Enhancing Pharmaceutical OT Security with Byos Secure Networking Platform

WHITE PAPER

Protecting ICS, SCADA, PLCs, and MES Without System Replacement

Pharmaceutical manufacturing is one of the most critical and regulated environments globally, relying on a complex tapestry of operational technology (OT) systems such as ICS (Industrial Control Systems), SCADA (Supervisory Control and Data Acquisition), PLCs (Programmable Logic Controllers), and MES (Manufacturing Execution Systems). These systems drive vital production and control processes but can be notoriously difficult—or even impossible—to patch or secure directly due to vendor restrictions, legacy software, or operational requirements. This creates a pressing need for robust cybersecurity measures that can be layered onto existing infrastructure, meeting regulatory standards while minimizing disruption and cost.

Challenges of Securing Pharmaceutical OT

Pharmaceutical manufacturers typically operate with a blend of legacy and modern OT systems. Many ICS, SCADA, PLCs, and MES platforms in use today cannot be patched or directly secured due to:

- **Vendor Lock-in**: Original Equipment Manufacturers (OEMs) may not support security upgrades or may invalidate warranties if third-party modifications are made. This fact is accentuated by the acknowledgment that up to 35% of CISA's critical ICS vulnerability CVE's have no known patch or remediation available today.[1]
- **Operational Constraints**: The critical nature of the systems driving the pharmaceutical manufacturing and supply chain makes downtime or system modifications unacceptable - it can jeopardize product quality, safety, regulatory compliance, or even patient safety.
- **Legacy Limitations**: Older hardware and software lack modern security capabilities, making them susceptible to attacks such as zero-day's, ransomware, sensitive data exposure / exfiltration, and industrial sabotage.

Yet another challenge is the time and cost associated with building out new, modernized pharmaceutical manufacturing and supply chain systems. The cost of standing up a new manufacturing and supply chain environment can be as high as $2B and take 5-10 years. Expanding or retrofitting an existing factory can carry similar costs and time.[2] These constraints are prohibitive under the best of circumstances, making timely and cost-effective modernization of current infrastructure and supply chain investments the more logical approach.

Byos Secure Edge and Secure Cluster Edge: A Modern Security Overlay

Byos (Bring Your Own Security) Secure Edge and Secure Cluster Edge offer innovative solutions that balance security with ease of use to bridge these security gaps without requiring wholesale system replacement.

As a platform that combines Edge security and a software-defined overlay network, these technologies integrate seamlessly with legacy OT, providing a variety of key functionalities:

- **Endpoint Microsegmentation**
- **Network Obfuscation**
- **FIPS 140-2 Validated Encryption**
- **Targeted and Advanced Zero Trust functionality for OT**
- **Centralized control of OT systems via Byos Secure Lobby**

[1] https://www.csoonline.com/article/574409/many-ics-flaws-remain-unpatched-as-attacks-against-criticalinfrastructure-rise.html

[2] https://cdn.aglty.io/phrma/global/resources/import/pdfs/Setting%20Up%20A%20Pharmaceutical%20Manufacturing%20Process%20and%20Supply%20Chain%20A%20Complex%20and%20Lengthy%20Undertaking.pdf

1. Endpoint Microsegmentation

Microsegmentation is the process of isolating endpoints—such as PLCs, SCADA nodes, and MES servers— from each other and from the broader network. Byos Secure Edge and Secure Cluster Edge can be deployed at the network interface of each device or group of devices. This achieves:

- **Containment of Threats**: If a device is compromised, microsegmentation prevents adversaries from moving laterally to other parts of the OT network, or achieving privilege escalation.
- **Granular Policy Enforcement**: Access policies can be defined on a per-device basis, limiting communication to only what is
- operationally necessary, supporting GMP-compliant workflows.
- **Protection of Unpatchable Devices**: Vulnerable endpoints are shielded from attack vectors without requiring intrusive software changes or downtime.

While **ISA-99/ISE 62443** prescribe segmenting networks into zones and conduits; endpoint microsegmentation differs from network segmentation in the way a network is protected. In network segmentation, each segment is protected as its own mini-network, and administrators create policies to define how traffic can flow from one segment to another. Users, endpoints, and network traffic already within an organization's perimeter are automatically trusted, so protecting the enterprise's system from the world beyond it becomes the priority. This approach has become less secure over time, and is currently being routinely exploited, per data obtained from a recent report of the Director of National Intelligence: Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023-April 2024.[3] Byos goes well beyond the zone and conduit approach to apply security closer to where it matters most - the endpoint. Unlike traditional segmentation, which assumes trust inside the perimeter, endpoint microsegmentation enforces granular trust boundaries around individual assets.

Benefits of Endpoint Microsegmentation

- **Enhanced Security**: By isolating endpoints, microsegmentation limits the spread of malware and other threats. Endpoint microsegmentation and network obfuscation also buys down risks associated with IT-OT convergence.
- **Improved control of traffic flows**: It provides granular visibility into network traffic, allowing for better monitoring and threat detection. The FDA observes that network visibility is a significant challenge in today's medical OT networks due to scale and operators not knowing "what" devices / firmware might be communicating on a given network.[4]
- **Compliance**: Microsegmentation helps meet regulatory requirements by enforcing strict access controls and security policies, including FDA 21 CFR Part 11,PHI / HIPPA, and good manufacturing processes (GMP) guidelines for active pharmaceutical ingredients (APIs).
- **Flexibility**: It allows for dynamic adjustments to security policies based on changing threats, network conditions or facility expansions.

Byos maintains logical separation between production, management, and update networks. Critical infrastructure remains segmented from corporate IT and has a minimal attack surface—exactly what CISA recommends for control system isolation.

