# Byos as a Strategic Enabler for OT Asset Inventory Guidance

WHITE PAPER

## Executive Summary

Organizations modernizing their OT cybersecurity face a common challenge: asset inventories are incomplete, inconsistent, or outdated. Without trusted visibility into what's connected, operators struggle with risk assessments, segmentation, and compliance.

The newly released Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators (the Guide) establishes a maturity-oriented framework for building accurate, actionable inventories. It emphasizes governance, taxonomy, lifecycle management, and risk-based use.

Byos Secure Edge Platform directly enables each stage of this framework. Byos delivers:

- Secure real-time data flow and asset visibility for decision-making, improved resilience, and unlocking greater operational efficiency
- Governed access and lifecycle integration aligned with change management processes.
- Actionable intelligence through risk tagging, vulnerability prioritization, and ability to export telemetry and metadata from Byos to SIEMs, CMDBs, or risk platforms.

The result: A trustworthy, real-time OT asset inventory that supports segmentation, compliance, and resilient operations. Byos doesn't just document assets—it operationalizes the Guide's principles, helping owners and operators accelerate maturity while maintaining safety and uptime.

## 1. Background: The Guide's Intent and Principles

The Guide mandates that asset inventory isn't merely a registry—it must:

- Be governed with clear scope and role assignments.
- Capture key asset attributes (protocols, ports/services, IP, MAC, manufacturer, criticality, etc.).
- Be organized using functional and risk-based taxonomies (e.g., Zones & Conduits per ISA/IEC 62443).
- Be centrally stored, protected, and integrated with risk and operations systems.
- Support lifecycle change management (onboard, operate, update, retire).
- Be actionable: used for vulnerability prioritization, segmentation, secure maintenance, and continuous improvement.

## 2. Byos' Core Capabilities Mapped to the Guide

***The Foundations for OT Cybersecurity: Asset Inventory Guidance*** defines six core principles for building and using an effective asset inventory. Byos directly supports each principle, turning guidance into operational practice.

### A. Governance, Scope & Role Management

**What the Guide Requires**: Clear ownership, scope definition, and role-based control over the asset inventory.

How Byos Helps: The Byos Management Console provides granular, role-based privileges for security, operations, and vendor staff. Flexible tagging (sites, zones, cells) ensures scope is clearly defined and aligned to organizational responsibilities.

**Outcome**: A governed inventory that is trustworthy, traceable, and aligned to enterprise ownership models.

### B. Asset Discovery & Attribute Collection

**What the Guide Requires**: Capture essential asset attributes such as IP, MAC, services, protocols, and criticality.

How Byos Helps: Byos automatically discovers assets at the NIC, collecting telemetry like IP/MAC, ports, VLANs, and communication flows. Metadata enrichment adds context such as role, owner, and location. Passive inference identifies manufacturer, model, and OS.

**Outcome**: A complete, real-time asset record that stays current without manual effort.

### C. Taxonomy, Segmentation & Visualization

**What the Guide Requires**: Organize assets by function and risk (e.g., ISA/IEC 62443 Zones & Conduits).

How Byos Helps: Zones are enforced directly at the device NIC, while conduits are defined as explicit allow-lists. Flow logs and visualizations provide evidence that segmentation matches design intent.

**Outcome**: Accurate, verifiable enforcement of segmentation that can be demonstrated to auditors and operators alike.

### D. Central Management & Integration

**What the Guide Requires**: A secure, centralized inventory that integrates with governance and risk systems.

How Byos Helps: Byos enforces role-based access and encrypts data in motion, with the Byos Management Console enabling admins to centralize policy enforcement and telemetry. It exports to SIEMs, CMDBs, or risk platforms to act as the authoritative source of record.

**Outcome**: A protected, enterprise-grade inventory that becomes actionable across governance, compliance, and monitoring workflows.

### E. Lifecycle & Change Management

**What the Guide Requires**: Inventories must adapt to onboarding, operation, maintenance, and retirement stages.

How Byos Helps: Byos integrates with CMDBs to automate updates whenever assets change state. Maintenance sessions are controlled and logged through Byos Management Console.

**Outcome**: Inventories that stay synchronized with real-world operations, reducing drift and ensuring lifecycle accuracy.

