Rockwell Automation

CLAROTY

# What's Driving Industrial Cybersecurity into the Cloud?

BIG GAINS: REAL-TIME OT THREAT INTELLIGENCE AND AUTOMATED RESPONSE CAPABILITIES

## Examining Industrial Sector Cybersecurity Challenges

No matter whether you make cookies or cars, there's almost no tolerance for downtime in Operational Technology and Industrial Control System (OT/ICS) operations. And in Critical Infrastructure sectors – such as healthcare, food/agriculture, or energy – protecting operations that sustain lives, distribute heat, food or electricity are simply not negotiable.

It can be difficult to take multiple OT systems offline simultaneously for maintenance and upgrades.

The concept of migrating industrial manufacturing cybersecurity to the cloud clearly makes good sense given the reliability, high availability, scalability, and efficiencies to be gained. But the gulf is wide between what appears obvious, and the challenges industrial organizations face in migrating OT cybersecurity to the cloud.

That's why it's worthwhile to examine current industrial cybersecurity challenges, along with how organizations can overcome these obstacles with a cloud-based solution.

### OT Challenges: Infrequent Patching & More

In the past, OT environments have traditionally been isolated from IT systems. That separation is disappearing **as OT devices are connected to the enterprise** and as IT/OT convergence offers productivity enhancements that most organizations want to leverage. These trends open OT networks to new threats that require stronger risk reduction strategies.

Meanwhile, **threat actors see the potential for significant disruption and financial gain,** using techniques such as ransomware, phishing, and social engineering to access industrial networks. Ransomware attacks are a significant concern, as they can have a devastating impact. In 2021, a ransomware attack on Colonial Pipeline, a leading pipeline operator, caused the company to shut down its operations for several days, creating widespread fuel shortages across the southeastern U.S.[1]

At the same time, **a shortage of skilled OT cybersecurity professionals** makes it challenging for industrial organizations to hire and maintain the staff needed to quickly respond and avoid damages or unplanned downtime in the aftermath of a cyberattack.

For many industrial organizations, it's unclear how they should implement and maintain effective cybersecurity for OT systems. Legacy **OT systems typically run outdated software** that's often not compatible with the latest security solutions.

Simultaneously, it can be difficult to take OT systems offline for maintenance and updates.

Finally, since many **OT environments traditionally haven't been patched often or well,** vulnerabilities tend to linger. The inherent complexity of OT environments is largely to blame. Patching OT systems can be difficult due to requirements to maintain production uptime, along with constraints imposed by industrial OEMs.

While some industrial sector leaders remain hesitant to move OT operations to the cloud, most acknowledge the need to better protect OT/ICS cybersecurity and reduce risks. What they may not fully realize is how and why migrating to the cloud can help them to improve security, especially OT threat detection, while reducing cost and complexity, and freeing personnel to focus on mission-critical tasks.

## Modernizing OT Cybersecurity to Deter Threats

Industrial organizations increasingly recognize the need to improve visibility across assets and activities on OT networks. They need real-time OT threat detection intelligence and automated response capabilities to detect and deter threats, especially in the emerging era of artificial intelligence (AI).

Cloud-based cybersecurity can help modernize and protect OT environments by providing much needed visibility, along with real-time threat intelligence to reduce vulnerabilities and risks, enterprise-wide. While some industrial plant engineers may have misgivings about moving OT cybersecurity to the cloud, the advantages to be gained from advances – from continuous monitoring and automated threat detection, to scalability, flexibility and access to the latest cybersecurity tools and techniques – are simply too great for today's industrial organizations to disregard.

And as a majority of these organizations are digitally transforming to optimize efficiency and reduce costs, in many cases, that transformation involves cloud-based software-as-a-service (SaaS) or remote managed services. Typically, industrial organizations use SaaS or managed services to automate OT system tasks such as preventive, predictive maintenance, remote

### Gain Clear Visibility to Continuously Detect Threats and Reduce Risks

Implementing a modular, cloud-based cybersecurity solution can help industrial organizations protect against cyberattacks, based on what works for each unique environment.

Asset discovery, for example, can be used to empower industrial organizations to gain clear visibility across IT and OT environments, continuously monitoring network traffic to identify and enrich asset details. It should also seamlessly integrate with common configuration management database (CMDB) and asset management tools to enrich asset details and optimize enterprise asset management.

Real-time threat intelligence, meanwhile, helps industrial organizations continuously monitor OT environments for the earliest indicators of known and emerging threats. All alerts should be contextualized to optimize response and remediation before a threat can impact operations.

### Automation Advantages

Automated response capabilities enabled by cloud-based cybersecurity can help users efficiently identify, prioritize, and remediate vulnerabilities across industrial environments. Whether you need to automate asset discovery, combat zero-day attacks, or aren't sure where to start, migrating OT cybersecurity to the cloud can help quickly support and grow your organization's security posture, to keep pace with current and emerging threats.

