Why Byos Solutions are the Best Defense Against Critical OT Vulnerabilities in Manufacturing

BYOS

WHITE PAPER

Abstract

The recently published Palo Alto-Siemens whitepaper highlights critical cybersecurity vulnerabilities within operational technology (OT) environments, emphasizing the growing risks faced by the manufacturing sector. As industrial systems become increasingly connected, traditional security approaches fail to provide sufficient protection against sophisticated cyber threats. Byos (Bring Your Own Security) offers a paradigm shift in securing OT environments by providing a microsegmentation and Zero Trust architecture that protects connected assets at the endpoint level. This whitepaper explores how Byos solutions directly address the vulnerabilities flagged in the Palo Alto-Siemens report, offering a scalable, resilient, and proactive defense against cyberattacks in manufacturing and other industrial sectors.

Introduction

Cybersecurity threats targeting Industrial Control Systems (ICS) and OT networks have escalated in recent years. The Palo Alto-Siemens whitepaper highlights the increasing attack surface of manufacturing systems due to IT/OT convergence, legacy device vulnerabilities, and lack of network segmentation. Traditional perimeter-based security models are insufficient to protect against modern attack vectors, necessitating a more granular, endpoint-centric security approach. Conventional flat networks in industrial environments enable lateral movement for attackers, further increasing the potential impact of a breach.

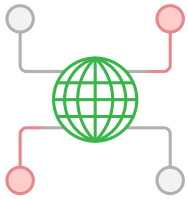
Byos provides a game-changing security architecture that isolates endpoints from threats while allowing secure connectivity. This whitepaper examines why Byos solutions are the best choice to mitigate the risks identified in the recent cybersecurity report.

Key OT Vulnerabilities Identified in the Palo Alto-Siemens Whitepaper

The whitepaper outlines several critical security risks in OT environments, including:

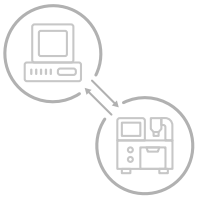
- **Legacy Systems with Unpatched Vulnerabilities**

Many OT devices run outdated operating systems with known security flaws that cannot be patched due to operational constraints. Compromised third-party software or hardware components can introduce hidden vulnerabilities into OT environments.



- **Insecure Remote Access**

The rise of remote monitoring and maintenance has introduced attack vectors through poorly secured VPNs and remote desktop connections.



- **Convergence of IT and OT Networks**

Increased connectivity between IT and OT systems expands the attack surface, exposing industrial processes to IT threats, including ransomware and data exfiltration.

How Byos Solutions Directly Address These Vulnerabilities

1. Zero Trust Network Access (ZTNA) for OT Environments

Byos implements a Zero Trust model where all connections must be explicitly verified before access is granted. This ensures:

- **Strict access control: Only authorized devices and users can communicate with OT assets.**
- **No implicit trust: Every connection undergoes rigorous authentication, mitigating risks from compromised credentials.**

2. Secure Remote Access Without VPN Exposure

Traditional VPNs create a broad attack surface by exposing networks to unauthorized access. Byos eliminates VPN vulnerabilities by:

- **Providing agent-based, device-level tunneling: Secure, encrypted access to specific OT assets without internet exposure and without exposing the entire network.**
- **Reduces risks from compromised third-party software or hardware: Only verified, authenticated connections can be established between third-party components and OT environments.**

3. Protection for Legacy Systems Without Patching

Since many industrial devices cannot be updated due to operational constraints, Byos provides an overlay security layer that:

- **Prevents exploitation of known vulnerabilities: Even unpatched devices remain secure, extending the operational life of older equipment**
- **Blocks unauthorized access: Legacy OT assets are protected from external threats without modifying existing infrastructure.**

Advantages of Byos Over Traditional OT Security Solutions

Traditional OT security solutions rely on perimeter defenses, VLAN segmentation, and role-based access controls—approaches that are no longer sufficient against modern cyber threats. Byos offers a lightweight, scalable alternative that provides security at the endpoint level without introducing operational complexities.

Feature	Traditional OT Security	Byos Solution
Network Segmentation	VLANs & Firewalls	Endpoint-Level Microsegmentation
Access Control	Role-Based Access	Zero Trust Network Access
Remote Access Security	VPN-Based	Secure, Isolated Tunneling
Patch Management	Requires Regular Patching	No Patching Required
Lateral Movement Prevention	Limited Effectiveness	Full Isolation of Endpoints
Deployment Complexity	High – Agent Based	- Lightweight - No Agents

Network Segmentation : The Modernized Approach

The cybersecurity risks outlined in the Palo Alto-Siemens whitepaper underscore the urgent need for a modernized security approach in OT environments. Traditional security models are no longer sufficient to counter the sophisticated threats targeting manufacturing systems. Byos solutions provide a comprehensive, proactive security framework that:

- **Prevents lateral movement within OT networks**
- **Secures legacy systems without requiring disruptive patching**
- **Enables safe remote access without exposing networks**

By implementing Byos, manufacturing companies can significantly enhance their cybersecurity posture, ensuring the resilience of industrial operations against evolving cyber threats.

Contact Byos today

For organizations looking to strengthen their OT security, adopting Byos is the most cost-effective yet powerful way to mitigate risks and safeguard critical infrastructure. Contact Byos at byos.io or David Stephens: david.stephens@byos.io, 571-437-1111 today to learn more about how microsegmentation and Zero Trust security can transform your cybersecurity strategy.