WHITE PAPER

# Claroty and Copia Joint Solution

The Convergence of Cybersecurity and Industrial DevOps: Safeguarding the Future of Industrial Operations

## TABLE OF CONTENTS

## Introduction

The increasing interconnectivity of Operational Technology (OT) environments and their Information Technology (IT) counterparts, driven by Industry 4.0 and the Industrial Internet of Things (IIoT), has brought forth significant opportunities for industrial enterprises to optimize processes, enhance productivity, and gain a competitive edge. However, this convergence has also exposed these environments to a broader range of cyber threats, making robust cybersecurity measures imperative. The practice of Industrial DevOps, which applies lean, agile, and DevOps principles to industrial operations, has emerged as a key strategy to manage this convergence effectively, ensuring both operational efficiency and cyber secure practices.

This white paper explores the challenges associated with the IT/OT convergence, the role of Industrial DevOps in addressing them, and the transformative impact it can have on industrial operations, drawing insights from a recent webinar featuring experts from Copia Automation and Claroty.

## Challenges of the IT/OT Convergence

1. **Increased Cyber Attacks:** The expanding attack surface resulting from the IT/OT convergence has led to a surge in cyberattacks targeting industrial control systems (ICS). The Claroty Global State of Industrial Cybersecurity Report highlights a 75% increase in organizations experiencing ransomware attacks, often originating from the IT environment and impacting OT operations.
2. **Unplanned Downtime:** Both cyberattacks and operational issues, such as misconfigurations and outdated software, can result in unplanned downtime causing substantial financial losses. Copia's State of Industrial DevOps Report reveals that the average cost of downtime is $4.2 million per hour, with 50% of all downtime attributed to industrial code.
3. **Legacy Systems:** The prevalence of legacy equipment in OT environments, often running on outdated operating systems and unsupported software, poses a significant challenge for security teams. These systems are particularly vulnerable to cyberattacks and require specialized security measures.
4. **Lack of Visibility:** The lack of comprehensive visibility into OT assets, their configurations, and vulnerabilities hinders effective risk management. According to Claroty's report, nearly 69% of OT assets have high-risk vulnerabilities, highlighting the need for improved asset discovery and vulnerability management.
5. **Siloed Teams:** The traditional separation between IT and OT teams can create communication gaps and hinder effective collaboration on security initiatives. This siloed approach can lead to ad-hoc fixes and security blind spots, increasing the risk of cyber incidents.

## Claroty's Approach to Cybersecurity

Claroty's approach to cybersecurity focuses on providing organizations with the visibility, control, and protection they need to secure their OT environments in the face of evolving threats. They emphasize the importance of understanding the unique requirements and constraints of industrial environments and offer solutions tailored to these specific needs. Claroty's solutions focus on several key areas that help organizations approach OT and organizational security in a gradual or accelerated way, depending on what is prioritized by the organization:

### Asset Discovery and Inventory

Creating a complete and accurate inventory of all OT assets, their configurations, and vulnerabilities is the foundation of effective cybersecurity. Claroty provides deep visibility into industrial networks, enabling organizations to identify and manage risks proactively.

### Exposure Management

Claroty helps organizations identify, assess, and prioritize exposures across their OT environments. This enables them to focus their efforts on the most critical areas and implement effective mitigation strategies.

### Network Protection

Claroty provides continuous monitoring and threat detection capabilities to identify and respond to cyber threats in real-time. Their solutions help prevent unauthorized access, detect anomalies, and protect against malicious activities.

### Secure Remote Access

Claroty enables secure remote access to OT environments, ensuring that authorized personnel can connect and manage systems without compromising security.

### Change Management

Claroty's solutions help organizations track and manage changes in their OT environments, ensuring that all modifications are authorized, documented, and monitored.

## Copia and Claroty: A Complementary Approach

Copia and Claroty offer complementary solutions that work together to address the challenges of IT/OT convergence and empower industrial teams to manage both operational efficiency and cybersecurity effectively.

Claroty's cybersecurity solutions provide deep visibility into OT environments, enabling organizations to identify and manage risks proactively. Their solutions complement Copia's capabilities by securing the OT network, providing threat detection, and creating an asset inventory. Copia's Industrial DevOps platform provides a comprehensive solution for managing and deploying industrial code changes across that asset inventory created by Claroty.

Copia brings vendor agnostic version control, configuration management, branching and merging, automated backup, and enhanced testing across OT devices so that organizations can implement changes safely and efficiently, minimizing downtime and reducing the risk of human error, all the while empowering the workforce to more effectively manage productivity while knowing that they are prepared in the event of disaster.

Together, Copia and Claroty empower industrial teams to embrace the Industrial DevOps practices that build a bridge for collaboration between IT and OT, enabling organizations to manage the complexities of IT/OT convergence effectively.

This bridge is needed for digital and industrial transformation to be successful. The future of IT and OT will bring an evolved organizational architecture. In a recent article in Harvard Business Review, Design Your Organization to Withstand Future Disasters, author Juliette Kayyem, former assistant secretary at the Department of Homeland Security and chair of the homeland security program at Harvard's Kennedy School of Government, talks about this change by digging into the Colonial Pipeline attack. She points out the common flaw that left them vulnerable: "Companies generally divide systems between operations and information technology." This is what results in the escalation of a manageable attack into a disaster. Without a unified organizational architecture to connect IT and OT by design, these types of attacks will continue to paralyze companies and their interconnected value chain. "They're [IT/OT] interdependent, which means a risk to one is a risk to the other."

