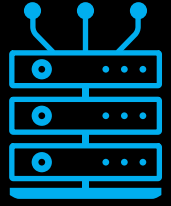


## BYOS



# Hardening Jump Box Security with Byos

With the rising adoption of hybrid or multi-cloud environments, Jump Boxes have traditionally been relied upon as the central points for securing connectivity across network boundaries. Coupled with the increasing need for secure remote access within government and defense-specific networks, Jump Boxes are being increasingly targeted by attackers, as they serve as the single point of failure for many networks.

We propose Byos' microsegmentation solution as a secure replacement for Jump Boxes. Byos solves a core issue of most Jump Boxes: unpatchable System-on-Chip firmware vulnerabilities. These vulnerabilities make Jump Boxes the low hanging fruit for the highest ROI on attack, but Byos provides High Assurance Network Access (HANA) technologies that makes devices and networks invisible, preventing compromises from spreading laterally and infecting additional networks. In addition to protecting networks against ransomware by containing the blast radius, the Byos Microsegmentation Solution has a Secure Overlay Network allowing for remote troubleshooting, streamlined data aggregation, secure 3rd-party access to critical production equipment, and more efficient centralized network management. All of these benefits come without exposure to the underlying network, meaning seamless deployment with minimal disruption to current operations.

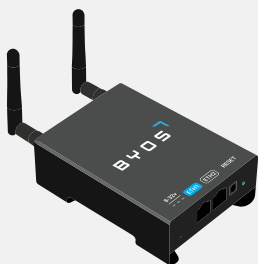
## The Challenges with Securing Current Jump Box Systems

Jump Boxes are ubiquitous and necessary inside of large complex networks, but they are not immune to certain security vulnerabilities:

- As Jump Boxes act as a centralized access point, if the Jump Box becomes unavailable or disrupted due to hardware failures, software issues, or cyberattacks, authorized users may lose access to the connected resources
- System-on-Chip vulnerabilities that are unpatchable can allow the Jump Box system to be compromised, resulting in potential loss of data
- Firmware vulnerabilities are common in devices that are long lived and are extremely difficult, and often impossible to remediate using software fixes - they run the risk of bricking a device completely, rendering it useless

## Replacing Jump Boxes with the Byos Secure Gateway Edge

The Byos Microsegmentation solution consists of two components - the Secure Gateway Edge device and the centralized Management Control plane.



The **Byos Secure Gateway Edge** is a plug-and-play gateway that replaces the Jump Box, isolating the assets behind it onto its own microsegment within the network, protecting across OSI layer 1-5. The Gateway Edge is the first hop for all assets downstream, meaning they are effectively invisible.



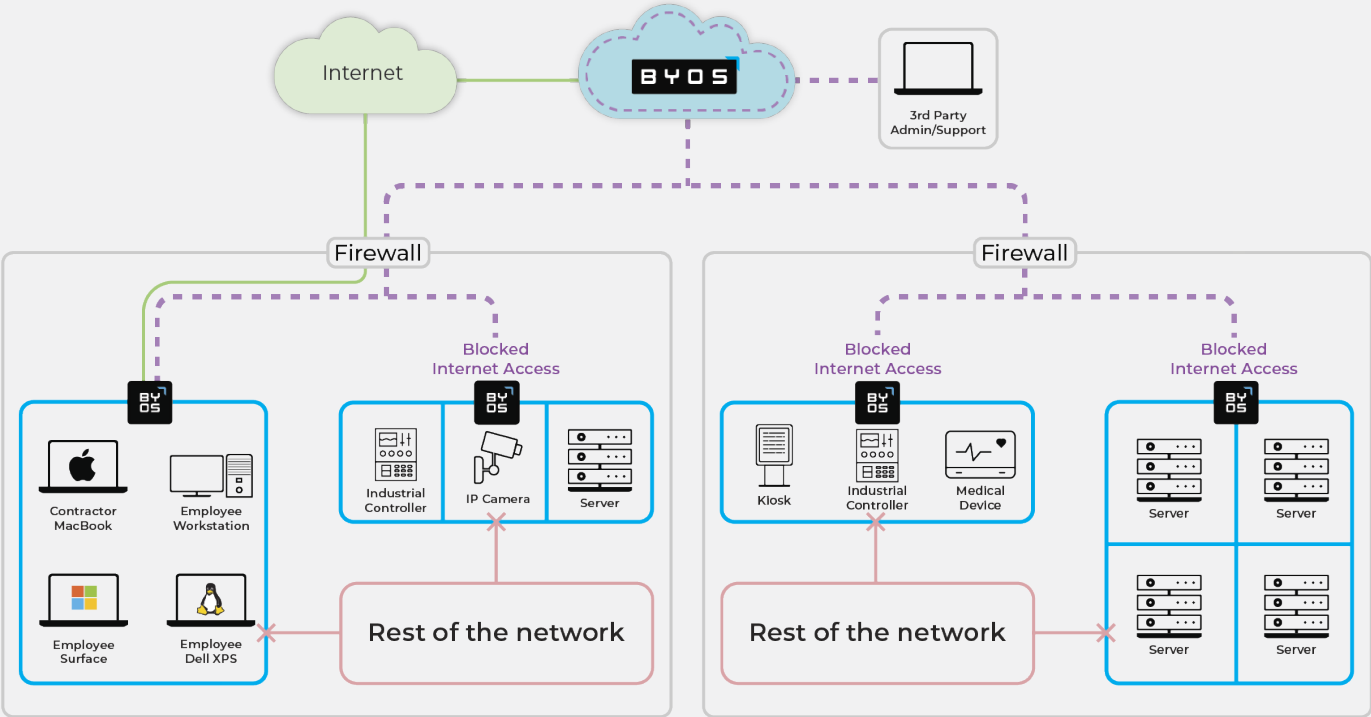
**Byos' Management Console** is the centralized control plane that helps network administrators provision, manage, and control their network of Byos Edges and all assets behind them. The Management Console can be deployed as either Cloud-based or on-premise. It enables:

