Why Trust Byos?

Team

Security is in our DNA and engrained in everything we do. Our commitment to security is reflected in the products we build and the way we operate, all for the protection and integrity of the customer.

From concept to solution, our team of industry-vetted cybersecurity veterans has designed and built our patented technology with security in mind at every stage. Our entire team of employees, advisors, and contractors is based out of North America.

Matias Katz - Founder & CEO

- Expert ethical hacker with 15+ years of hands-on experience at top Corporations and Government Entities
- Former security and infrastructure specialist at IBM; Previously founded a mid-tier MSSP in Argentina
- Official CISSP Instructor and frequent conference speaker (Black Hat, TEDx, Campus Party)

Technical Advisors

- **Paul Kocher** - Renowned security researcher. Co-Creator of SSL/TLS protocols
- **Jim Routh** - Former CISO, MassMutual, CVS Health, Aetna, and JP Morgan Chase
- **David Bauer** - Former CISO, Digital Asset, Merrill Lynch
- **Neil Daswani, PhD** - Co-Director, Stanford Advanced Computer Security Program

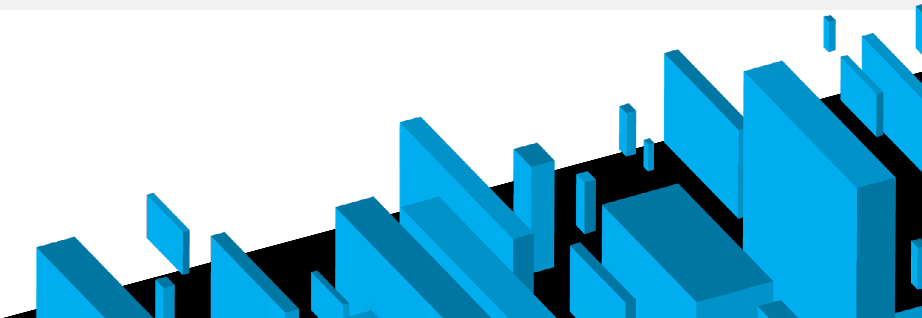
Secure Development Process

Byos' development team follows a Secure Software Development Lifecycle (SSDLC) with its internal security team performing continuous testing.

- Static Analysis & Unit Tests
- Continuous Integration - every build passes every test
- Dedicated Red Team - team of experienced security experts actively trying to break every piece of code

Our µGateway Security Testing Guide is used during a customer's testing process to validate the claims of the protection features we offer. We ask customers to test our claims for themselves, and encourage them to provide us with the results from their own pen-testing teams.

For external security testing, the company goes through continuous third-party audits, ensuring the highest level of accountability. Our contract penetration testing is performed by GoSecure (CounterTack)



