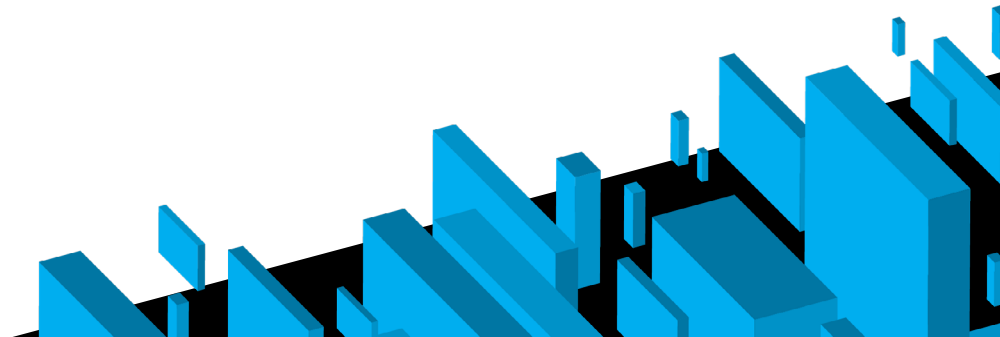
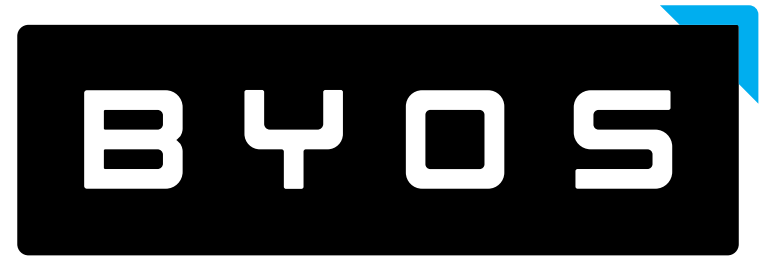


# Byos $\mu$ Gateway™

## Evaluation Guide



## Welcome to the Byos $\mu$ Gateway Evaluation Guide!

Here is the Evaluation Guide to help you make the most out of the Byos  $\mu$ Gateway ("micro-gateway") and take advantage of all its features. Please carefully review each section below and if you have any questions, please reach out to [support@byos.io](mailto:support@byos.io) or call 1-902-220-3384 for further assistance - we are based in Atlantic Time. You can also message us through the chatbot on our website.



## Table of Contents

### 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/USA.
- **Dimensions:** 10.5 x 3.4 x 1 cm (4.1 x 1.3 x 0.4 in)

Step 1: <a href="#">Learn more about the Byos µGateway</a>	4
Step 2: <a href="#">Login and Connect to the Wi-Fi</a>	5
Step 3: <a href="#">The Byos µGateway in action</a>	6
Robust Protection Mechanisms	6
Near Zero Performance Impact	7
Autoconnect Feature	7
Reviewing Controlled Access; Reviewing Controlled Access & Setting Up Desired Internet Traffic Security Policies	7
Optional - Advanced Security Testing your µGateway	7
Step 4: <a href="#">What's under the hood?</a>	8
Security and Privacy of the µGateway	8
Troubleshooting	9
I'm using a Windows Laptop or Tablet and the Home Dashboard at "My.byos/home" isn't loading...	9
Enterprise Deployment and Management Overview	10
Byos Company Overview	11

