FEATURE DATASHEET

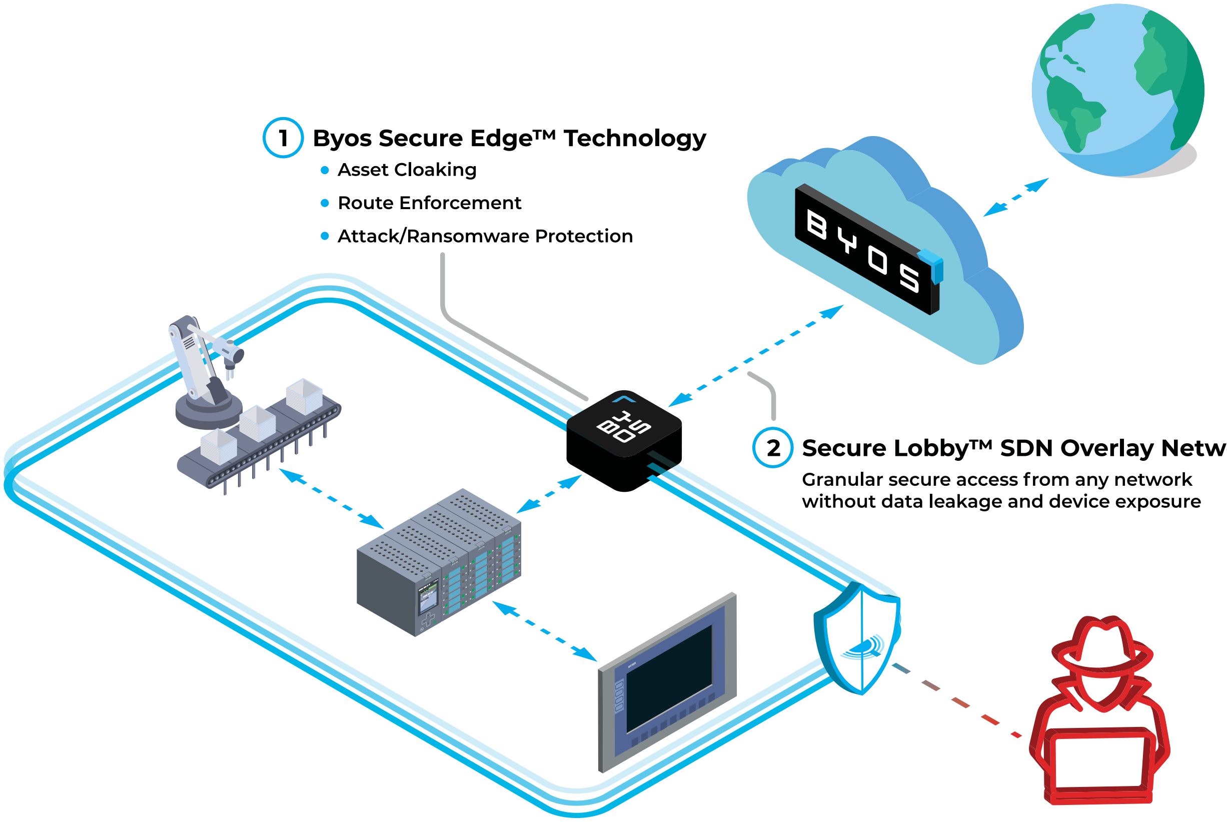
Secure Lobby Overview

Secure remote management and access to assets, without the exposure

Introduction

Byos Secure Lobby™ (SL) is a Secure Software-Defined Network (SDN) overlay that allows for secure remote access to assets protected by the Byos Edges, and to control the flow of information from Asset to Asset. Conventional remote access tools require opening up the perimeter, which adds unnecessary exposure and risk, to entire corporate networks. The Byos Secure Lobby™ Overlay allows for monitoring, troubleshooting, updating, and patching remotely, without exposing assets and traffic to the internet.

Byos Secure Edge™ devices connect to the Byos Secure Lobby™ SDN overlay using outbound Layer 2 tunnels. This connection happens before any packets travel over the network to ensure no leakage of traffic, and is determined by the policy group set inside the Byos Management Console.