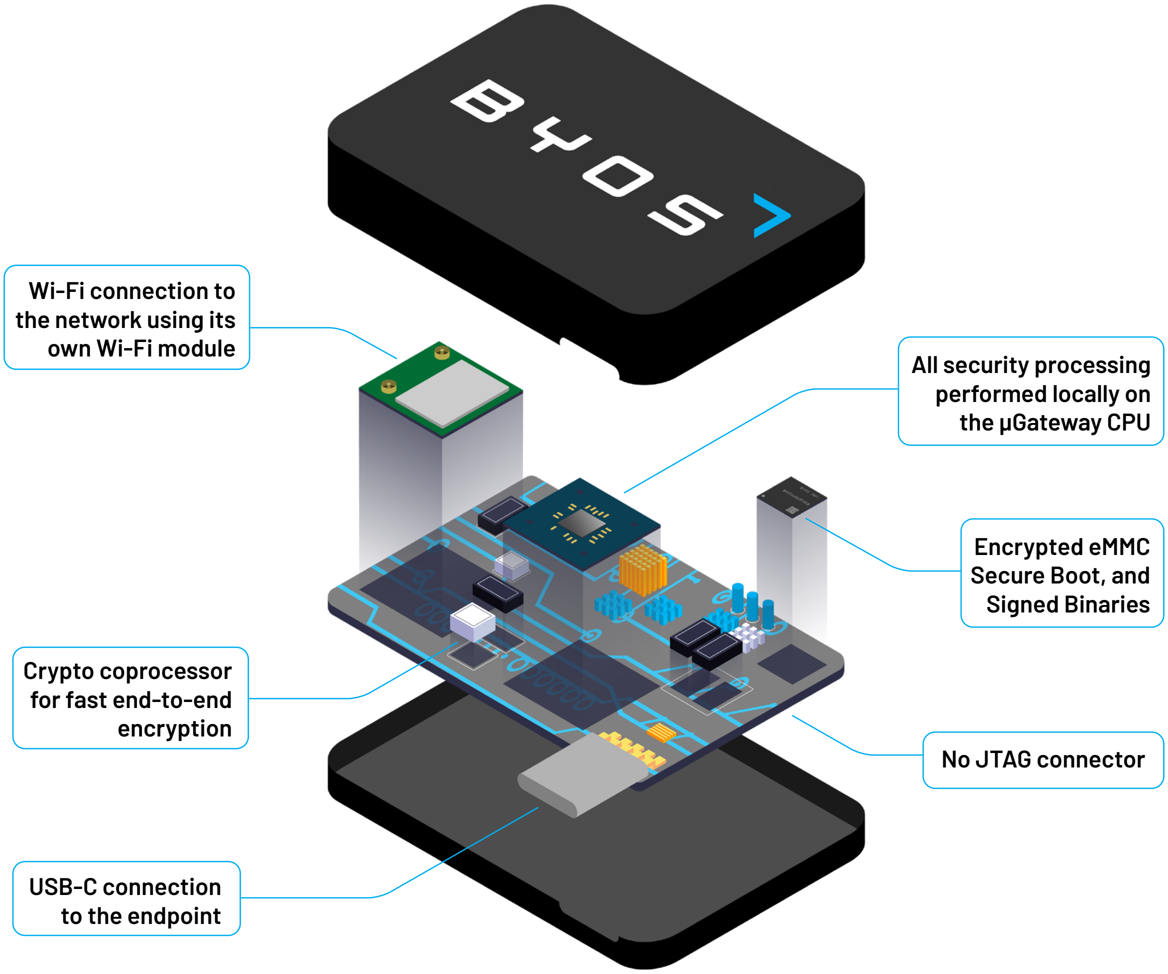
µGateway Internal Product Security

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 front end cannot speak directly to the base OS, and the Byos core cannot communicate directly with the hardware, thereby increasing security.

The µGateway's enclosure is tamper-resistant. The enclosure is a screwless, snap-fit design, that cannot be opened without being obviously damaged, significantly reducing the risk of someone opening the enclosure and making modifications without the user's knowledge.



Wi-Fi connection to the network using its own Wi-Fi module

All security processing performed locally on the µGateway CPU

Encrypted eMMC Secure Boot, and Signed Binaries

Crypto coprocessor for fast end-to-end encryption

No JTAG connector

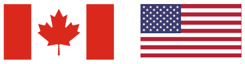
USB-C connection to the endpoint

Manufacturing and Supply Chain

Components inside the µGateway are sourced through Arrow Electronics - a Fortune 500 global leader in distribution of electronic components and value-added services headquartered in Colorado. Our product's component comes exclusively from their American warehouse in Nevada and Arrow pre-flashes our components before they even arrive at our Contract Manufacturing Partner. Arrow's advanced databases also allow for detailed lot code tracing for quality - based on a Byos serial number, we can identify which reel on the manufacturing line each component inside came from.

Our Californian-based Contract Manufacturer completes the hardware design entirely in-house with Byos feeding requirements and owning the resulting IP.

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



Cloud Security

Our servers are compliant with Cloud Security Alliance standards:

- Data in transit encryption is TLS 1.3
- Data at rest encryption is AES 256
- Encryption IVs are unique per device and rotate randomly upon every connection to the Internet
- We do not retain or track DNS log information
- We do not break the TLS layer of the user's session, we do not read any browsing data
- We do not store personal customer information in our servers
- We do not read µGateway traffic data and we also never sell or rent personal information to third parties

Bug Bounty Program:

As part of Byos' commitment to security, we run an open Bug Bounty Program, rewarding researchers who share with us critical issues and the techniques used to exploit them. We make it a priority to resolve confirmed issues as quickly as possible in order to best protect customers. Vulnerabilities found in the following aspects of the Byos Endpoint Micro-Segmentation Solution are encouraged to be reported to Byos:

- Hardware
- Firmware
- Reverse Engineering
- Networking
- Cryptography
- Cloud-based Threats
- Web-based Attacks

Whitepapers:

- BlackHat
- Hardwear.io

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

or connect with us at

engage@byos.io