BYOS

Protect a Distributed Workforce with the Byos Secure Endpoint Edge Solution

Protect, manage, and control remote workers through microsegmentation for High Assurance Network Access

Devices connecting to unmanaged networks like public and home Wi-Fi expands the sprawling attack surface.

- Endpoints are visible and discoverable on Wi-Fi networks, and vulnerable to lateral movement
- Security/GRC teams can't enforce geographic data governance compliance for employees who travel outside of regulated regions
- IT Security teams can't enforce or control access of corporate resources from 3rd-party, unmanaged devices of contractors, and remote employees
- Software & DevOps teams can't efficiently and securely collaborate P2P while using the public internet

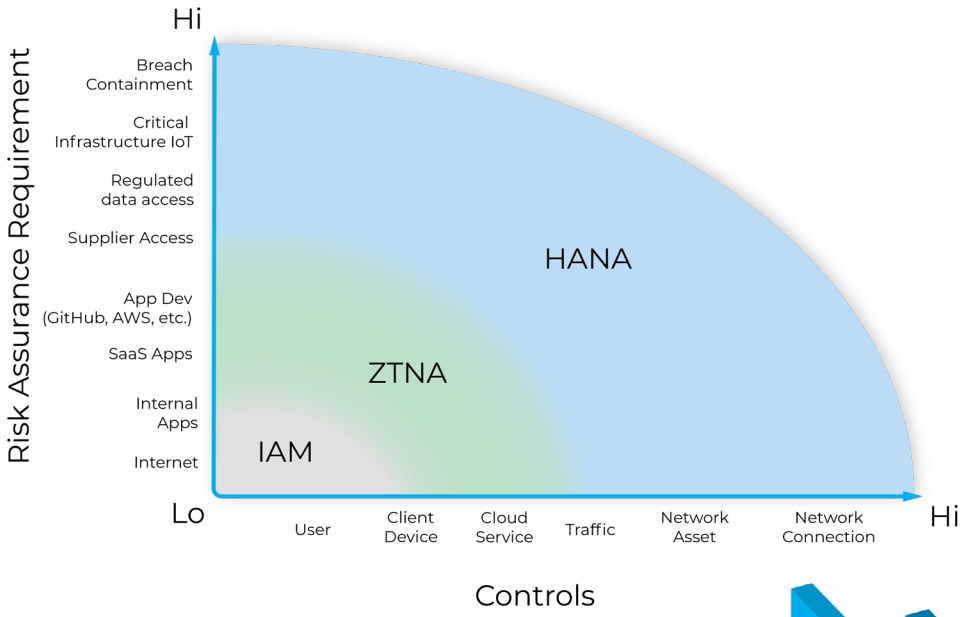
What is High Assurance Network Access (HANA)?

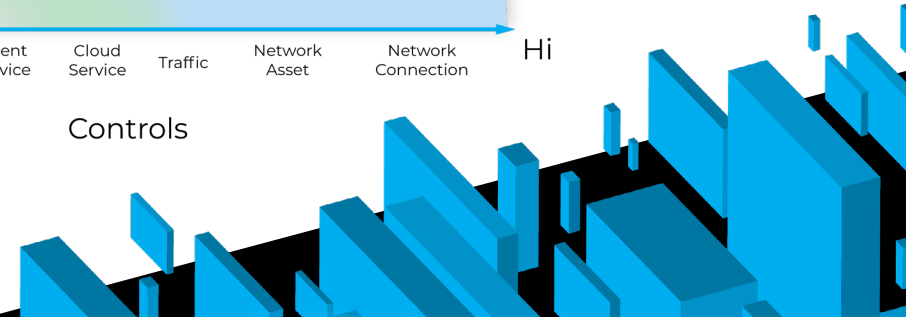
High Assurance Network Access (HANA) asserts that the most critical or risky actions taken inside of a network, should be managed using the strongest control mechanisms.

Basic access operations within today's networks are sufficiently secured by existing IAM and ZTNA technologies. As an example, managing access to a cloud-based SaaS app (action) using a cloud service (control mechanism) is one covered by existing ZTNA solutions.

However, when you have actions like containing a breach (disconnecting endpoints) or accessing critical infrastructure IoT devices remotely, ZTNA doesn't provide enough coverage over the control mechanisms. This is where HANA fills the gap - Providing high assurance security and management of the networking assets and their network connections through microsegmentation.

HANA complements existing IAM and ZTNA strategies by filling in the gap of protection for devices that connect to Wi-Fi networks.





What does the Byos microsegmentation solution offer?

The Byos Secure Endpoint Edge Solution has three main capabilities, incorporating different components for security, management, and access of distributed workforces using public Wi-Fi networks:

Plug-and-play network security at the edge, independent of the host or the cloud

Byos Secure Endpoint Edge™ - is a small plug-and-play hardware edge device that provides the "first hop" protection when connecting to an unmanaged network (public or home Wi-Fi). It provides microsegmentation and route enforcement by replacing the endpoint's native Wi-Fi, protecting across OSI layers 1-5 by becoming the gateway.

