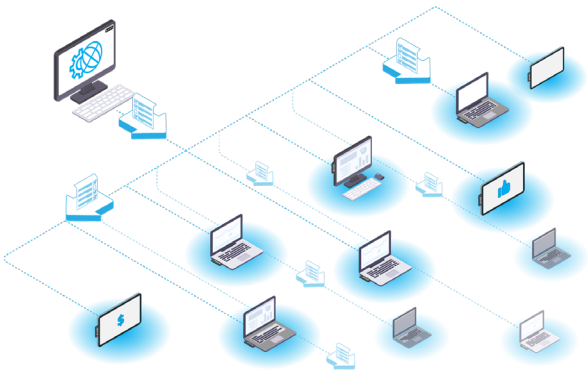


Byos µGateway

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.



Streamlined provisioning and centralized management give IT and security teams a simpler, more efficient approach to security policy definition, enforcement, and management for all aspects of device lifecycle management. Administrators simply issue a µGateway to visitors when they want to connect to the guest network. The plug-and-play nature of the solution allows visitors to plug the µGateway into their devices and securely connect under the control of the network administrator.

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.

To get your Business Starter 5-Pack today, visit:

byos.io/get-started