# Step 1: Learn more about the Byos $\mu$ Gateway

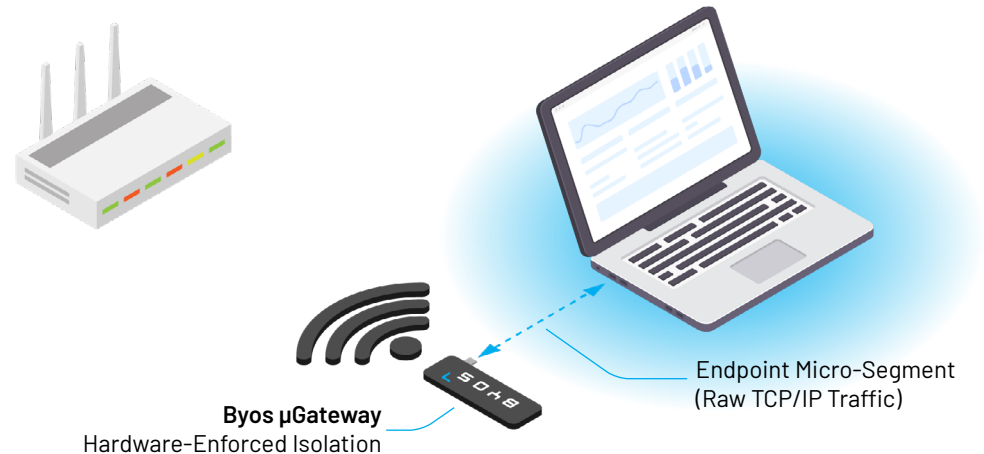
## Product Overview

The  $\mu$ Gateway is the endpoint security solution built specifically for protection on public Wi-Fi networks like those found in Airports, Hotels, Conferences, Cafes as well as guest networks - what we call "dirty networks".

The  $\mu$ Gateway is the world's only plug-and-play, transparent security gateway on a USB device, allowing individuals, employees, and devices to safely and securely connect any network, regardless of their location or network environment.

We took the proven approach of network segmentation but applied it to the endpoint, creating a *micro-segment of 1*.

The  $\mu$ Gateway retails for \$299 including hardware and a 1 year security service subscription, and is available for purchase at [byos.io](https://byos.io). The  $\mu$ Gateway is the only endpoint micro-segmentation solution that isolates and protects your devices from dirty Wi-Fi networks.



The  $\mu$ Gateway facilitates the endpoint's connection to the local network, sitting at the ingress/egress point of communication between the network and the endpoint. This eliminates any device exposure to the network, making it invisible to attackers.

Even with the use of an antivirus, VPN, or secure web gateway, there are a number of attacks that endpoints are remain vulnerable to, which are protected by the  $\mu$ Gateway such as:

- Scanning/Enumeration/Fingerprinting
- Eavesdropping
- Remote Access Exploits
- Evil-twin Wi-Fi
- Lateral network movement
- DNS hijacking

## Step 2: Login and Connect to the Wi-Fi

### How to Connect for the First Time:

1. Turn off your device's Wi-Fi (place it in airplane mode). Plug in the  $\mu$ Gateway using either the standard USB-C port or use an adapter for an USB-A port.
2. The  $\mu$ Gateway will take 20 seconds to boot up. After 20 seconds, open up a browser and type "[my.byos/home](https://my.byos/home)" into the URL bar. This will take you to the Sign-in page of the Home Dashboard. This dashboard is self-hosted on the  $\mu$ Gateway.
3. Create your account username and password, and log in. Click "Remember Me" so you will log in automatically every time you plug in your  $\mu$ Gateway.
4. You will now be prompted to select a network in range to connect to. Select your desired network and type in the password. The device will now perform a network health and security check before connecting. If the network has a captive portal, you will be prompted to accept its terms before traffic will be allowed to flow.
5. If you wish to connect to a hidden network, click cancel and then navigate to the Wi-Fi page from the button in the left navigation bar. Once on the Wi-Fi page, click "Connect to a hidden network" and enter in the credentials.
6. Once the connection is established, you will now see the home Dashboard with your network traffic map by country. You are now free to work securely.
7. **Optional: Configure your VPN** - If you also subscribe to a VPN service, you can run it through the  $\mu$ Gateway. Click "VPN" on the left navigation bar, click "Add VPN", and select your provider.

Now that you are connected to the internet using your Byos  $\mu$ Gateway, you are fully isolated from the rest of the devices on the network and can close the dashboard.

