Rockwell Automation

# Securing Operations for Consumer Packaged Goods

**Case studies** in implementing cybersecurity solutions for stronger business

Let's start

# Cyberattacks Rising in Frequency and Cost

Among CPG companies, cybersecurity incidents are rising. More than 40% of CPG manufacturers were hit by a cyberattack in 2020. And the financial consequences of compromise are high and rising.

The average cost of data breaches in the CPG sector soared to $3.7 million in 2021, a 42.9% jump over the year before*.

Trends expected to drive increased cybersecurity requirements include more use of Internet of Things (IoT) sensors and devices, the growing availability of 5G, and IT / OT network convergence. More devices and operating systems will connect and transmit data across networks, significantly expanding attack surfaces.

Industrial automation suppliers have a unique perspective and knowledge of the technologies that power CPG facilities. Collaborating with them (and their network of partners) can accelerate time-to-value resulting in lower costs and improved cybersecurity posture.

*Source: www.consumergoods.com/how-cpg-manufacturers-can-prevent-costly-network-breaches

# Leverage Best Practices Across CPG Peers

The following case studies show a wide range of challenges experienced by Rockwell Automation CPG manufacturing customers. Yet all have elements in common.

The best OT cybersecurity solutions – in terms of quality of protection, speed of deployment and ongoing service that minimizes downtime and defends against cyberattacks – require industrial operations experience.

Discover just some of the impactful results that CPG companies are realizing today.

1. A Fortune 500 food manufacturer unified threat management across 46 global sites
2. A food and beverage manufacturer boosted incident response and improved OEE by 5%
3. A food and beverage company increased system reliability and uptime
4. A CPG manufacturer improved response time for critical alarms by 90%; reducing downtime

# A Fortune 500 food manufacturer unified threat management across 46 global sites

## Cybersecurity aligned among dozens of acquired companies

Cyberattacks are increasingly commonplace and costly, interconnected OT and IT systems can jeopardize industrial control systems, and evolving public-safety requirements demand agility.

To overcome these hurdles, one Fortune 500 consumer food manufacturer needed a clear understanding of cybersecurity vulnerabilities to its OT and IT networks. Complicating matters, the company had acquired dozens of food businesses over the past two decades, each with disparate technology and security ecosystems.

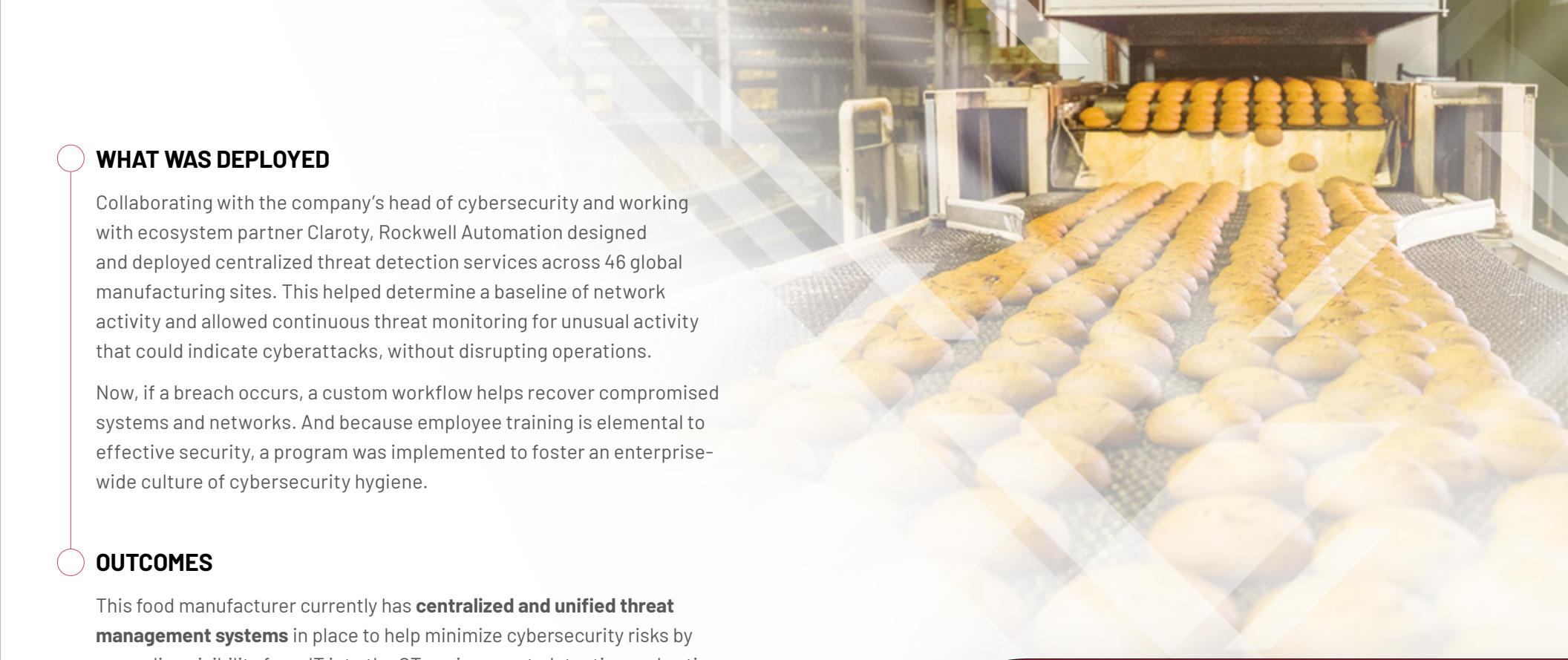
As a result, the manufacturer lacked a centralized, real-time view into the security of systems across its 46 global manufacturing sites. Achieving transparency would require a standard risk-based security strategy and unified threat management capabilities.

