BYOS

µGateway Technical Overview

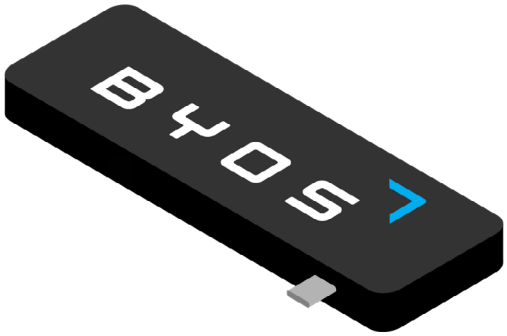
Plug-and-Play Protection through Hardware-enforced Isolation

Extend Zero-Trust Access to Any Remote Wi-Fi Connection

Easily deployed, provisioned and managed, the Byos™ Endpoint Micro-Segmentation Solution simplifies remote user and device protection through Byos µGateways and the Byos Management Console.

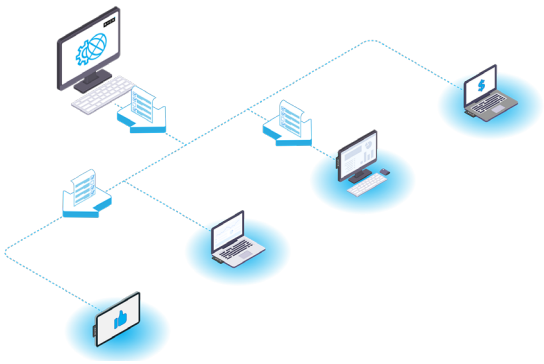
Byos µGateway

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.



Robust Endpoint Protection

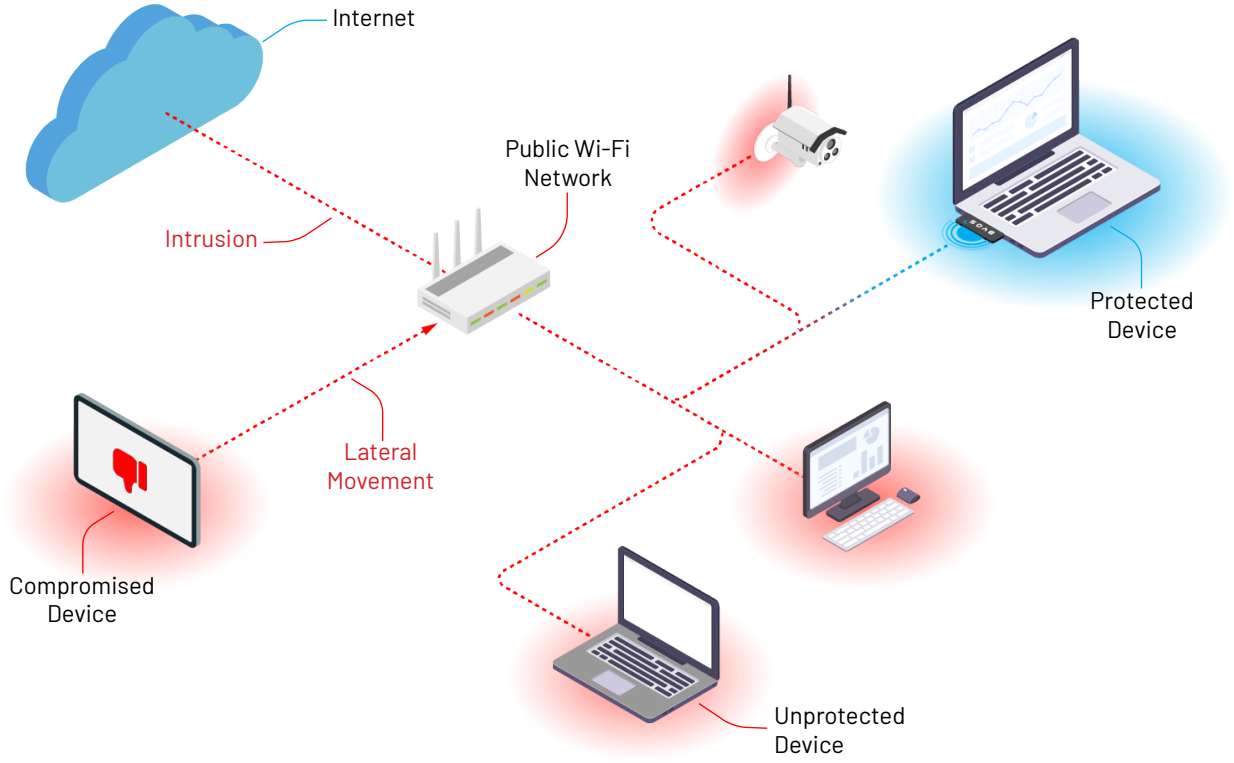
Hardware-enforced isolation created by the Byos µGateway hardware device puts the user in a protected environment isolated from the local network. Because the µGateway is a "security stack on a stick," all security service processing occurs on its hardware with no protection dependencies in the cloud. The specific security services running on the µGateway include:

- **Controlled access**
  Byos runs a bi-directional firewall, offering incoming and outgoing access control based on country-based and protocol-based traffic, restricting specific domain names, IP addresses and ports.
- **Wi-Fi protection**
  The user's Wi-Fi connection is prevented from being intercepted, cloned, bypassed or hijacked.
- **Eavesdropping prevention**
  The µGateway maintains direct and confidential communications with the network gateway without allowing the poisoning of routing tables.
- **Private DNS queries**
  The µGateway runs an in-device encrypted DNS server to prevent DNS hijacking and preserve the confidentiality of the user's browsing data.
- **Infiltration prevention**
  The µGateway detects changes in packet routing to the Internet and takes the necessary actions to prevent any data leakage.
- **Traffic volume control**
  The µGateway detects exponential changes in network traffic volume often triggered by hidden malware running on the user's device.
- **Attack detection**
  The µGateway runs an internal IPS/IDS service to detect directed threats and block fingerprinting, enumeration, DoS and exploit attacks.
- **Tracking and ad-blocking**
  The µGateway blocks ads and tracking transparently on the network level without requiring additional software on the host or in the browser.

Threat Management

The µGateway performs continuous analysis on the connected Wi-Fi network, alerting IT of threats immediately and, if required, cutting network access autonomously when the network environment becomes hostile.

Any attack attempts against the µGateway will be detected by the in-device threat management, and live alerts will be sent to the user and IT through the Management Console. The µGateway also autonomously blocks attacks without the need for interference from the user or the IT department, and can decide in real time whether the user should be disconnected from the network as a fail-safe.



OSI Model Protections

The Byos µGateway provides multi-layer protection across OSI layers 1 to 5, covering multiple attack vectors.

- **OSI 1 - Physical**
  - Wired connection to host
  - Hardware security layers
  - Rogue AP protection
- **OSI 2 - Data Link**
  - Wi-Fi identity checks
  - ARP-poisoning protection
  - Gateway integrity checks
- **OSI 3 - Network**
  - Restrictive firewall
  - Route alteration detection
  - Network identity checks
- **OSI 4 - Transport**
  - In-device encrypted DNS
  - Malware containment
  - Multi-factor traffic control
- **OSI 5 - Session**
  - Bandwidth spike checks
  - In-device VPN tunneling
  - Multi-factor Network Access Control

BYOS

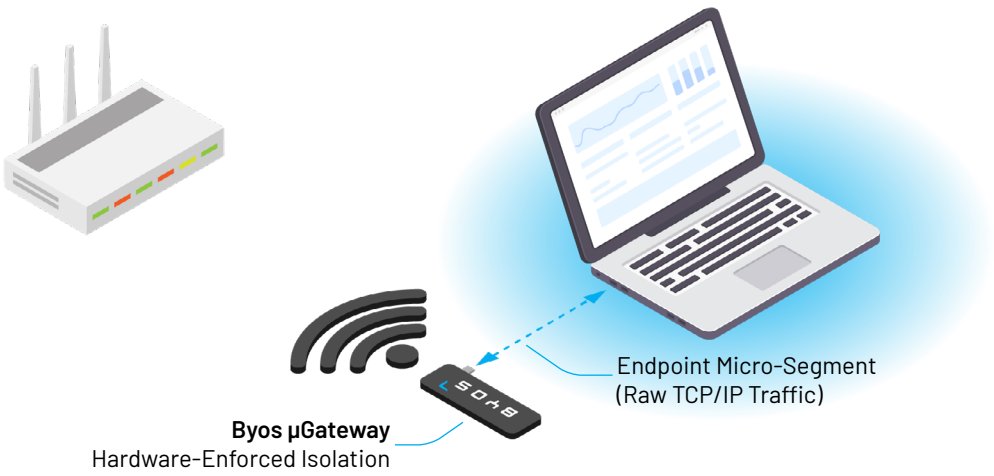
Byos µGateway Technical Specifications:

- **Type of device:** Plug-and-Play USB Ethernet Gateway (RNDIS Gadget).
- **Port Requirements:** USB-C (USB 3.0/3.1 adapters can be used to connect to a USB-A port).
- **Power consumption:** Under 5W. The Byos µGateway can be powered solely through its male USB-C connector.
- **OS Requirements:** Any OS compatible with USB-OTG (The product has been tested with Windows, OSX, iOS, and Linux operating systems).
- **Driver requirements:** None (For some Windows devices: USB-OTG driver auto-installs over Wi-Fi if not present).
- **Software Requirements:** Home Dashboard accessed via web browser; tested with current versions of Chrome, Firefox, Safari, Internet Explorer, Edge, and Opera. No additional plug-ins or software required.
- **Manufactured:** In Canada and USA.
- **Dimensions:** 10.5 x 3.4 x 1 cm (4.1 x 1.3 x 0.4 in).