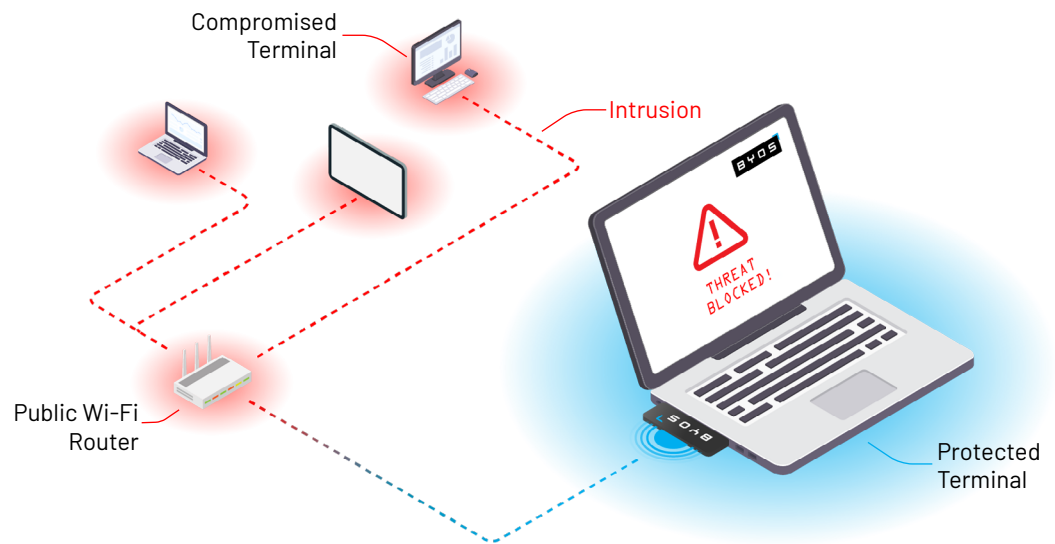
You will need to use the dashboard to connect to the Wi-Fi every time you enter a new network environment. We also suggest always using the  $\mu$ Gateway wherever you are to protect yourself from the risks associated with public and Home Wi-Fi networks.

## Step 3: The Byos $\mu$ Gateway in Action

### Robust Protection Mechanisms

The  $\mu$ Gateway is a “security stack on a stick” processing all of the protection services on its hardware, with no protection dependencies in the cloud. The specific security services running on the  $\mu$ Gateway 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** - prevents the user's Wi-Fi connection from being intercepted, cloned, bypassed or hijacked.
  - **Eavesdropping Prevention** - the  $\mu$ Gateway maintains direct and confidential communications with the network gateway, without allowing the poisoning of the routing tables.
  - **Private DNS Queries** - the  $\mu$ Gateway runs an in-device Encrypted DNS server, preserving confidentiality of the user's browsing data.
  - **Infiltration Prevention** - the  $\mu$ Gateway detects changes in the routing of packets to the Internet, and takes the necessary actions to prevent any data leakage.
- **Traffic Volume Control** - the  $\mu$ Gateway detects exponential changes in network traffic volume, often triggered by hidden malware running on the user's device.
  - **Attack Detection** - the  $\mu$ Gateway runs an internal IPS/IDS service, detecting directed threats, blocking fingerprinting, enumeration, DoS, and exploit attacks. Any attack attempts against the  $\mu$ Gateway will alert the user.
  - **Tracking and Ad-blocking** - the  $\mu$ Gateway also blocks ads and tracking transparently on the network level, without requiring additional software.



## Step 3: The Byos $\mu$ Gateway in Action

### Near Zero Performance Impact

The  $\mu$ Gateway is powered by the USB port, without the need of external power, and unlike software solutions, it doesn't steal computing resources from your device. It will also not restrict the internet connection speed.

**Try it yourself:** simply run a connection speed test with and without your  $\mu$ Gateway, and compare the results.

### Autoconnect Feature

Your  $\mu$ Gateway will store the network credentials for any previous network connections so that when you replug it in and the same network is in range, the  $\mu$ Gateway will autoconnect for a transparent and seamless connection.

**Try it yourself:** connect to a new network via the  $\mu$ Gateway, unplug your  $\mu$ Gateway and replug it in, seeing that it connects automatically.

### Optional - Advanced Security Testing your $\mu$ Gateway

The protection mechanisms offered Byos  $\mu$ Gateway can be verified by performing various penetration tests on the device, including:

- Sniffing/Eavesdropping
- Exploit Attacks
- Man-in-the-Middle Attacks
- Scanning/Fingerprinting/Enumeration Attacks
- Black Box penetration test methods (SQL injection, XSS, DDoS, etc.)

If you would like our assistance setting up these tests, please contact us at [support@byos.io](mailto:support@byos.io).

### Reviewing Controlled Access; Reviewing Controlled Access & Setting Up Desired Internet Traffic Security Policies

In an enterprise setting, IT admins typically configure access permissions based on corporate policies and automatically push these security rules to individual  $\mu$ Gateways under their control. To sample how this functionality on your individual  $\mu$ Gateway device, in the the "Access Control" button on the left navigation bar of the home Dashboard, you will see commands for:

1. **Block Country** - Selecting specific countries to block will forbid your device from establishing a connection with a server located in said country. Blocking a country turns it red on the home dashboard's network traffic map. The easiest way to block traffic to a specific country from the home dashboard involves simply right clicking on the country you wish to block.
2. **Block Domain Name, IP Addresses and Ports** these features will block traffic from specific websites, IP addresses, and ports.