**43%**

**increase in cost**

The average cost of a data breach among CPG companies soared to $3.7 million in 2021, a 42.9% increse over 2020.

SOURCE: IBM SECURITY, COST OF A DATABREACH REPORT 2021, JULY 2021



## WHAT WAS DEPLOYED

Collaborating with the company's head of cybersecurity and working with ecosystem partner Claroty, Rockwell Automation designed and deployed centralized threat detection services across 46 global manufacturing sites. This helped determine a baseline of network activity and allowed continuous threat monitoring for unusual activity that could indicate cyberattacks, without disrupting operations.

Now, if a breach occurs, a custom workflow helps recover compromised systems and networks. And because employee training is elemental to effective security, a program was implemented to foster an enterprise-wide culture of cybersecurity hygiene.

## OUTCOMES

This food manufacturer currently has **centralized and unified threat management systems** in place to help minimize cybersecurity risks by expanding visibility from IT into the OT environment, detecting and acting on cyber threats before they become breaches. Employees have new cybersecurity awareness resulting from the enterprise-wide training program. Going forward, the company is **positioned to implement consistent cybersecurity programs** as it continues to grow through future acquisitions.

## SOLUTIONS

- Centralized threat detection >
- Continuous threat monitoring >
- Workflow for threat response >
- Employee training program >

# A food and beverage manufacturer boosted incident response and improved OEE by 5%

## Manufacturer finds that investing in cybersecurity and incident response brings peace of mind

Following a malware attack that disrupted computing systems and production lines, a global snack foods company needed to strengthen cybersecurity defenses and modernize its network infrastructure across 80 sites worldwide. It had earlier attempted to deploy an Overall Equipment Effectiveness (OEE) platform to help measure and mitigate security risks and improve performance of existing applications. But the initiative sputtered due to incompatibilities among the OEE software and the company's enterprise control layer and network requirements.

The business asked Rockwell Automation to help create a global inventory of its digital assets and modernize its incident response and overarching cybersecurity capabilities.

**60%**
**of organizations' breaches**
led to increases in prices passed on to customers

SOURCE: IBM SECURITY, COST OF A DATABREACH REPORT 2021, JULY 2021

## WHAT WAS DEPLOYED

Rockwell Automation collaborated with the company's global director of engineering to assess its networks and help ensure the data needed to measure OEE would be compatible with enterprise networks and applications. Rockwell Automation then conducted comprehensive network assessments across the company's global facilities and implemented interoperable Industrial Data Centers (IDCs) for remote monitoring and management of digital assets. After an in-depth assessment, our team developed a plan to mitigate network conflicts with the OEE application and implement 24/7/365 remote monitoring and administration by the Rockwell Automation support team.

## OUTCOMES

With the new network infrastructure in place, this snack foods manufacturer quickly saw improvements in **data accuracy and standardized global reporting**. A unified infrastructure, paired with our managed services helped the business **decrease downtime, increase data accuracy, and more quickly respond to cybersecurity incidents** using service level agreements (SLAs).