- Real-time provisioning and policy-enforcement of one-to-thousands of devices
- Secure remote access to devices inside the Byos-protected network, without having to expose the network to the internet like other remote access technologies
- Connect your existing unconnected air-gapped devices to improve efficiency without exposing them to the network and adding risk



# Benefits of the Byos Microsegmentation Approach within Highly Critical and Sensitive Networks

Here is a simple diagram of how the Byos Solution gets deployed within a network:



## Unidirectional restricted access to assets within the Jump Box network

The Byos Secure Gateway Edge acts as the intermediary between the assets and the rest of the network - both WAN and LAN. Using the Management Console centralized control plane, admins are able to set up networking rules within the Byos Secure Overlay so that only authorized Byos Edges are allowed to access the Jump Box and the assets within the Jump Boxes' network. These access control rules are established across Layers 2-4, while maintaining invisibility to any potential rogue actor on the underlying local network.

## Compartmentalization of access to resources

Compartmentalizing access is key to reducing the risk of resource misuse and ensuring sensitive resources can be isolated and protected from unauthorized access. Through the Byos Management Console, administrators can establish networking "Zones" which are OSI Layer 2 enforced networking boundaries within the Byos Overlay. After assets within the Jump Box networks have been automatically discovered by the Byos Edges, admins enable Layer 3 and 4 access control routes to specific resources (ports and service combinations) on specific Byos Edges. An admin is only authorized to access a resource within the Byos network after all three controls are completed to ensure granular secure communications across devices connecting from unknown networks.

## Remote data collection and data pull actions within air-gapped networks and devices

Because every asset behind the Byos Edge is now accessible through the Byos Secure Overlay, accessing resources over an untrusted network is as secure yet easy as ever. Administrators can be on their Home Wi-Fi, connecting granularly (down to the port and service) to a classified resource on a secure network on-prem somewhere in the world through the Byos Overlay, without any exposure to the public internet, other assets within the microsegmented network, and other Byos Edges within the Byos network. This ability to access resources running on assets inside of protected networks, from any untrusted network in the world is what sets Byos apart from other solutions.



### Controlled software-defined "airgaps" for Immediate Incident Response Lockdown

After the deployment of Byos, the assets in the microsegment are effectively "air-gapped" from the WAN network they connect to - all of their networking is governed by the Byos Secure Gateway Edge, and don't actually have a Layer 0 or 1 link to the network. In the Management Console control plane, there is a routing rule that denies assets internet access, but allows traffic out to the Secure Overlay. This feature, in combination with the software-defined "airgap", is a unique incident response feature that allows complete lock down of a network without actually losing connectivity to the microsegment. There is no longer a need to power off devices to stop a ransomware attack - simply stop their ability to communicate to the internet.

### Multi-layer Protection

The Byos Secure Edge Technology's protection works across OSI layers 1-5, covering multiple attack vectors:

#### OSI 1 - Physical

- Wired connection to host
- Hardware security layers

#### OSI 2 - Data Link

- Traffic poisoning prevention
- Private overlay networking

#### OSI 3 - Network

- Enumeration prevention
- L3 traffic access control

#### OSI 4 - Transport


- In-device encrypted DNS
- L4 traffic access control

#### OSI 5 - Session

- East-West traffic prevention
- IAM enforcement

**Key Product Security Features:**

- Hardened Linux-based OS
- Custom re-compiled kernel
- Signed proprietary binaries
- Customized network services
- HW security layers
- Certified supply chain
- Industry tested and validated
- Over-the-air updates

**Built in North America** 

### Byos makes Jump Box Integration and Security Easy to Deploy

Integrated in a secure Jump Box approach, Byos serves as the gateway for both Wired and Wireless TCP/IP communications. In fact, Byos is already working with one of the largest U.S. intelligence agencies with this approach. Byos can also be easily deployed for different use cases, giving you extended network reach, providing resilience, improved security and unidirectional remote access, enabling monitoring and control, offering isolation and segmentation, and facilitating scalable network expansion in all cases.

Byos is simple to deploy, manage, scale, without having to change the underlying network. If you're looking for more secure remote access across your network, or looking to securely add more connectivity, request a demo here: [byos.io/request-demo](https://byos.io/request-demo)

