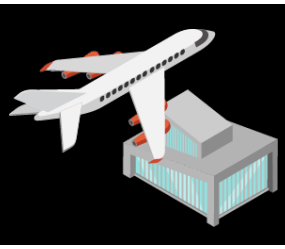
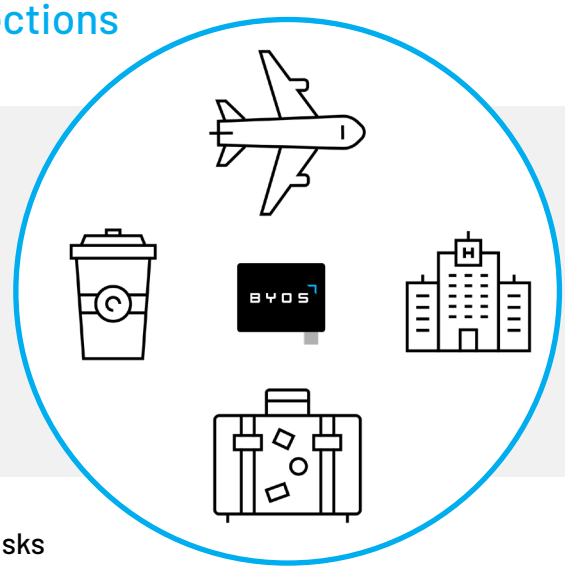
BYOS

Protect Traveling Employees



Extend Zero Trust Access to Remote Wi-Fi Connections



Remote Access is a Must-Have for Today's Travelling Professionals

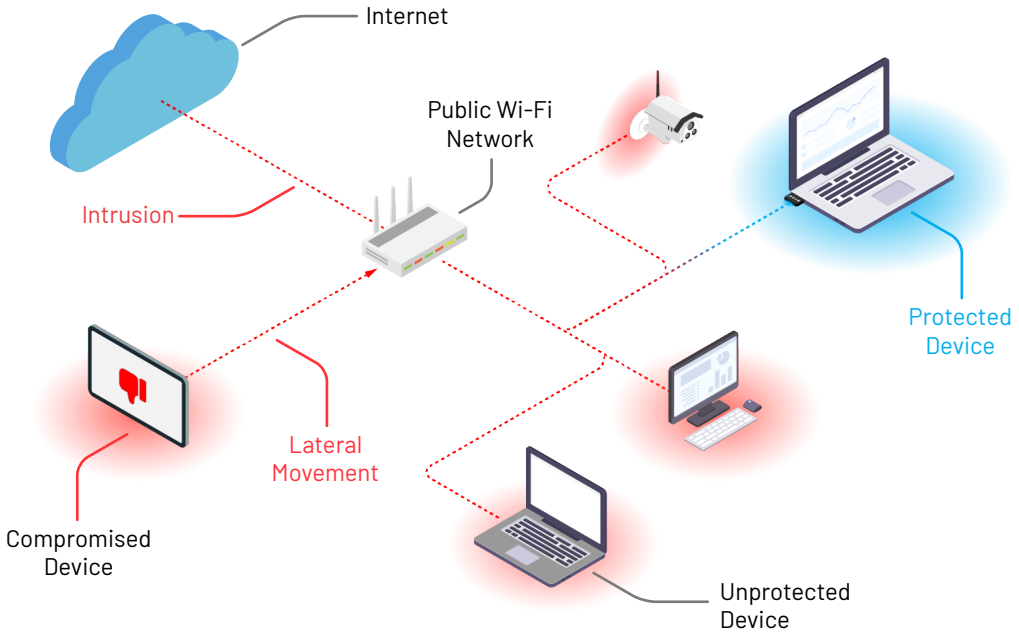
Traveling is a necessity for conducting business. Connecting to Public Wi-Fi represents convenience for users, but represents risk for IT security teams.

Users are connecting a multitude of devices to insecure networks in cafés, hotels and airports all over the world, and security teams have little control over the security of their Internet connections. While public Wi-Fi is essential to today's business traveler, it also creates a massive security risk.

