How Microsegmentation Enhances OT Security: Insights for Network Security Architects

Microsegmentation · Operational Technology

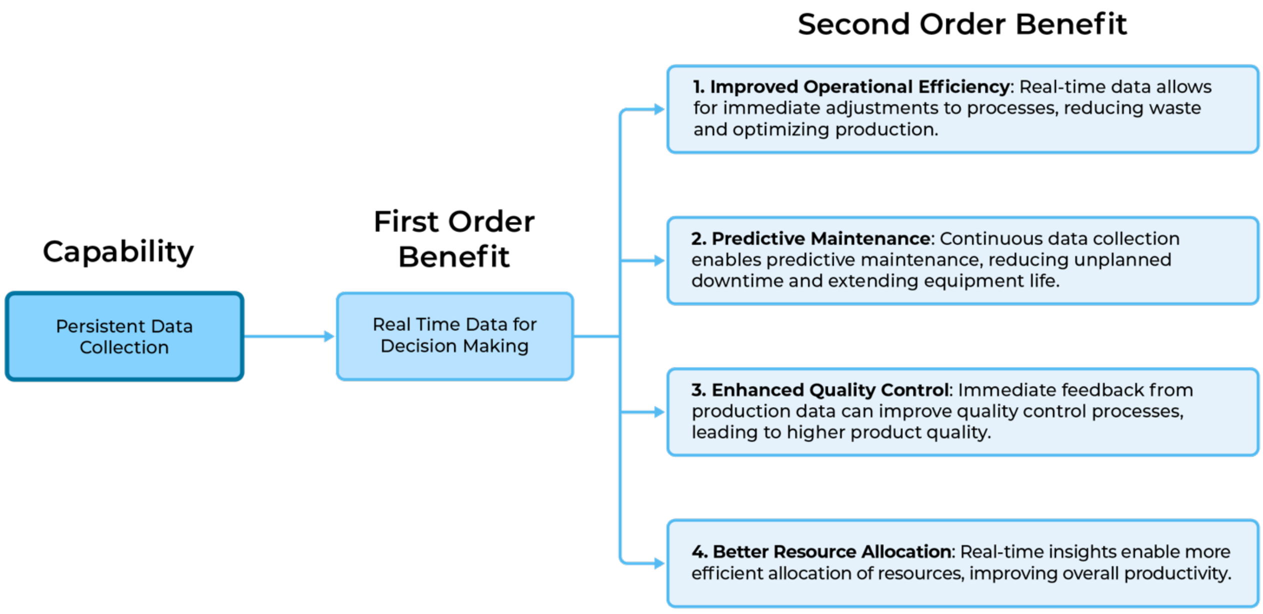
In today's industrial landscape, the convergence of Operational Technology (OT) and Information Technology (IT) has introduced both efficiency and connectivity. However, it also brings new cybersecurity challenges. For a Network Security Architect looking to safeguard OT environments, and microsegmentation is a powerful tool in achieving this. This article explores how the four key capabilities of microsegmentation, particularly with the design of Byos' microsegmentation platform —enables wireless connectivity for industrial devices, eliminates lateral movement exposure, remote management of legacy controllers, and increased manufacturing flexibility— delivers essential benefits for OT security.

1. Increased Manufacturing Flexibility: Data Collection for Adapting Securely to Change

The ability of microsegmentation to provide increased manufacturing flexibility is crucial for OT environments that need to adapt to changing production demands. This flexibility allows for secure adjustments to network configurations without compromising security.

Key Benefits:

- **First Order Benefit: Operational Agility**
  Microsegmentation enables organizations to quickly and securely reconfigure their networks to meet new production requirements, ensuring that security keeps pace with change.
- **Second Order Benefit: Support for Innovation**
  Increased flexibility encourages innovation within the OT environment, allowing teams to experiment with new processes and technologies while maintaining robust security controls.
- **Third Order Benefit: Competitive Advantage**
  The ability to adapt quickly to market demands without sacrificing security provides organizations with a significant competitive edge, enhancing their position in the industry.


Capability
Persistent Data Collection
First Order Benefit
Real Time Data for Decision Making
Second Order Benefit

1. Improved Operational Efficiency: Real-time data allows for immediate adjustments to processes, reducing waste and optimizing production.

2. Predictive Maintenance: Continuous data collection enables predictive maintenance, reducing unplanned downtime and extending equipment life.

3. Enhanced Quality Control: Immediate feedback from production data can improve quality control processes, leading to higher product quality.

4. Better Resource Allocation: Real-time insights enable more efficient allocation of resources, improving overall productivity.