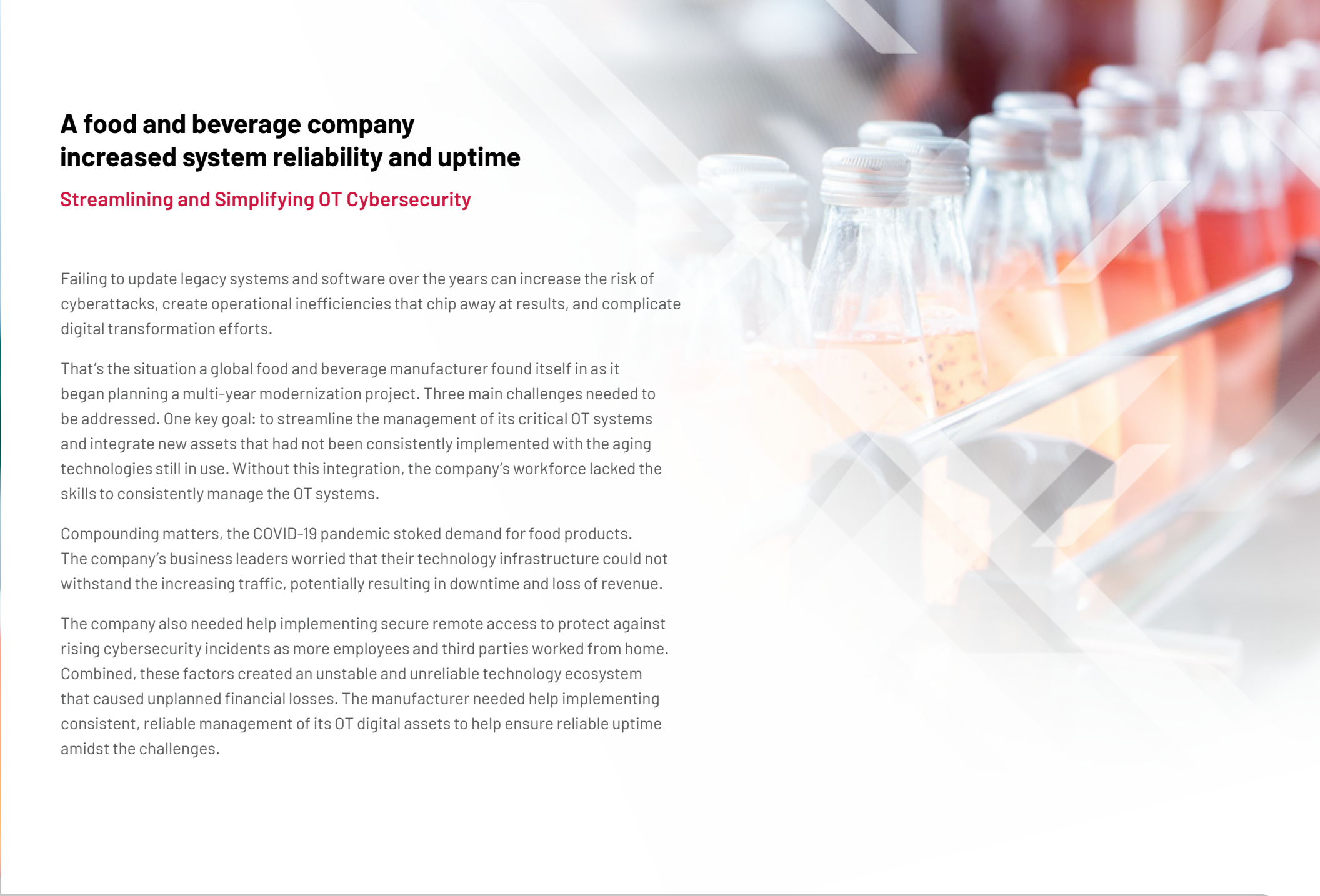
Together, these factors helped the food and beverage company **boost its overall OEE score by 5%**.

## SOLUTIONS

- Network assessment >
- Global Asset Inventory >
- IDC deployment for 24/7 remote monitoring and management >
- Incident Response >

# A food and beverage company increased system reliability and uptime

## Streamlining and Simplifying OT Cybersecurity



Failing to update legacy systems and software over the years can increase the risk of cyberattacks, create operational inefficiencies that chip away at results, and complicate digital transformation efforts.

That's the situation a global food and beverage manufacturer found itself in as it began planning a multi-year modernization project. Three main challenges needed to be addressed. One key goal: to streamline the management of its critical OT systems and integrate new assets that had not been consistently implemented with the aging technologies still in use. Without this integration, the company's workforce lacked the skills to consistently manage the OT systems.

Compounding matters, the COVID-19 pandemic stoked demand for food products. The company's business leaders worried that their technology infrastructure could not withstand the increasing traffic, potentially resulting in downtime and loss of revenue.

The company also needed help implementing secure remote access to protect against rising cybersecurity incidents as more employees and third parties worked from home. Combined, these factors created an unstable and unreliable technology ecosystem that caused unplanned financial losses. The manufacturer needed help implementing consistent, reliable management of its OT digital assets to help ensure reliable uptime amidst the challenges.

## WHAT WAS DEPLOYED

Rockwell Automation worked with the company to design an enterprise OT Managed Support Services program that supports all digital infrastructure equipment. Additional solutions were implemented to enable consistent deployment and support for critical applications, software, and infrastructure, as well as 24x7 remote monitoring.