1 **Byos Secure Edge™ Technology**

- Asset Cloaking
- Route Enforcement
- Attack/Ransomware Protection

2 **Secure Lobby™ SDN Overlay Network**

Granular secure access from any network without data leakage and device exposure

Key Features

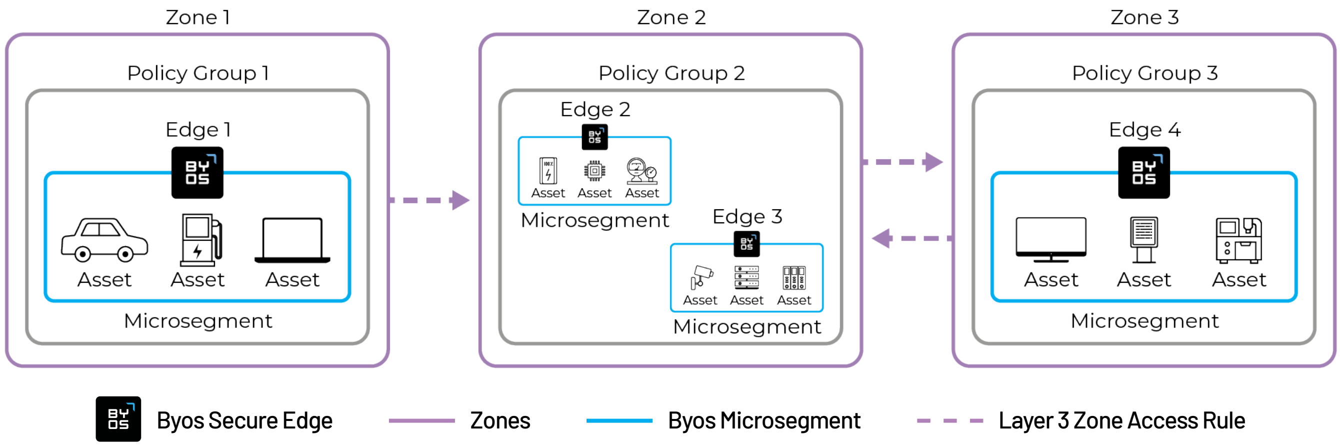
- **Fully encrypted and anonymized traffic** - Administrators have the option to route all traffic through Secure Lobby (both Byos control plane traffic and the endpoint's Internet traffic).
- **Zero public internet packet leakage** - Admins also have the option to auto-connect to Secure Lobby on boot, 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.

Want to see the Secure Lobby in action?
Visit byos.io/request-demo

Byos Secure Lobby Concepts

Secure Lobby™ has a number of different components, each playing a part in how it operates.

- **Zones** - Network zones within the Byos Secure Lobby Overlay, with Layer 3 Access Control Rules determining which communications between Zones are allowed.
- **Policy Group** - An Edge or a group of Edges, with an assigned set of policies, that has been configured in the Management Console. Policy Groups determine how the Edges talk to Secure Lobby™ via the External Routing Rules (which are outlined below).
- **Edge** - A Byos Secure Edge device, Gateway or Endpoint.
- **Microsegment** - The internal network created by the Byos Edge, isolated from the outer WAN side of the Edge.
- **Asset** - Any Device connected to the Byos Edge, inside the microsegment.



External Routing Rules, set via Policy Group

Administrators have different options for setting the external routing rules for Edges in a policy group, each determined by how they want traffic to originate from the Edge. There are three variables in different combinations for each routing rule: i) internet access, ii) Secure Lobby™ connection (with directionality), and iii) outbound LAN Access

- Scenario A - Internet Access Only
- Scenario B - Internet Access, Inbound SL Access, Outbound Access to LAN
- Scenario C - Internet Access, Bidirectional SL Access, Outbound Access to LAN
- Scenario D - Internet Access (tunneled through SL), Bidirectional SL Access, No Access to LAN
- Scenario E - No Internet Access, Bidirectional SL Access, No Access to LAN
- Scenario F - No Internet Access, Inbound SL Access only, No Access to LAN
- Scenario G - Full Airgap (No Internet, No SL, No LAN access)
- Scenario H - Internet Access, Bidirectional SL Access