2. Granular Third Party Access and Remote Management of Legacy Controllers: Securing Critical

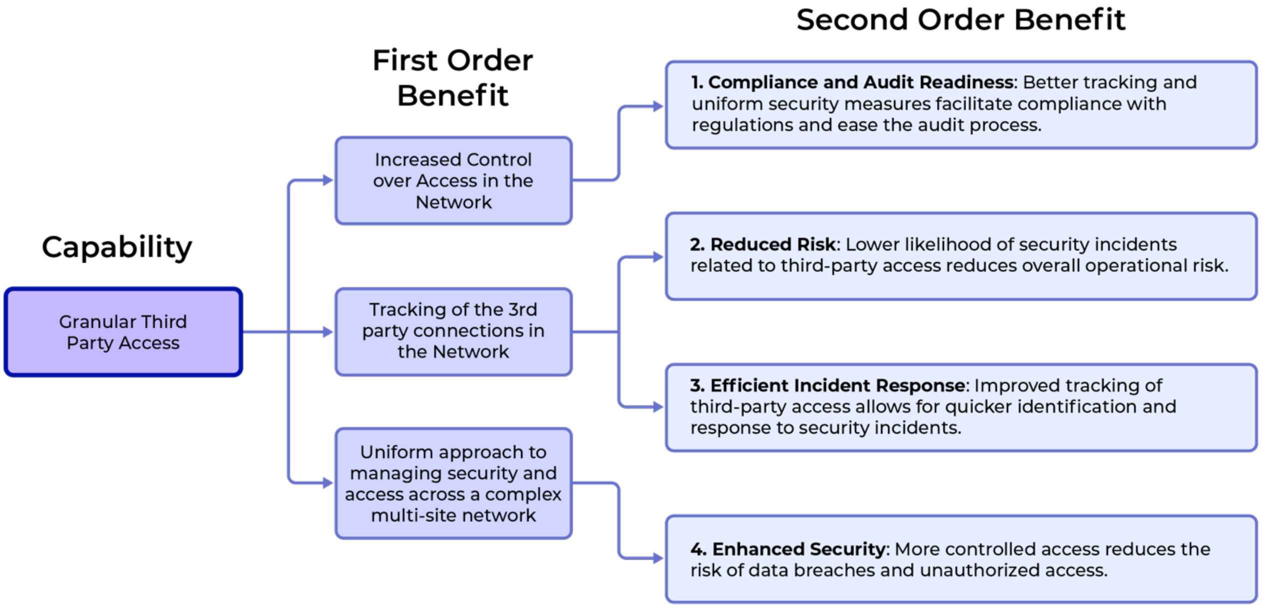
Assets

Microsegmentation helps enable granular third-party access, allowing precise control over the access and permissions granted to external vendors, contractors, or partners. This capability is crucial in OT environments where third parties often need access to specific parts of the network for maintenance, monitoring, or other services. Byos' microsegmentation platform is additionally designed to enable the remote management of legacy controllers, which are often critical to OT operations but may not be designed with modern security in mind. This capability allows organizations to secure these older systems without requiring expensive upgrades.

Key Benefits:

- **First Order Benefit: Controlled Access to Critical Systems**
  By limiting third-party access to only the necessary segments of the network, microsegmentation minimizes the risk of unauthorized access to sensitive areas.
- **Second Order Benefit: Reduced Exposure to External Threats**
  Granular control over third-party access reduces the potential attack vectors that external parties could introduce, thereby strengthening the overall security posture of the OT environment. The ability to manage legacy controllers remotely reduces the need for on-site intervention, streamlining operations and improving overall efficiency while the greatly reducing the risk when connecting these devices to the network.
- **Third Order Benefit: Improved Vendor Management and Compliance**
  With detailed access controls, organizations can better manage vendor relationships and ensure compliance with regulatory

requirements regarding third-party access and data handling.


Capability
Granular Third Party Access
First Order Benefit
Increased Control over Access in the Network
Tracking of the 3rd party connections in the Network
Uniform approach to managing security and access across a complex multi-site network
Second Order Benefit

1. Compliance and Audit Readiness: Better tracking and uniform security measures facilitate compliance with regulations and ease the audit process.

2. Reduced Risk: Lower likelihood of security incidents related to third-party access reduces overall operational risk.

3. Efficient Incident Response: Improved tracking of third-party access allows for quicker identification and response to security incidents.