In addition, industrial cloud-based cybersecurity services can also alleviate the skills shortage challenge by providing a turnkey solution that can be deployed and managed by a small team of security experts, reducing or removing the burden on current personnel.

## Cloud Cybersecurity Advantages

Cloud-based OT cybersecurity advantages include:

- **Visibility –** across IT and OT environments, which enables organizations to continuously monitor network traffic for vulnerabilities.
- **Speed –** via automated response capabilities that prioritize and remediate threats across industrial environments.
- **Scalability –** to easily scale up or down and meet growing or shrinking demand in production operations.
- **Flexibility –** to be deployed and maintained from any location, with minimal upfront investment.
- **Access to the latest technologies** – encompassing a range of leading security technologies and expertise.
- **Compliance –** streamlining reporting to meet emerging requirements.
- **Lower total cost of ownership (TCO)** – which reduces the need for costly hardware, software and cybersecurity personnel investments.

Cloud-based threat detection enables crucial data capture and reporting to keep pace with evolving oversight requirements.

## Reflections and Migration Advice

### Looking Ahead

Cybersecurity disclosure and reporting requirements are also rising. OT and Critical Infrastructure operators must take steps to prepare.

As ransomware threats escalate and geopolitical tensions fuel the rise of nation-state attacks, regulators are increasing oversight, issuing rules about disclosure and risk mitigation. In the U.S., the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) mandates that owners and operators of Critical Infrastructure report all cybersecurity incidents and ransom payments to the Cybersecurity and Infrastructure Security Agency (CISA) within a specified time frame.

On the plus side, increased reporting will help improve every defenders' visibility into current and emerging threats, making it easier to mitigate risks and protect against the most prevalent OT cybersecurity threats. What's more, cloud-based threat monitoring and detection can enable key data capture and reporting processes to help meet evolving compliance requirements.

### Getting Started

Here are key factors to keep in mind when migrating OT cybersecurity to the cloud.

### Before you Migrate

- **Start with a plan.** Assess your current OT environment and identify specific cloud solution requirements. Develop a migration plan that outlines the steps to move OT cybersecurity to the cloud, including a timeline, budget, and resources needed.
- **Work with a qualified partner.** Make sure your provider has a strong track record of security and compliance working in the industrial sector. A qualified partner can help you to develop a migration plan, choose the right cloud provider, and implement needed security controls.

### During Migration

- **Segment your networks.** Segment OT networks from IT networks and from the public internet. This will help contain the spread if a cyberattack occurs.
- **Use a layered security approach.** A layered security approach includes technical and non-technical controls. Technical controls include firewalls, intrusion detection systems, and data encryption. Non-technical controls include security awareness training for employees and background checks for new hires.
- **Test your systems.** Before migrating OT cybersecurity to the cloud, test your systems thoroughly to ensure all security controls, backup and recovery plans, and your ability to respond to cyberattacks are working properly.

### After Migration

- **Monitor your networks for suspicious activity.** Continuously monitor your networks and systems for suspicious activity 24/7 to help detect and respond to cyberattacks quickly and effectively.
- **Make sure there's a backup and recovery plan in place.** This will help restore your data and systems in the event of a cyberattack or other disaster.

By following these steps, industrial organizations can minimize risks, while improving and modernizing cybersecurity protections.

## Why Choose Claroty and Rockwell Automation?

Working with leading OT industry partners will help minimize risks associated with migrating OT cybersecurity to the cloud, and increase your chances of success.

Claroty's xDome is an industrial cybersecurity platform that delivers deep visibility into the cyber-physical systems (CPS) that underpin your OT environment, integrates with your IT tools and workflows, and extends your existing IT security controls and governance to OT. Claroty's industry experts will leverage their deep domain knowledge from hundreds of global customer deployments to help you develop a tailored CPS protection strategy based on your organization's specific needs. Industry expertise, technical expertise, and experience migrating OT cybersecurity to the cloud are all important factors to keep in mind. So too is working with partners committed to your success and responsive to your needs.

**Claroty** empowers industrial, healthcare, commercial, and public sector organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, network protection, threat detection, and secure remote access. Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally.

For more information, visit claroty.com or email contact@claroty.com.

**Rockwell Automation** has over 100 years of experience managing production operations for industrial clients. We understand OT environments in depth and have implemented industrial cybersecurity strategies for over a decade with some of the world's largest organizations. Our expertise and offerings span the NIST Cybersecurity Framework categories of Identify, Protect, Detect, Respond and Recover.

Claroty and Rockwell's industry experts can help better protect your OT/ICS operations from today's most serious threats. Talk to an expert today.

You can also:

- Download a copy of our latest OT cybersecurity research study.
- Take an online assessment to see how your organization stacks up.

[1] "Colonial Pipeline Attack Leads to Calls for Cyber Regs," n.d. https://www.databreachtoday.com/colonial-pipeline-attack-leads-to-calls-for-cyber-regs-a-16574?highlight=true.

Rockwell Automation

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

*Publication # GMSN-SP031A-EN-P October 2023*