Deployment and Implementation

With streamlined provisioning for all categories of endpoint devices, Byos enables zero-trust migration and implementation through simple plug-and-play security. There is no need to physically install software or agents on users' devices. The solution is easy to use and requires no previous end user security knowledge.

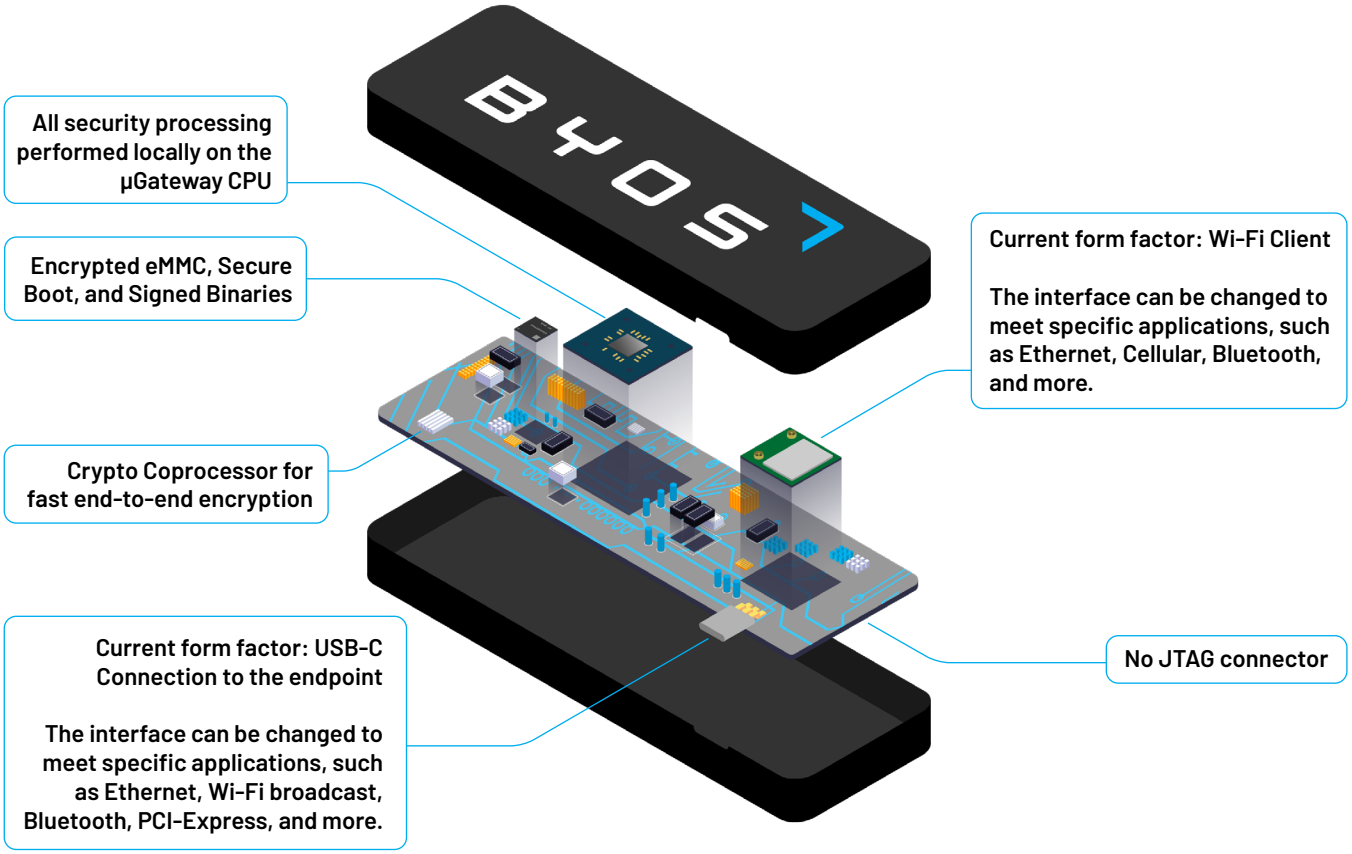
- Portable and lightweight, the µGateway fits in the palm of your hand and can be transported anywhere by the user
- The µGateway is powered solely by the USB connector of the user's device with no need for a power outlet or battery
- Automatic device enrollment and integration into enterprise security programs and infrastructure
- The µGateway is technology agnostic, can be used with any connected device regardless of its operating system, model or age
- Does not impact or restrict connection speeds



The µGateway does not perform Deep Packet Inspection. The µGateway maintains TLS encryption as the traffic passes through it – the Internet connection is transparent to the endpoint and the egress traffic is clean, which allows it to communicate as the endpoint normally would. Because there is no software running on the endpoint the user's privacy is maintained.