4. Enhanced Security: More controlled access reduces the risk of data breaches and unauthorized access.

3. Eliminating Lateral Movement Exposure: Strengthening OT Security

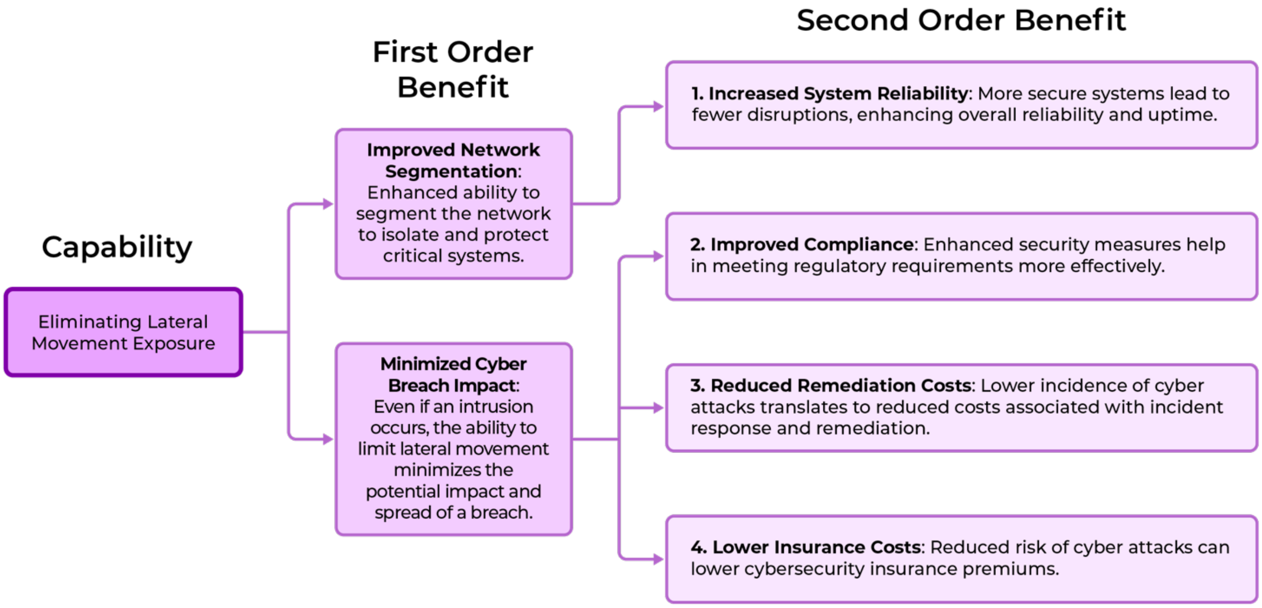
One of the most critical capabilities of microsegmentation is its ability to eliminate lateral movement exposure within OT networks. By segmenting the network into isolated zones, microsegmentation prevents attackers from moving freely across the network if they breach one part of it.

Key Benefits:

- **First Order Benefit: Enhanced Network Security**
  By containing potential threats within a single segment, microsegmentation significantly reduces the attack surface and limits the damage that can be done by a breach.
- **Second Order Benefit: Faster Incident Response**
  With lateral movement restricted, security teams can more quickly

identify and contain breaches, leading to faster incident resolution.

- **Third Order Benefit: Long-Term Risk Reduction**
  Preventing lateral movement reduces the long-term risk of widespread network compromise, contributing to the overall resilience of the OT environment.


Capability
Eliminating Lateral Movement Exposure
First Order Benefit
Improved Network Segmentation: Enhanced ability to segment the network to isolate and protect critical systems.
Minimized Cyber Breach Impact: Even if an intrusion occurs, the ability to limit lateral movement minimizes the potential impact and spread of a breach.
Second Order Benefit
1. Increased System Reliability: More secure systems lead to fewer disruptions, enhancing overall reliability and uptime.
2. Improved Compliance: Enhanced security measures help in meeting regulatory requirements more effectively.
3. Reduced Remediation Costs: Lower incidence of cyber attacks translates to reduced costs associated with incident response and remediation.
4. Lower Insurance Costs: Reduced risk of cyber attacks can lower cybersecurity insurance premiums.