The whole premise behind the  $\mu$ Gateway is that you should be in control of what countries, domains, IP addresses, and ports your device connects to. Most people don't realize the amount of connections their devices make on a day-to-day basis, let alone which countries these servers are in.

## Step 4: What's under the hood?

The µGateway is technology-agnostic meaning it works with any type of endpoint, regardless of the OS type or version; it does not require installation of any software agent on the host endpoint. The µGateway runs a proprietary, hardened Linux OS that has customized network services and signed Hardware drivers. It also has a proprietary attack knowledge base and network health detection service. For hardware security, the µGateway has an encrypted file system, secure boot, no JTAG connector, and PKI-signed code, making it resistant to hardware attacks.

The µGateway has a proprietary Hardware board that is manufactured in Canada and the USA. It has a certified supply chain of components and a certified chain of custody of Software, so we have full assurance the product does not have hidden backdoors.

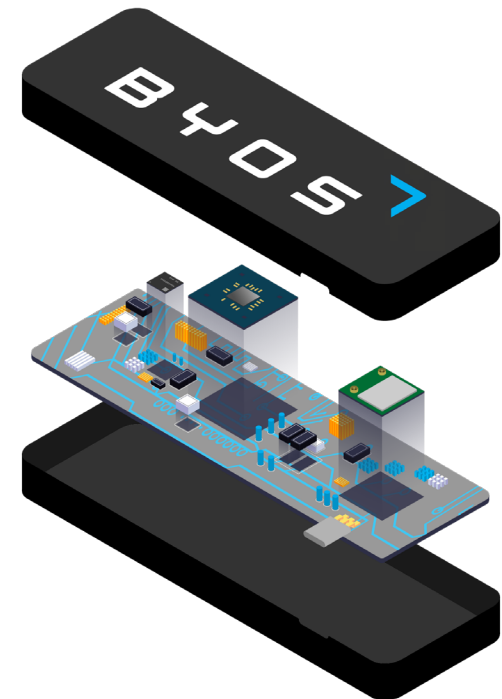
### Security and Privacy of the µGateway



We perform extensive white-box and black-box testing on the µGateway to ensure our product is secure. The µGateway is NIST, SANS Top 20, and COBIT compliant.

For industry security validation, we also run a bug bounty program. A bug bounty program allows security researchers to perform penetration testing against the µGateway to find security vulnerabilities/weaknesses and to validate the protection claims made,

reporting the bugs found to our internal security team. You can find more information about the results of our previous bug bounty events at [byos.io/resources](https://byos.io/resources).

To preserve the users' privacy, we never collect logs about your usage of the µGateway. The only time the µGateway will communicate with our servers is during boot; It will check to see if the license is valid and if there are any updates available. This can be verified by analyzing the traffic between the µGateway and the router.



Byos is manufactured in North America, with a certified supply chain of components.  



# Troubleshooting

I'm using a Windows Laptop or Tablet and the Home Dashboard at "my.byos/home" isn't loading...

If the Home Dashboard at "[my.byos/home](https://my.byos/home)" isn't loading on your Windows laptop or tablet, the USB-OTG driver is likely disabled. Open up your network settings, and see if your device has recognized the  $\mu$ Gateway. The  $\mu$ Gateway uses the "USB-OTG" specification and should be recognized by your device as a "RNDIS/Ethernet Gadget".

If your device does not recognize  $\mu$ Gateway, unplug it. The driver will be automatically installed on the host device if the device has an internet connection the first time the Byos  $\mu$ Gateway is plugged in. Turn your Wi-Fi back on and re-plug in the  $\mu$ Gateway; leaving your Wi-Fi on while the  $\mu$ Gateway is booting up should trigger an automatic download of the driver.

If the  $\mu$ Gateway is still not being recognized by your device, [visit this link](#) for instructions to re-install the USB-OTG driver.



## USB device not recognised

The last USB device you connected to this computer malfunctioned and Windows does not recognise it.