Customizable Board for Complex Deployments

The Byos µGateway hardware design makes IoT implementation simple and flexible across use cases – from legacy IoT devices to embedded applications. The Byos proprietary hardware board can be customized to fit different size and power requirements with minimal variability in PCB design, making it applicable for any TCP/IP connected device and different I/O network interfaces.



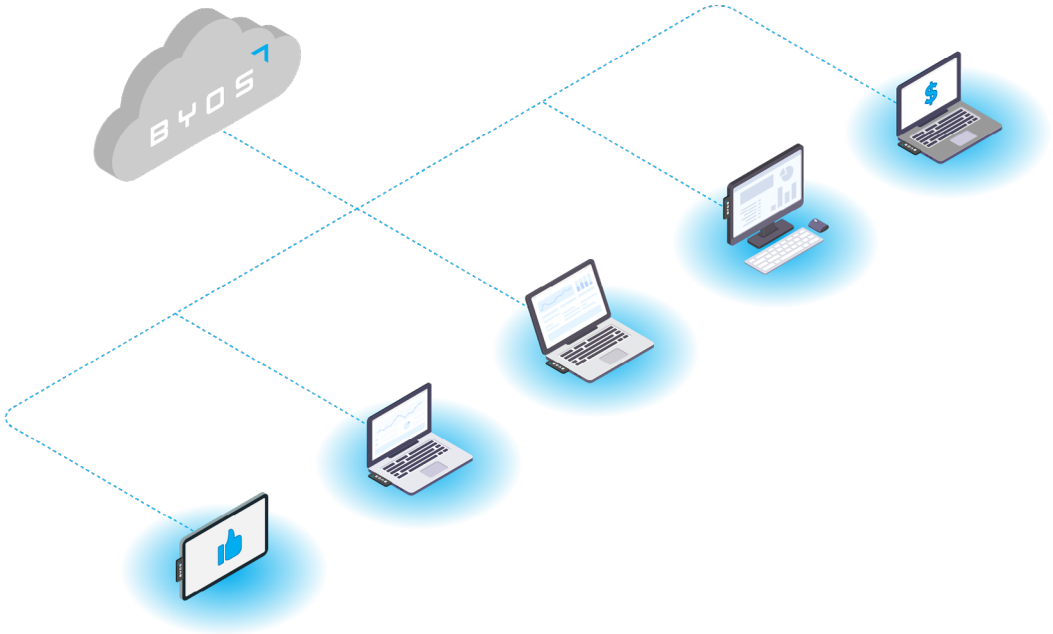
µGateway Internal Product Security

Byos µGateway hardware runs a proprietary, hardened and customized Unix-based OS that has customized network services, signed hardware drivers, and a recompiled kernel to change its fingerprint. Residing above the base OS, the Byos core has a proprietary attack knowledge base, decision-making algorithm, network health detection service and multi-layer API. Input sanitization of communication requests between the layers occurs within the µGateway, as different layers cannot speak directly with each other – the frontend cannot speak directly to the base OS, and the Byos core cannot communicate directly with the hardware, thereby increasing security.

Byos' development team follows a Secure Software Development Lifecycle (SSDLC) with its internal security team performing continuous testing. For external security testing, the company goes through continuous third-party audits and an open bug bounty program, ensuring the highest level of accountability. For more information, please visit byos.io/resources to read the whitepapers.

The µGateway has a proprietary hardware board that is manufactured in Canada and the USA, with a certified supply chain of components and a certified chain of custody of software, so there is full assurance the product does not have hidden backdoors.

The Byos Business Starter 5-Pack



Ready to ensure that remote users are safe to connect and free to work? We've made it easy. The Byos Business Starter 5-pack includes:

- 5 µGateway devices
- Cloud-based Management Console access

The Business Starter 5-Pack will show you how easy deployment, usage, and provisioning are with the Byos Endpoint Micro-Segmentation Solution. Start small with a pilot deployment, see the value, and then deploy more µGateways across your organization from there.

Order your Byos Business Starter 5-Pack today

byos.io/get-started

If you would like to learn more about Byos or are interested in deploying to a larger group or enterprise with self-hosting capability, contact us at engage@byos.io.