BYOS

Securing Industrial Control Networks in Manufacturing

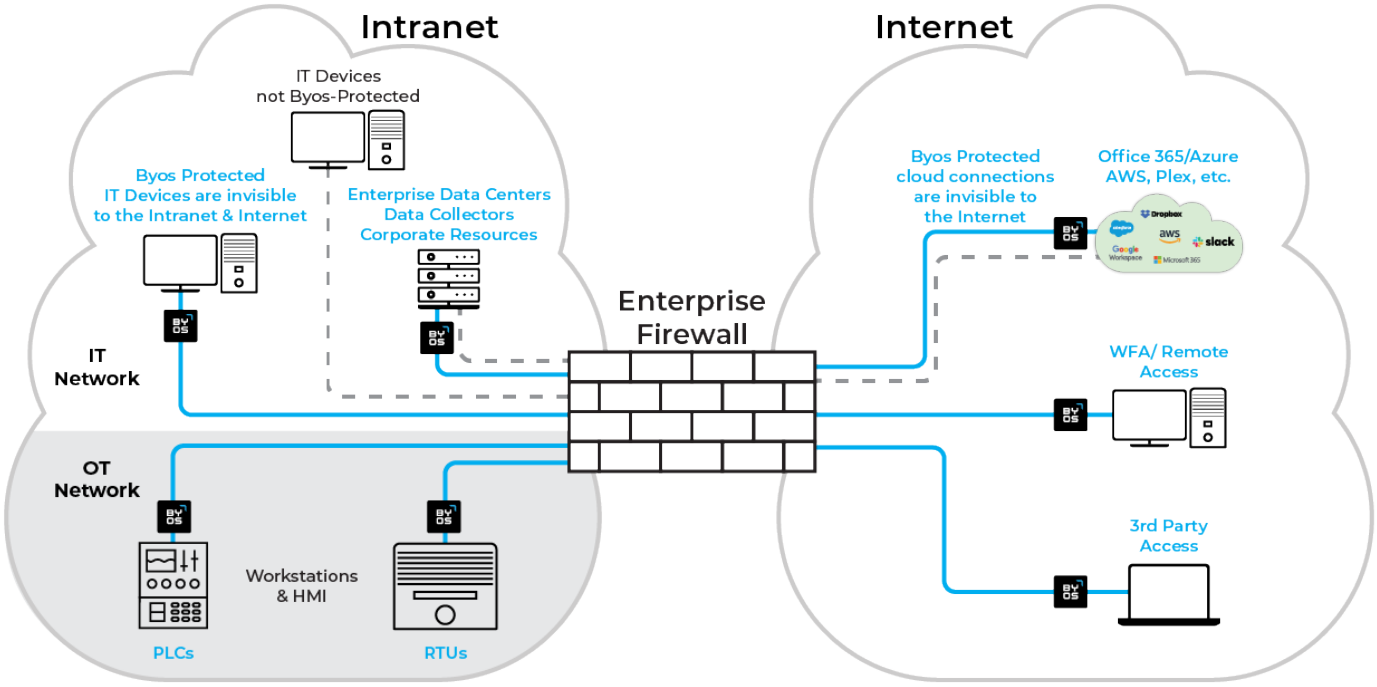
To reap the rewards of Industry 4.0 digital transformation, manufacturers are digitizing their data collection and real-time production visibility, while hardening the OT networks. But, networks supporting industrial control systems have cybersecurity requirements unlike any other industry. Legacy devices, hierarchical controls, proprietary protocols, a multitude of vendors & models, and the demands of OT that are different from IT make securing these networks especially challenging.

You recognize the advantages of having simple, consistent access to your entire ICS network regardless of location. Access to plant floor devices is growing at a faster rate than in any other industry. That includes external access by workers from home, vendors, and other third parties. Benefits are clear:

- Central data acquisition, monitoring & control
- More efficient, effective and proactive maintenance
- Analytics improve planning, maintenance & production scheduling

The Challenges Manufacturers Face in Securing their Networks

- Connecting these devices that cannot be secured makes them vulnerable to attack
- Security and cabling limitations meant that devices were connected in small, isolated networks, or not at all
- Legacy devices let bad actors move throughout the network with ease if even a single device is compromised
- Change in industrial technology is accelerating, resulting in even more complexity



Visibility Across a Worldwide Plant Infrastructure

Byos can make the enterprise IIoT network so that all the plant systems can be administered and secured as a single system. Manufacturers gain real-time visibility into the entire fleet of ICS devices from the Byos administrative console to monitor the security & connection status, including external access by vendors and other third parties. Manufacturing operations teams centralize, as appropriate.

Increase Productivity and Decrease Operational Technology Complexity

Plant Operations is complex enough to begin with. In the past, full control & visibility to devices distributed across geographically diverse plants, or even lines or zones within a plant, has only added to that complexity. Some devices simply can't be monitored or managed without physical or local network access.

Manufacturers are greatly simplifying how they secure their networks, and at the same time, increasing the visibility and security of all their IIoT devices. Byos' approach makes the OT network invisible to outsiders, while giving visibility and control to those who are identified as being authorized to access only those devices to which they are entitled.

Harden Your OT Network

Byos-protected devices are invisible to all unauthorized devices on the network. This protection ensures that your devices are only communicating with other credentialed and fully authorized devices. This core feature allows extremely limited access to be provided to third-parties so that they have access to ONLY the devices and users that need access, and only for specific periods of time and from specific geographies, and other specific parameters.

Byos' Management Console and Secure Lobby help plant floor operators, internal vendor support teams, and plant/IT/cybersecurity support to control and manage their fleet of Byos-protected IIoT devices. Byos enables:

- Real-time provisioning and policy-enforcement of thousands of devices from a centralized console
- Secure remote access to devices inside the Byos-cloaked network, without having to expose the network to the internet like other remote access technologies
- Connect your legacy controllers to improve efficiency without exposing them to the network and adding risk

Byos is unique because it makes the Factory Network Invisible to Outsiders

Byos combines network/endpoint security with ease of use into one solution that it is simple to deploy, manage, scale, without having to change the underlying network.

Benefits of Byos for OT and IT

- Byos is designed so that plant engineers perform day-to-day administration with little to no IT expertise, while remaining within the parameters set by global security policies
- Works over the existing enterprise network and internet without modification
- Extends the private, cloaked network to any Byos-protected device on the internet, but accessible ONLY from devices protected by Byos.
- Making all the devices invisible reduces lateral movement, discoverability, threat surface and security event logs.
- Leverages existing WAN/internet/cloud connections building upon fault-tolerance access to critical applications and resources

If you're looking for more visibility across your manufacturing operations, or looking to harden your OT network, request a demo here: byos.io/request-demo