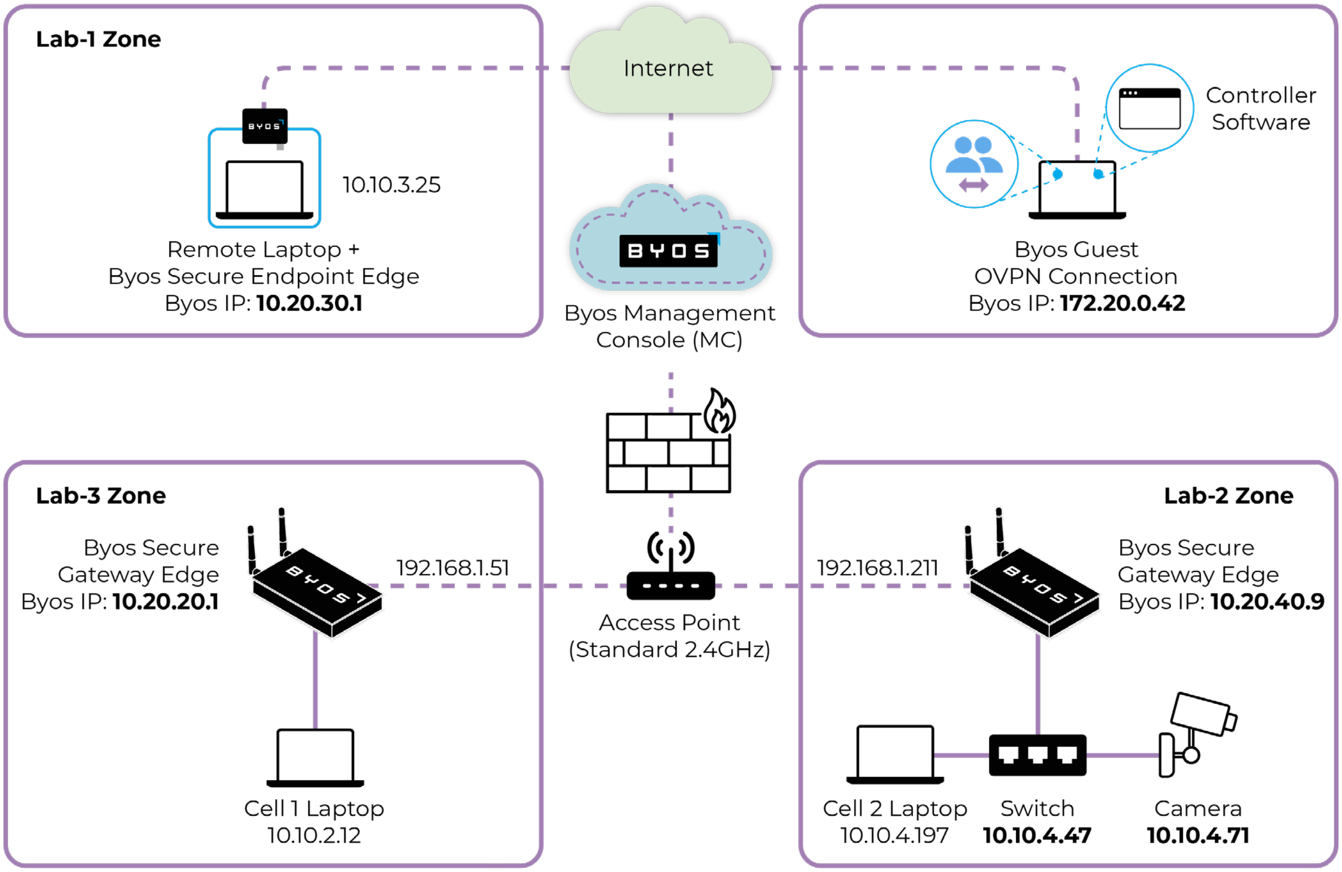
Zones and Assets - Layer 3 and 4 Access Controls

Once you have selected the external routing rules for your Edges, Layer 3 Access Control in Secure Lobby SDN is facilitated using Zones for logically segmenting traffic within the SL Overlay. Add unidirectional or bidirectional traffic rules to control traffic between different Zones!

Then, after Edges are connected to the Overlay and Zones connections have been established, Admins can make discovered Assets visible in SL on a specific port and service basis! For example, just because an Asset has SSH/22 exposed to the Byos Edge doesn't mean that Asset can be reached using SSH/22 from the Secure Lobby™ Overlay! This gives the Admin maximum control over what can be accessed on their Assets.

How to Use Secure Lobby

1. First, the Network Admin or Service Technician initiates the Secure Lobby connection in the Byos Management Console.
2. Upon receiving the command from the Management Console, the Byos Edge then establishes an outgoing 4096 RSA-encrypted connection with the Secure Lobby, which is not impacted by the corporate network firewall and does not require weakening the perimeter security of the main network.
3. The user then connects their computer to the Secure Lobby using an encrypted connection.
4. Once the user is inside of the Secure Lobby, the Byos Edge allows traffic to and from the protected asset, allowing the user to interact with the endpoint directly.



Key Benefits

- Securely prolong the life of IT infrastructure running legacy applications and unsupported OS that are not ready to be retired. Previously air-gapped devices can be connected to the network for more efficient and secure remote maintenance and monitoring.
- Non-intrusive deployment to existing network configurations, without having to expose internal devices to the internet, and eliminating any spread of internal threats like lateral movement and ransomware to unpatched legacy networked devices.
- Savings on operational expenses through reduced technician trips onsite for service and maintenance.

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

or connect with us at engage@byos.io