It provides the connected endpoint with true isolation from the rest of the network, and fills the gap left by security software by being the ingress/egress point for all internet traffic and not being susceptible to bypass and stealth attacks originating inside the endpoint's OS.

Use cases & applications

The Byos Secure Endpoint Edge is used with laptops and tablets and is used for:

- Isolating employee laptops from home and public Wi-Fi networks
- Protecting and managing 3rd-party contractor devices that connect from unmanaged networks
- Ensuring all traffic and data originating from endpoints on unmanaged networks flows through controlled exit nodes

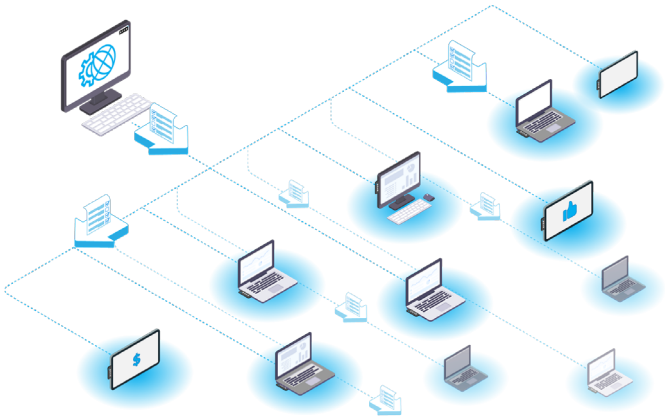
Byos Secure Endpoint Edge Technical Specifications:

- **Dimensions:** 1.76 x 1.38 x 0.57 in. (4.48 x 3.49 x 1.45 cm)
- **Type of Device:** Plug-and-Play USB Ethernet Gateway
- **Power Consumption:** Under 2W
- **Connector:** USB-C 2.0 (Compatible w/USB-A adapters)
- **OS Requirements:** Any OS compatible with USB-OTG
- **Special Driver Requirements:** None
- **Manufactured in:** Canada/USA
- **Certified Supply Chain of Hardware components:** Yes
- **Certified Chain of Custody of Software:** Yes
- **Software Updates:** Automatic, Over-the-air

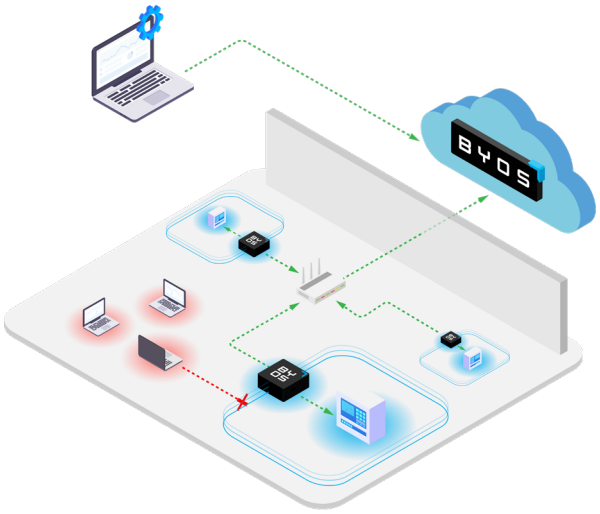
Centralized control for security management and monitoring

The **Byos Management Console (MC)** is the first component of the Byos Cloud Infrastructure. It is a cloud-based control plane used for centrally managing all deployed Byos Secure Endpoint Edge devices, allowing for efficient control, rapid incident response and breach containment. Key features include:

- *Security policy provisioning* - Administrators can provision devices into different "groups" based on their specific characteristics, and can apply granular security policies to those groups at the click of a button.
- *Threat management* - The Byos Secure Endpoint Edge collects threat signals and reports them back to the Management Console, and allows the administrator to have a view into the overall security posture of the fleet. Administrators can enable the Ransomware killswitch, which will automatically isolate the device from the internet when the Secure Endpoint Edge detects malicious network activity.
- *Security stack integration* - The edge telemetry data of each deployed Secure Endpoint Edge is aggregated centrally in the management console. Administrators can integrate a number of existing tools including SIEM, IAM, and Asset Management tools.