## The Role of Industrial DevOps

Industrial DevOps offers a holistic approach to address these challenges by bridging the gap between IT and OT, fostering collaboration, and enabling the safe and efficient deployment of updates and changes in industrial environments. Key benefits of Industrial DevOps include:

1. **Improved Cybersecurity:** Industrial DevOps enables organizations to implement robust security practices, such as version control, configuration management, access tracking, and automated testing, to mitigate cyber risks and ensure compliance with industry regulations.
2. **Elevated Disaster Recovery:** By enabling controlled code deployments and automated backups, Industrial DevOps helps minimize unplanned downtime caused by both cyberattacks and operational issues.
3. **Enhanced Visibility:** Industrial DevOps provides a comprehensive view of OT asset files, their configurations, and vulnerabilities, enabling proactive risk management and complementing risk detection.
4. **Streamlined Change Management:** Through standardized processes and automation, Industrial DevOps facilitates efficient and controlled change management, reducing the risk of human error and ensuring operational stability.
5. **Increased Collaboration:** Industrial DevOps fosters collaboration between IT and OT teams, breaking downsilos and enabling a unified approach to cybersecurity and operational efficiency.

## 4-Month Guide to Getting Fully Backed Up and Cyber Secure

The convergence of IT and OT has revolutionized industrial operations, but it has also brought increased cybersecurity risks. This infographic presents a four-month plan for industrial organizations to get fully backed up and cyber secure, utilizing Industrial DevOps principles and solutions like Copia Automation and Claroty.

### Month 1

**Establish Visibility & Control:**

1. **Asset Discovery:** Conduct an inventory of all OT assets, including their configurations and vulnerabilities, using Claroty's deep visibility solutions.
2. **Risk Assessment:** Identify, assess, and prioritize cybersecurity risks based on asset criticality and vulnerabilities.
3. **Implement Backup Solutions:** Deploy robust backup and recovery solutions for critical OT data and systems to ensure business continuity in the event of a cyberattack or system failure.

### Month 2

**Secure the Network:**

1. **Network Segmentation:** Segment the OT network to isolate critical systems and limit the lateral movement of attackers in the event of a breach.
2. **Access Control:** Enforce strict access controls and authentication mechanisms to prevent unauthorized access to OT systems.
3. **Vulnerability Management:** Patch and remediate vulnerabilities in OT systems, prioritizing those with the highest risk.

### Month 3

**Strengthen Security Posture:**

1. **Continuous Monitoring & Threat Detection:** Deploy solutions such as Claroty's to continuously monitor and detect cyber threats in real time.
2. **Secure Remote Access:** Implement secure remote access solutions to enable authorized personnel to connect to and manage OT systems without compromising security.

### Month 4

**Embrace Industrial DevOps:**

1. **Version Control & Configuration Management:** Use tools like Copilot's Industrial DevOps platform to implement version control and configuration management for OT code, ensuring efficient and controlled change management.
2. **Automated Testing:** Employ automated testing procedures to confirm that code changes do not introduce new vulnerabilities or disrupt operations.
3. **Collaboration & Training:** Foster collaboration between IT and OT teams and provide ongoing training and education on cybersecurity best practices.

By following this four-month plan, industrial organizations can enhance cybersecurity posture, protect critical infrastructure, and ensure operational resilience in the face of evolving threats. Remember, the journey to cyber secure operations is continuous. By embracing Industrial DevOps and leveraging solutions like Copia and Claroty, organizations can stay ahead of the curve and build a secure and resilient future for their operations.

## Recommendations

1. **Embrace Industrial DevOps:** Adopt Industrial DevOps principles and practices to bridge the IT/OT gap, foster collaboration, and enable the safe and efficient deployment of changes in industrial environments.
2. **Prioritize Asset Visibility:** Establish a comprehensive inventory of OT assets, their configurations, and vulnerabilities to enable effective risk management and threat detection.
3. **Implement Robust Security Controls:** Apply security measures, such as network segmentation, access control, and vulnerability management, to mitigate cyber risks and ensure compliance.
4. **Establish Disaster Recovery Best Practices:** Bolster your Business Continuity Plan (BCP) with automated backup and a best-in-class approach to Disaster Recovery (DR).
5. **Invest in Training and Education:** Provide training and education programs to equip IT and OT teams with the skills and knowledge necessary to implement and manage Industrial DevOps practices effectively.

By embracing Industrial DevOps and taking a proactive approach to cybersecurity, organizations can navigate the complexities of IT/OT convergence, safeguard their critical infrastructure, and build a secure and resilient future for industrial operations.

## Conclusion

The convergence of IT and OT has ushered in a new era of industrial operations, marked by increased connectivity, data-driven insights, and enhanced productivity. However, this convergence also brings forth significant cybersecurity challenges that require a proactive and holistic approach. Industrial DevOps, with its emphasis on collaboration, automation, change management, and continuous improvement, provides a powerful framework to address these challenges, ensuring the resilience and security of industrial operations.

As the industrial landscape continues to evolve, embracing Industrial DevOps will be crucial for organizations to safeguard their critical infrastructure, maintain operational continuity, and gain a competitive edge in the digital age. The convergence of cybersecurity and Industrial DevOps is not just a technological shift, but a cultural transformation that empowers organizations to build a secure and resilient future for industrial operations.

**About Claroty**

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.

**About Copia Automation**

Copia Automation delivers an Industrial DevOps Platform that empowers enterprises - large, mid-sized, and small - to effectively manage their operational technology, achieving industrial automation success. Copia's cloud-based Industrial DevOps Platform empowers companies with unparalleled visibility, governance, and control of automation code across multi-vendor devices. This provides a single source of truth, which enforces continuous quality control, increased uptime, automated backup, and preemptive crisis management. With the addition of AI-powered features like Copia Copilot, Copia Automation continues to drive the future of industrial automation forward.

With its headquarters in New York City, Copia Automation is a member of the World Economic Forum as a Technology Pioneer in Manufacturing.

For more information, visit www.copia.io.