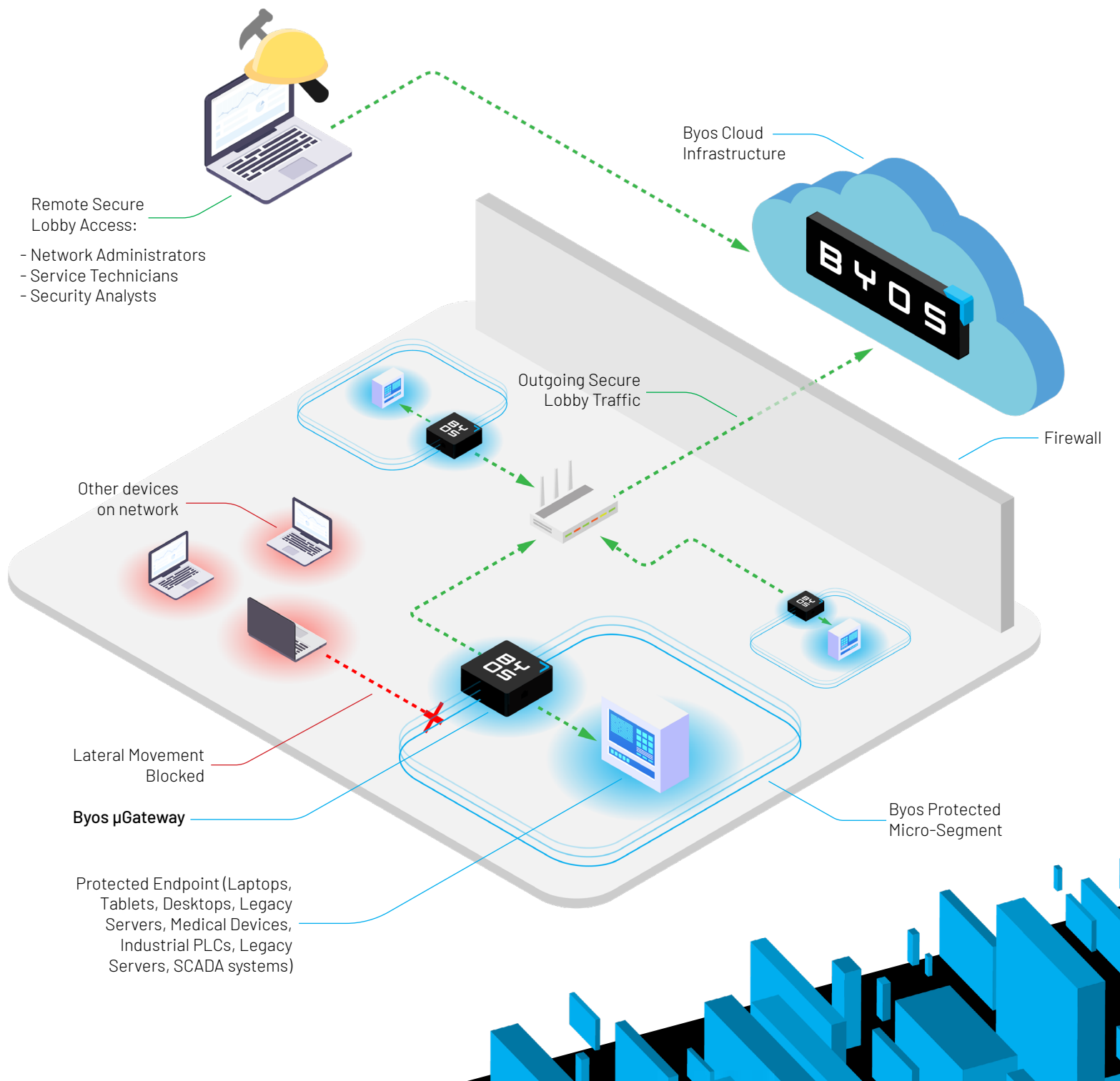


# Secure Lobby

The Secure Lobby feature allows for secure remote access to endpoints protected by the Byos  $\mu$ Gateway. Conventional remote access tools require opening up the perimeter, which adds unnecessary exposure risk to entire corporate networks. The Secure Lobby allows for monitoring, troubleshooting, updating, and patching remotely, without exposing internal endpoints to the internet.

The Secure Lobby creates a secure connection between the  $\mu$ Gateway and the Byos Management Console using an outbound connection, originating from inside of the corporate network perimeter, as to not interfere with local network configurations. This saves both Network Administrators and Service Technicians time when servicing Byos-protected endpoints remotely.



## How the Secure Lobby Works:

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  $\mu$ Gateway 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  $\mu$ Gateway allows traffic to and from the protected endpoint, allowing the user to interact with the endpoint directly.

### Benefits

- Securely prolong the life of IT infrastructure running legacy applications and unsupported OS that are not ready to be retired.
- Connecting previously air-gapped devices 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.
- Eliminated exposure of unpatched legacy networked devices to internal threats like lateral movement and ransomware.
- Reduced technician trips onsite for service and maintenance saving operational expenses.

## How is Byos $\mu$ Gateway different from other solutions?

- The Byos  $\mu$ Gateway facilitates secure Remote Monitoring, Updating, Patching, and Troubleshooting through its Secure Lobby, for improved efficiency without compromising on security.
- Managing remote endpoints is limited, cumbersome, and inefficient. Byos  $\mu$ Gateways can be managed centrally, allowing for comprehensive fleet management, simplified policy pushing, provisioning, and threat detection.
- The Byos  $\mu$ Gateway provides an entirely independent network security stack on top of providing basic networking functionality.
- The Byos  $\mu$ Gateway was built by our team of industry-vetted cybersecurity veterans with security in mind at every stage - secure development and continual testing, recurrent external peer reviews, a certified supply chain of components, and North American manufacturing.<sup>1</sup>

If you'd like to learn more about Byos, visit us at [byos.io](https://byos.io)

or connect with us at

[engage@byos.io](mailto:engage@byos.io)

1. For more information about why you should trust Byos, visit [byos.io/trust](https://byos.io/trust)