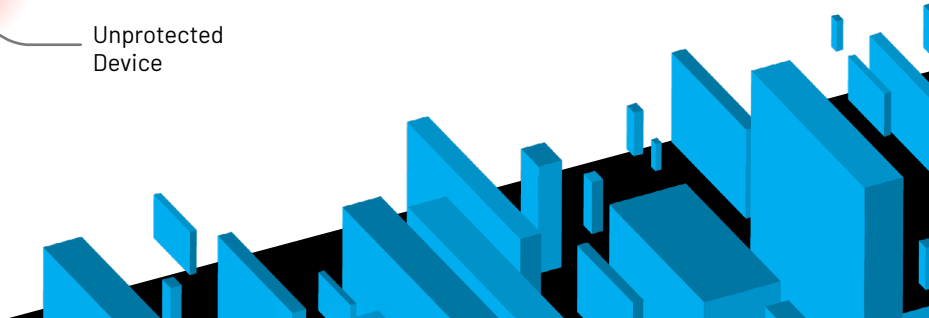
Traveling Employees Accessing Public Wi-Fi Bring Increased Security Risks

The rise in free, public Wi-Fi has been a tremendous boon for traveling professionals – and hackers. Malicious attackers take advantage of uncontrollable dirty networks that lack the security measures needed to ensure that endpoints are protected.

As a result, devices are exposed to the risks inherent to the local Wi-Fi network. This creates a gap in protection for every remote device - a problem that grows exponentially as the number increases. Travelers who rely on public Wi-Fi are vulnerable to a variety of tactics attackers use to gain access to devices and resources:



- Man-in-the-middle
- DNS Hijacking
- Packet Rerouting
- Eavesdropping
- Scanning and Enumeration
- Fingerprinting and Exploiting
- Lateral Network Infections
- Rogue VPN

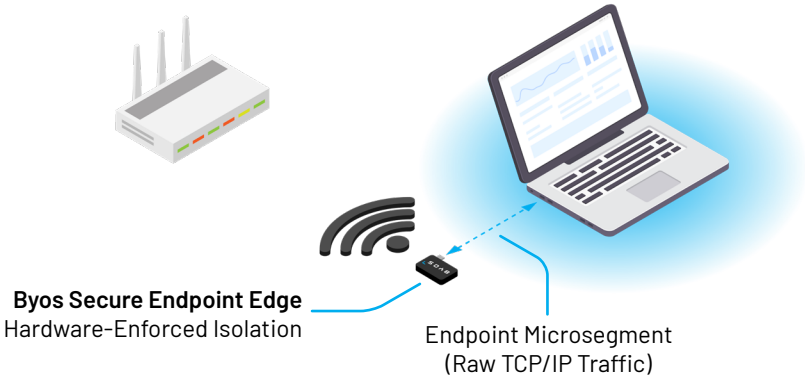


1. Skift, "The State of Business Travel 2020."

Solutions such as VPNs only encrypt data in transit and don't isolate the device from the Wi-Fi 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. IT teams are challenged to support traveling users because there is no effective or scalable way to track or enforce secure behavior.

Byos Edge Microsegmentation Solution: Trusted and Secure Network Connections for Business Travelers

The Byos™ Edge Microsegmentation Solution simplifies the protection of remote users and devices through Byos Secure Endpoint Edge and the Byos Management Console. By leveraging Edge Microsegmentation, Byos eliminates the need for complex home security protocols, the cellular data expenses incurred for remote device connections, and costly travel loaner device programs.

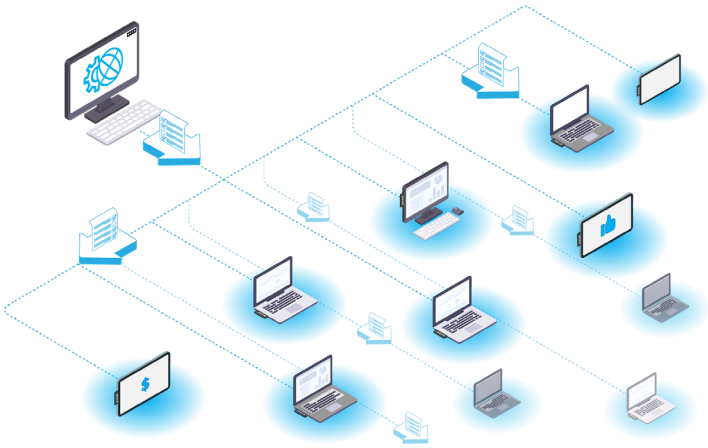


Byos Secure Endpoint Edge

A hardened security stack on a simple plug-and-play USB-C device, the Byos Secure Endpoint Edge provides protection from OSI layers 1 to 5 through hardware-enforced isolation. Each Byos Secure Endpoint Edge isolates the connected endpoint onto its own microsegment 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 Secure Endpoint Edge 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 Secure Endpoint Edge 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.

If you'd like to learn more about Byos, visit us at byos.io

or connect with us at
engage@byos.io