2. Network Obfuscation

Network obfuscation by Byos works by making OT devices effectively invisible to unauthorized users and automated network scans. This is realized through a combination of:

- **Stealth Networking**: Devices behind Byos Secure Edge / Secure Cluster Edge are not discoverable through standard network enumeration techniques, reducing visibility to attackers. This functionality was recently demonstrated at **Defend The Airport 2025**. This two-day event featured an NSA Cyber SME demonstrating how an advanced adversary compromises a critical production network. The attacker implanted a variety of zero-day compromises on the network, and demonstrated how "living off the land" enables adversaries to achieve persistence on a targeted network to attack at will.

  Byos was the only system demonstrated at this event that not only stopped the adversary from sending a C2 "kill shot" on the infected network but prevented the attacker from gaining any intelligence about the nature of Byos defensive capabilities at the SEIM, attack surface analysis, and network monitoring layer of the airport network (via Byos obfuscation technologies).
- **Dynamic Addressing**: Byos randomizes network parameters, filters unsolicited traffic, and renders endpoints unreachable from outside the authorized perimeter—dramatically reducing their exposure to reconnaissance-based attacks.

This dramatically reduces the likelihood of opportunistic attacks or targeted exploits by making the OT environment opaque to outsiders.

[3] https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

[4] https://www.fda.gov/media/187159/download?attachment

3. FIPS 140-2 Validated Encryption

Encryption is a cornerstone of modern cybersecurity, and FIPS 140-2 is the gold standard for cryptographic modules in regulated industries like pharmaceuticals. Many OT devices do not meet the FIPS 140-2 standard today, because they were not designed to address emerging security requirements. Byos Secure Edge and Secure Cluster Edge provide:

- **End-to-End Data Protection**: All data in transit between OT devices and control systems are encrypted to FIPS 140-2 standards, ensuring confidentiality and integrity.
- **Regulatory Compliance**: Adhering to FIPS 140-2 helps meet HIPPA, NIST, and ISA security requirements for critical infrastructure, facilitating audits and compliance reporting.
- **Extended coverage**: Many OT devices are not FIPS compliant - Byos instantly adds FIPS-validated security. Byos brings NSA 2.0 quantum-resistant encryption to legacy devices without software changes from day 1.

4. Target and Advanced Zero Trust Functionality for Endpoints

In alignment with FDA recommendations and NIST SP 800-207, Byos delivers granular Zero Trust capabilities across legacy and modern OT. Byos solutions extend Zero Trust to remote Wi-Fi connections, and support a number of target level and advanced Zero Trust Architecture (ZTA) requirements.

Key features include:

- **Rapid user and system inventory mapping.**
- **Establishes a basic set of user attributes for authentication and authorization as well as adding / updating attributes within the solution.**
- **Enables conditional user access / just-in-time access / just enough administration methods.**
- **Enables dynamic access decision making down to the specific endpoint / microsegment.**
- **Enables enclave / Denied, Disrupted, Intermittent and Low-Bandwidth (DDIL) identity, credential, and access management.**
- **Provides multi-factor authentication for users and machines in a single application.**
- **Ensures privileged access management down to the endpoint / microsegment.**
- **Meets interoperability standards for data rights management and protection down to the endpoint / microsegment**

Byos delivers these ZTA benefits at a low cost per endpoint with the flexibility to scale to an entire enterprise with no disruption to continuing operations.

5. Regulatory Compliance Without Replacement

Both NIST (National Institute of Standards and Technology) and ISA (International Society of Automation) provide detailed frameworks for securing OT environments, including:

- **NIST SP 800-82**: Guide to Industrial Control Systems Security
- **EISA/IEC 62443**: Security for Industrial Automation and Control Systems

Byos Secure Edge and Secure Cluster Edge enable pharmaceutical manufacturers to meet these requirements by adding zero-trust functionality, segmentation, and encryption to existing systems—without having to rip and replace critical OT assets.

6. Cost Savings and Engineering Effort Reduction

By deploying Byos solutions as an overlay, pharmaceutical companies benefit from:

- **Reducing Immediate Costly System Replacements**: Protect end of life systems and high value assets until budgets allow their replacement, and secure any asset where vulnerabilities might remain "forever days", all without disrupting validated systems or triggering new FDA submissions.
- **Minimized Engineering Overhead**: Rapid deployment and minimal need for redesign or rearchitecture of existing systems.
- **Streamlined Compliance**: Built-in logging, policy enforcement, and cryptographic controls reduce the labor required to document and maintain regulatory compliance.
- **Low-Risk Path to implementation**: Byos solutions are "plug and play" on most networks and devices, reducing the need to re-architect these production environments. Since Byos solutions are data-agnostic, time associated with deconflicting interoperability challenges across disparate OT products from multiple vendors (PLC's, MES, SCADA, etc.) is also eliminated.
- **Balancing security with usability**: modern security solutions are only as effective as their ease of use. Human error remains the greatest threat to the cybersecurity posture of any network. The Engineers at Byos know this, and have designed a system that eliminates the kind of technical debt associated with many modern alternatives.

Conclusion

Byos Secure Edge and Secure Cluster Edge empower pharmaceutical companies to protect their most vulnerable operational technologies—ICS, SCADA, PLCs, and MES—even when those systems cannot be patched or directly secured by their OEMs. With endpoint microsegmentation, network obfuscation, and FIPS 140-2 encryption, Byos delivers the layered security and regulatory compliance demanded by today's threat landscape and regulatory climate. Most importantly, they do so in a way that preserves existing investments, reduces costs, and minimizes engineering complexity—enabling secure, compliant, and resilient pharmaceutical manufacturing operations.

For more information or to schedule a demo, please contact:

David Stephens
VP of Sales Public Sector and Strategic Accounts
david@byos.io
571-437-1111