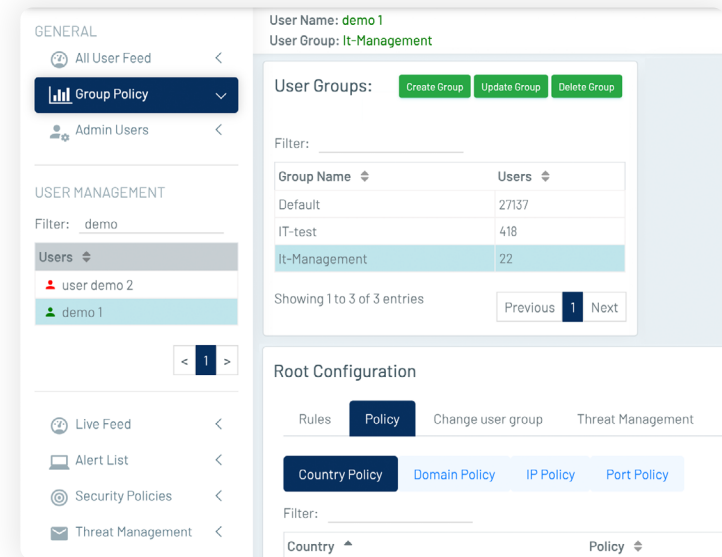
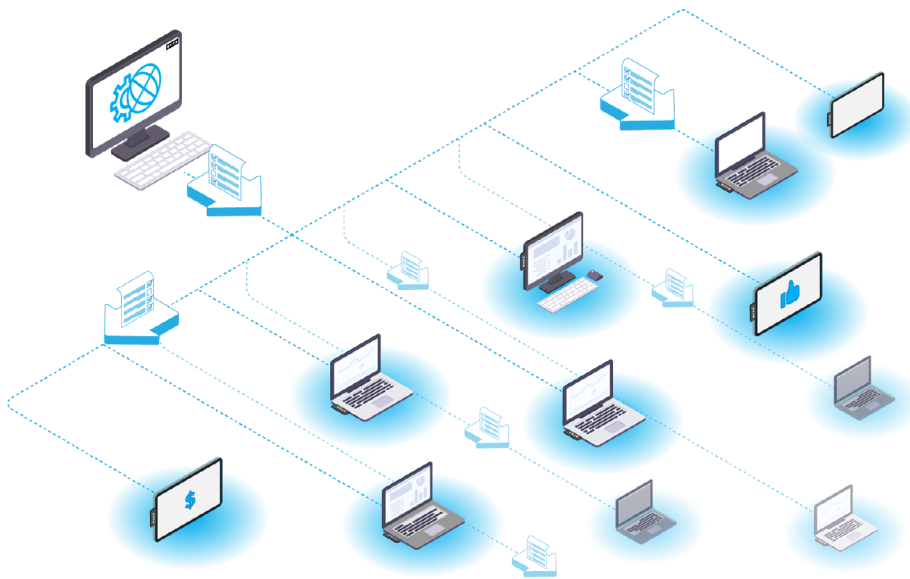
Windows Explorer

# Enterprise Deployment and Management Overview

## For the Enterprise

For enterprise clients, the Byos Endpoint Micro-Segmentation Solution is delivered with an enterprise-class Management Console to deploy and manage  $\mu$ Gateways at scale.

This allows IT security teams to confidently, efficiently and cost-effectively manage a global workforce centrally, streamlining user and device provisioning, all while having granular visibility and control over remote endpoint corporate access connections. The  $\mu$ Gateway also facilitates Zero Trust access from any remote network connection.



# Byos Company Overview

Byos is the endpoint micro-segmentation company dedicated to helping organizations protect themselves from the risk of ubiquitous remote, guest and IoT network connectivity. Byos allows employees, contractors and devices to safely and securely connect to any network, regardless of their location or network environment.

The Byos  $\mu$ Gateway, implemented as a portable “security stack on a USB stick” or as embedded circuitry directly in a device, automatically creates a *micro-segment of 1* delivering hardware enforced protection of the device from the inherent risks on dirty networks while allowing secure zero-trust based access to corporate resources. The Byos Management Console provides centralized policy management and reporting across enterprise wide deployments of  $\mu$ Gateways.

Byos is backed by leading Silicon Valley investors and advisors, is headquartered in Halifax Canada, and sources and manufactures all components in North America. With Byos, work from home, traveling and remote workforces are Safe to Connect, and Free to Work. (To learn more and get started securing your remote WiFi connections visit [byos.io/get-started](https://byos.io/get-started)).