4. Wireless Connectivity for Industrial Devices: Secure and Scalable Networking

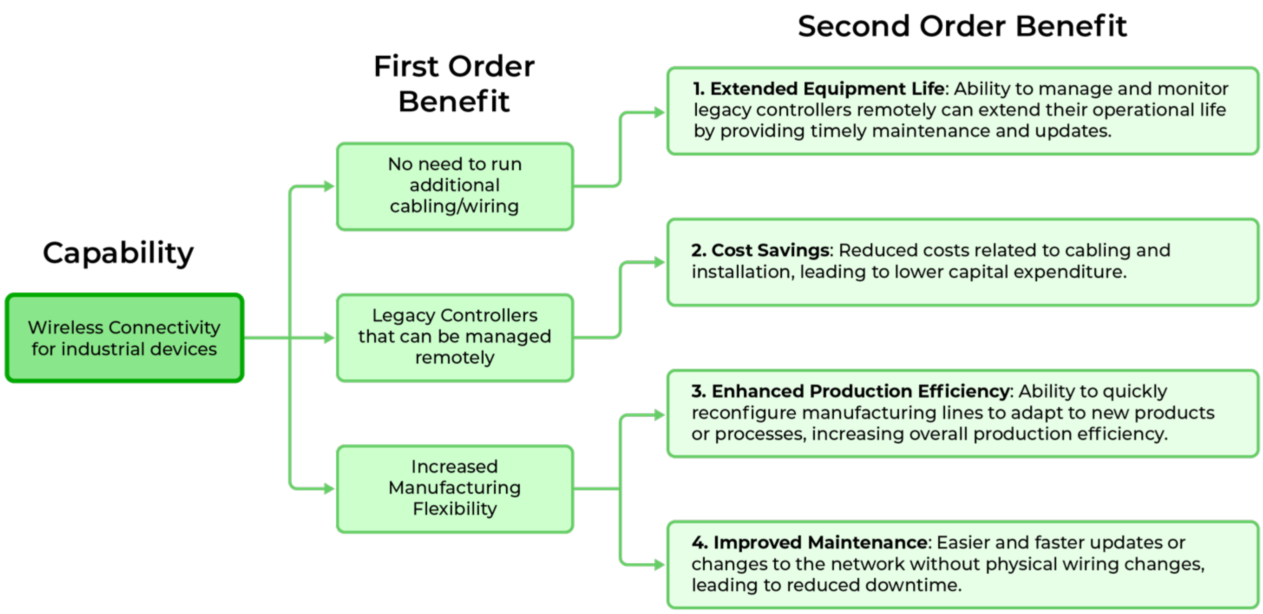
Microsegmentation enables wireless connectivity for industrial devices, allowing for more flexible and scalable network designs without compromising security. This capability eliminates the need for additional cabling, which simplifies the deployment of industrial devices within OT environments.

Key Benefits:

- **First Order Benefit: Simplified Network Infrastructure**
  Removing the requirement for extensive cabling reduces network

complexity, making it easier to deploy and manage devices securely.

- **Second Order Benefit: Extended Equipment Life**
  Wireless connectivity, backed by microsegmentation, facilitates remote monitoring and management of industrial devices, extending their operational life while maintaining security.
- **Third Order Benefit: Scalability and Cost Efficiency**
  The ability to easily scale the network by adding new devices without extensive physical infrastructure leads to cost savings and greater operational flexibility.


Capability
Wireless Connectivity for industrial devices
First Order Benefit
No need to run additional cabling/wiring
Legacy Controllers that can be managed remotely
Increased Manufacturing Flexibility
Second Order Benefit

1. **Extended Equipment Life**: Ability to manage and monitor legacy controllers remotely can extend their operational life by providing timely maintenance and updates.

2. **Cost Savings**: Reduced costs related to cabling and installation, leading to lower capital expenditure.

3. **Enhanced Production Efficiency**: Ability to quickly reconfigure manufacturing lines to adapt to new products or processes, increasing overall production efficiency.

4. **Improved Maintenance**: Easier and faster updates or changes to the network without physical wiring changes, leading to reduced downtime.

management of legacy controllers, and increased manufacturing flexibility—are essential in achieving this balance. By leveraging these capabilities, organizations can ensure their OT environments are secure, adaptable, and prepared for the future.

Byos' microsegmentation platform was designed with the input and real-world challenges of Network Security Architects in mind, to create a uniform approach for managing security and access across a complex network of disparate devices. It eliminates internet exposure to production devices, protects against ransomware attacks, and streamlines remote access in a multi-site operation.

Byos' Microsegmentation Solution has three main components:

1) The **Secure Gateway Edge™** ensures secure, reliable access to machine data through microsegmentation and granular access controls, with full compatibility for often neglected legacy devices. Microsegmenting assets ensures that the blast radius of any attack is contained to the smallest possible attack surface.

2) The **Byos Secure Lobby™** is a Software Defined Network (SDN) Overlay. It enables OSI Layer 2, 3, and 4 protections and access controls. Data capture and real-time monitoring of network devices, traffic, and user activities can continue without adding unnecessary exposure to the network.

3) The **Byos Management Console™** is a cloud-managed centralized control plane that enables simple centralized control of distributed unmanaged assets on uncontrolled networks, allowing for access control and management of third-parties and across different types of devices.

To further understand how Byos' hardware-enforced microsegmentation can be a robust solution and delivers benefits and flexibility beyond conventional tools, click here to see a full video explanation or book a demo today.