USE CASE

Boosting Efficiency and Connectivity in Utilities

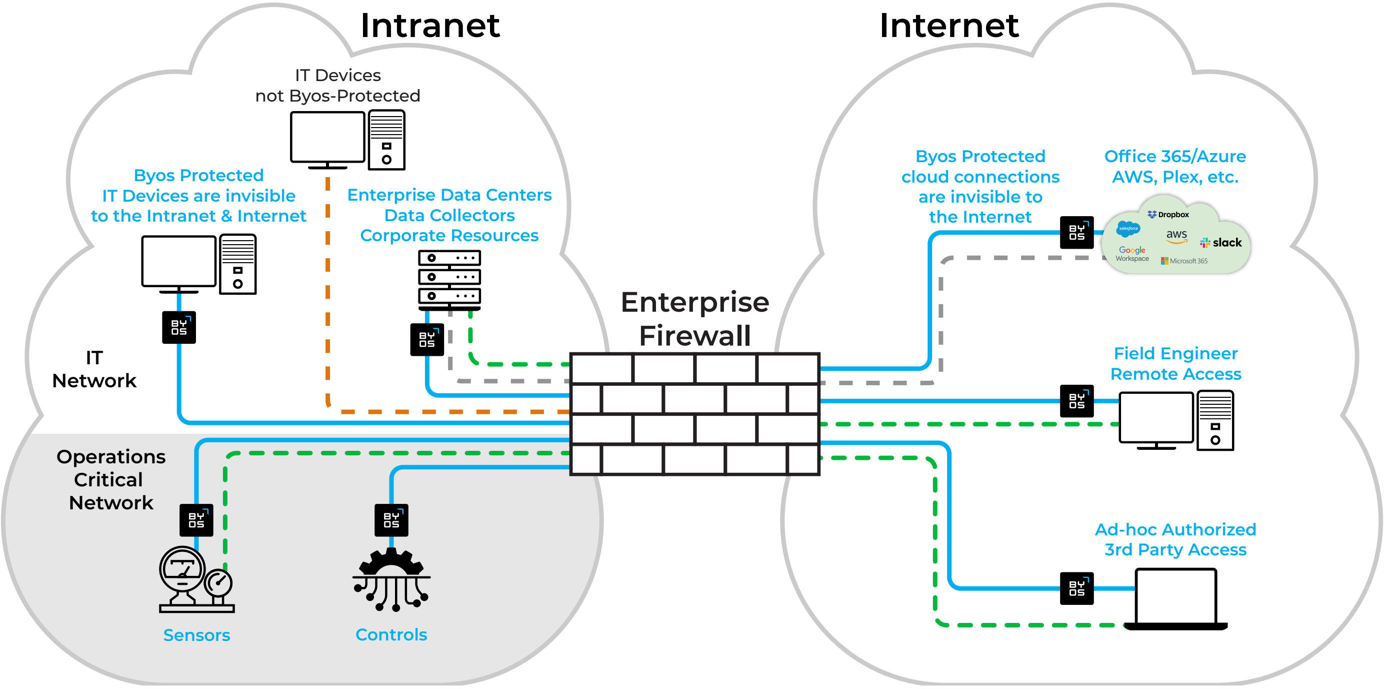
With the potential of Industry 4.0 digital transformation to dramatically improve real-time decision making and operational agility, utility providers are increasingly digitizing their data collection and real-time production visibility, while hardening their OT devices. But networks supporting utilities control systems have cybersecurity requirements unlike any other industry. Legacy machinery, hierarchical and proprietary protocols, a multitude of vendors & models, and the demands of the SCADA network that are different from IT make securing these networks especially challenging.

You need simple, consistent visibility and access to all devices on your network regardless of location. What if you could have that visibility and access even when you had taken them offline? As operational troubleshooting and maintenance moves outside your physical plant, it becomes more critical for your network to focus on:

- **Central data acquisition, monitoring & control**
- **More efficient, effective and proactive maintenance**
- **Improving analytics for better planning, maintenance & performance**

The Challenges Utilities Providers 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



Wireless Connectivity Boosts Utility Operator Efficiency

Byos unifies utility substations communications, enabling efficient administration and security through a single platform. Utility operators gain real-time visibility into networked devices, monitoring security, connection status, and third-party access. Byos offers significant value to utility providers by enabling wireless connectivity for traditionally hardwired components within their operations. This streamlines telemetry aggregation on legacy systems, allowing for faster data collection and analysis. As a result, providers can identify bottlenecks and inefficiencies more effectively, leading to increased operational efficiency. Furthermore, the reduction in wiring and associated maintenance costs contributes to direct cost savings. In essence, simplifying utility infrastructure while optimizing performance and reducing expenses.

BYOS

Increasing Remote Access while Decreasing System Complexity

Critical infrastructure operations are particularly complex. Cybersecurity technologies too often are only partially deployed. Each remote point of access becomes a potential attack vector that opens the door to wider access to the network. Byos simplifies security management with "plug-and-play" design that eliminates the need for multiple technologies. Byos' approach makes the operational network invisible to unauthorized access, minimizing the potential of a massive outage and impact if an intrusion occurs. And Byos' ease-of-use means that day-to-day administration can be performed by plant engineers without having to resort to a complex series of calls and escalations to perform, what should have been from the very start, operational tasks.

Harden Your OT Network

Byos-protected devices are invisible to all unauthorized entities. That kind of protection ensures that your network precisely limits communications to only credentialed and fully authorized entities. You give extremely limited access to third-parties so that it's ONLY for tthe devices and users that need access, and only for specific periods of time, and only from specific geographies, and other parameters.

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

- **Real-time provisioning and policy-enforcement of an unlimited number of devices from a centralized command**
- **Secure remote access to devices inside the Byos-cloaked network, without having to expose the network to the internet like other remote access technologies**
- **Legacy controllers to be connected to the network wirelessly so telemetry can be aggregated to improve efficiency, without exposing them to the network and adding risk**

Byos makes the network invisible to outsiders

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

Benefits of Byos for IT

- Byos is designed so that 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 infrastructure operations, or looking to harden your network, request a demo here: byos.io/request-demo