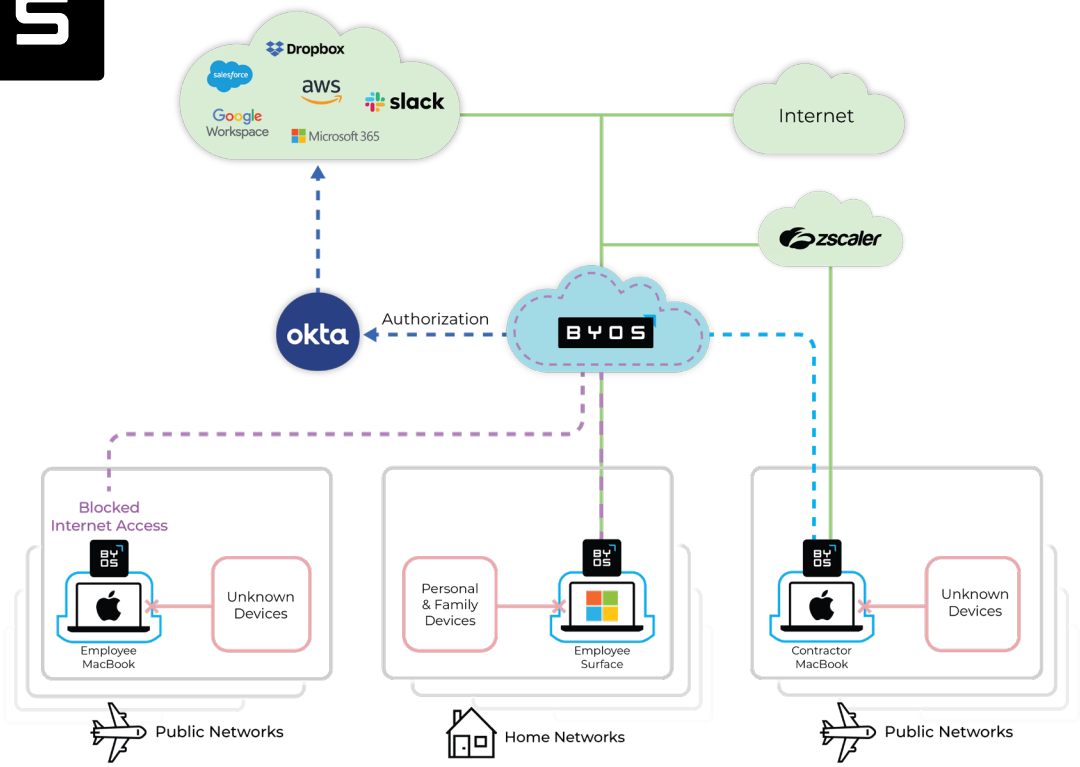


Secure networking for hostile networks



The **Byos Secure Lobby™ (SL)** is the second part of the Byos Cloud Infrastructure that is used for secure networking, regardless of the Wi-Fi network's location or configuration. Secure Lobby gives administrators maximum control over their microsegment's traffic for maximum obfuscation and anonymity. Key features include:

- *Fully encrypted and anonymized traffic* - Administrators have the option to route all traffic through Secure Lobby (both Byos control plane traffic and the endpoint's Internet traffic).
- *Zero public internet packet leakage* - Admins also have the option to auto-connect to Secure Lobby on boot, so not a single packet is sent or received until the connection is established.
- *Direct inter-microsegment routing* - Byos microsegments inside of Secure Lobby are one hop away from each other so that users can communicate efficiently on the Byos network without exposure to the other devices on the local network or the public internet.



Byos Secure Edge - The Byos Secure Endpoint Edge device performs all networking on behalf of the endpoint (performs NAT, has its own DHCP, encrypted DNS server, proprietary network security stack), thus replacing the endpoint's native Wi-Fi.

Byos Microsegment - The protected zone created by the Secure Endpoint Edge, which the endpoint sits inside, so that it remains invisible to fingerprinting, enumeration, or discovery attacks on the local network.

Internet Traffic - The Secure Endpoint Edge routes clean TLS traffic to the internet, and can be routed to an organization's existing cloud security solutions.

Traditional Perimeter - The Byos Secure Endpoint Edge device is agentless as nothing needs to be installed on the endpoint and deploys easily without requiring changes to the local network configuration.

Byos-leveraged IAM - Byos integrates with identity solutions so the Secure Endpoint Edge can act as an authorization signal - eg. "John Doe is using his Byos Secure Endpoint Edge, therefore he can access Github".

Secure Lobby Tunnel without Internet Access - Policies can be set by the Admin from the Byos Management Console to block internet access to/from the endpoint. However, this endpoint can still communicate to other Secure Endpoint Edge also connected to Secure Lobby.

Secure Lobby Tunnel with Internet - Endpoints using a Secure Endpoint Edge can have all internet traffic routed through Secure Lobby, to a controlled exit node set by the Administrator, so that no packet touches public servers before reaching the internet.

Byos control plane traffic - Constant pull beacons from the Secure Endpoint Edge to the Byos Management Console for centralized command and control.

Safe to Connect, Free to Work.

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.

Get Started

Get your Business Starter 5-pack today: byos.io/get-started

or connect with us at engage@byos.io