BYOS

Work-From-Home Users

Extend Zero Trust Access to Remote Wi-Fi Connections

The Rise in Work-From-Home Users

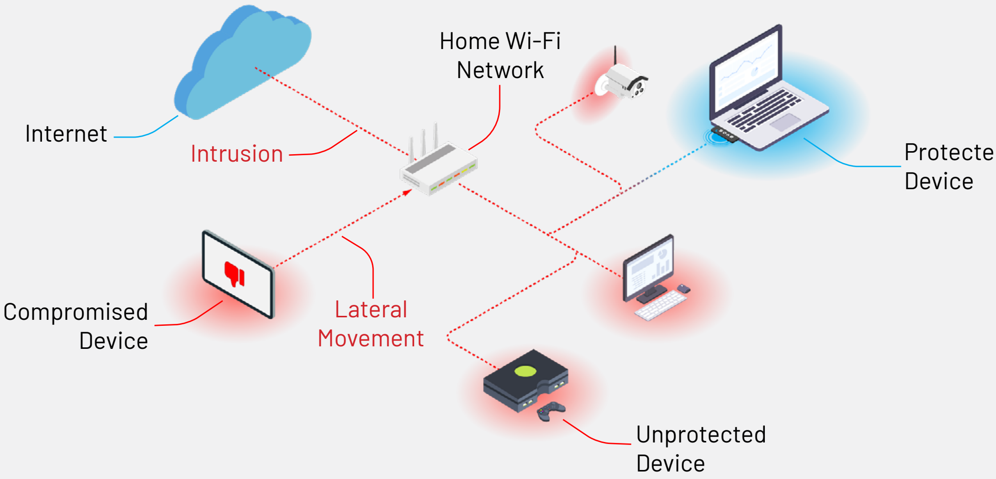
Work-from-home policies have long been an emerging and accelerating trend in the workplace. Reasons for this range from the ability to attract and retain talent, to business continuity when adapting to unpredictable situations, to supporting new types of gig and contingent workforces.

Add in the proliferation of remote work-friendly collaboration tools like Slack and Zoom, and this trend is expected to continue into both the near and foreseeable future.

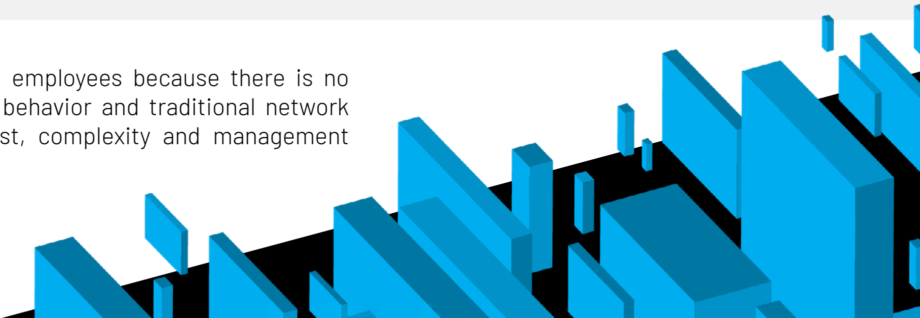
Improved Business Flexibility Brings Increased Security Risks

Attacks on employees working from home are increasing as attackers adjust tactics to this new reality.

- Employees working from home don't have the same firewalls, network-based intrusion detection systems, and other defenses they have in the office. Organizations, therefore, have no visibility into the network traffic that exists on a home Wi-Fi and cannot trust these networks.
- Once an attacker or malware gets into a device, they often go undetected and can seize or manipulate data with the ultimate goal of moving from a single remote device into the big prize: the company network of servers.
- A shared home network can mean there are unmanaged devices in the hands of children, teens and other adults. These tablets, cellphones, home IoT devices, and gaming consoles increase the attack surface and the risk.



IT teams are challenged to support work-from-home employees because there is no effective or scalable way to track or enforce secure behavior and traditional network segmentation techniques are impractical due to cost, complexity and management inefficiency.

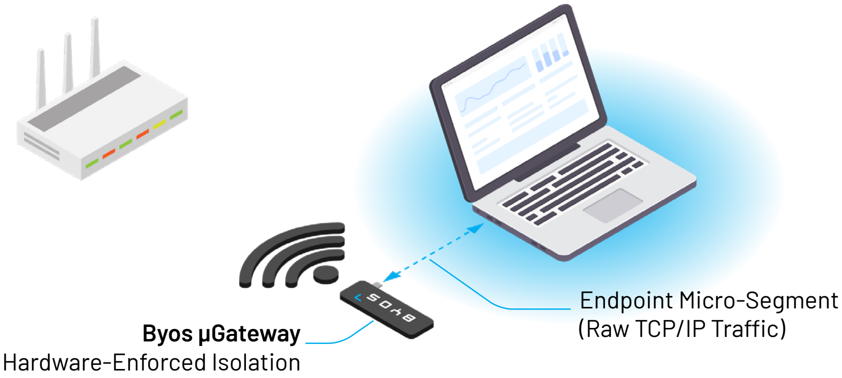


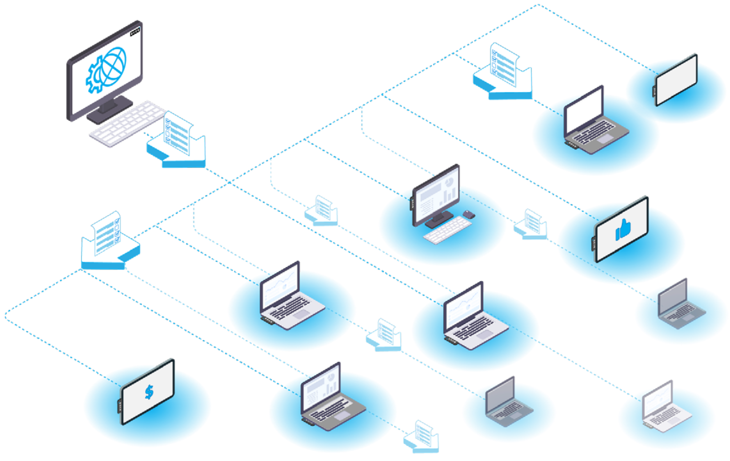
Byos Endpoint Micro-Segmentation Solution: Trusted and Secure Remote Network Connections for Work-from-home Users

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 through hardware-enforced isolation, Byos gives IT and security teams the confidence to support work-from-home users on any uncontrolled home Wi-Fi network.

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 for hardware-enforced isolation. Each Byos µGateway isolates the connected endpoint onto its own *micro-segment of one* that protects endpoints from compromised networks and networks from compromised endpoints.





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. 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 a Business Starter 5-Pack today, visit:

byos.io/get-started