### F. Actionable Intelligence & Risk-Based Controls

**What the Guide Requires**: Inventories must inform vulnerability prioritization and access controls.

How Byos Helps: Byos tags assets with KEV/CVE identifiers, maps telemetry to MITRE ATT&CK for ICS, and dynamically adjusts policies to isolate high-risk assets.

**Outcome**: Inventories that directly drive defense—transforming raw data into real-time protection for critical OT assets.

## 3. Design Benefits: What Byos Brings

| Guide Objective | How Byos Delivers | Practical Benefits |
|---|---|---|
| **Accurate mapping of communication** | First-hop isolation + flow logging (device-level packet visibility) | Clear, verifiable records of how assets communicate, reducing blind spots. |
| **Controlled segmentation during mitigation** | Enforces allow-only policies at the NIC | Prevents lateral spread of threats while patches or fixes are delayed. |
| **Audited remote access** | Secure Lobby enables logged, least-privilege maintenance sessions. | Vendors and staff gain controlled access, with full accountability. |
| **Scalable taxonomy validation** | Tags, visualizations, and flows allow for continuous verification of zone/conduit definitions. | Ensures that logical architectures match real-world traffic patterns. |
| **Aligns authoritative asset information** | Metadata integration with CMDB/CMMS anchors Byos data in enterprise-grade inventory. | Single source of truth for asset data across IT, OT, and governance systems. |
| **Supports risk-driven prioritization** | CVE/KEV tagging and ATT&CK for ICS mapping | Segmentation policies adapt dynamically to protect high-risk or vulnerable assets. |

## 4. Implementation Roadmap (Guide-Aligned)

| Phase | Byos Implementation Action | Guide Alignment | Value |
|---|---|---|---|
| **Phase 1: Foundation** | Deploy Byos; enroll representative OT assets across zones; tag core attributes (role, criticality, location, ownership). | Steps 1 & 2: Define scope/ governance; identify assets and collect attributes. | Builds confidence that the asset database is accurate, complete, and structured for segmentation |
| **Phase 2: Taxonomy and Enforcement** | Work with OT/ICS risk teams to define Zones & Conduits per ISA/IEC 62443 and enforce policies via Byos. | Step 3: Create taxonomy; organize zones & conduits; validate relationships. | Provides operators with clear visibility and assurance that segmentation matches both design and reality. |
| **Phase 3: Integration** | Export telemetry and metadata from Byos to SIEMs, CMDBs, or risk platforms. | Step 4: Manage and collect data; centralize and secure the inventory. | Eliminates duplication, ensures inventories stay current, and embeds visibility into enterprise workflows. |
| **Phase 4: Risk Coordination** | Correlate asset records with vulnerability feeds (CVE/ KEV) and ATT&CK for ICS techniques, dynamically adjust Byos policies to mitigate risks. | Step 5: Use inventory for risk prioritization; strengthen architecture with segmentation, access control. | Protects vulnerable OT assets dynamically—without waiting for patch cycles |
| **Phase 5: Governance & Continuous Maturity** | Embed Byos into change management; schedule taxonomy and flow reviews. | Lifecycle management: update inventory on asset changes; continuous improvement. | Creates a sustainable model where inventory, segmentation, and security controls remain aligned over time. |

## 5. Summary & Strategic Value

The Foundations for OT Cybersecurity: Asset Inventory Guidance makes clear that an inventory is not just a list of devices—it is the foundation for secure operations, segmentation, and risk management.

Byos operationalizes this vision by combining automated discovery, policy-driven segmentation, governed remote access, and lifecycle integration into a single platform. With Byos, organizations can move beyond static inventories toward a living, real-time record of assets and their behaviors, backed by controls that reduce both risk and operational complexity.

### Key Takeaways

- Byos enforces ISA/IEC 62443 Zones & Conduits directly at the device level, providing immediate segmentation benefits.
- Telemetry-driven validation ensures inventories are both accurate and actionable, with clear visibility into relationships between assets.
- Risk-based adjustments (e.g., isolating vulnerable or unpatched devices) protect operations without requiring downtime.
- Integration with SIEM and CMDB systems makes asset data usable across governance, compliance, and incident response workflows.

### Strategic Outcome

Building a secure OT Asset Inventory with Byos delivers more than compliance—it creates a resilient, adaptive architecture where real-time asset inventories actively strengthen security. This positions organizations to significantly reduce risk and complexity today while building a sustainable path toward higher OT cybersecurity maturity tomorrow.