Rockwell Automation also helped the company deploy 19 OT Industrial Data Centers (IDCs) with a continuous threat detection platform to address cybersecurity risks. And to protect home-bound workers, we designed and implemented secure remote access at 40 North American sites.

## OUTCOMES

The modernized infrastructure and supporting managed services allowed the manufacturer to **reduce cybersecurity threats** to its corporate and OT networks through 24/7 threat monitoring, while minimizing downtime risks. Consistent deployment and integration of technology assets have helped **boost system reliability, and improve application management and plant uptime**. Deployment of secure remote access capabilities protects employees, third-party partners and the company's operational infrastructure from cyber risks.

## SOLUTIONS

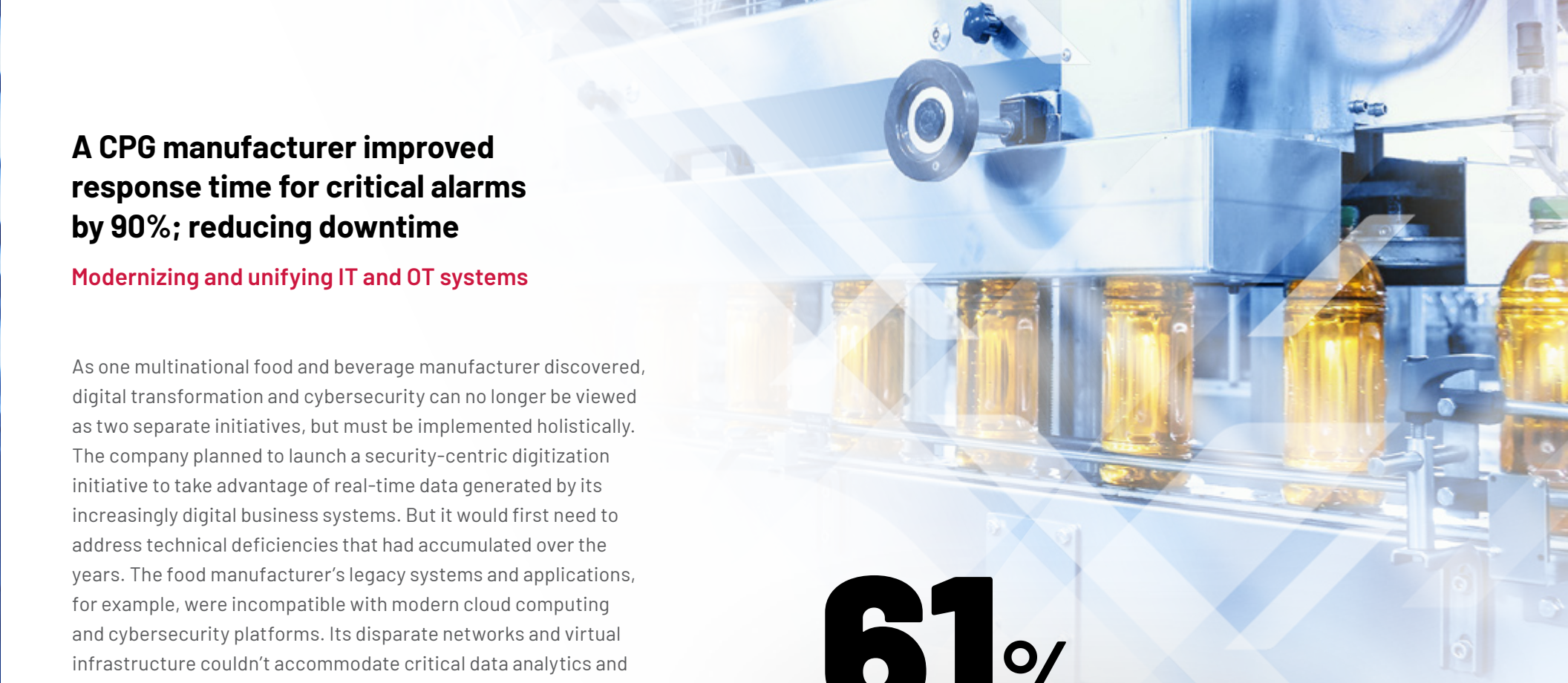
- Managed support for all digital infrastructure equipment >
- 19 OT Industrial Data Centers >
- Secure remote access >
- 24/7 threat detection >

# A CPG manufacturer improved response time for critical alarms by 90%; reducing downtime

## Modernizing and unifying IT and OT systems

As one multinational food and beverage manufacturer discovered, digital transformation and cybersecurity can no longer be viewed as two separate initiatives, but must be implemented holistically. The company planned to launch a security-centric digitization initiative to take advantage of real-time data generated by its increasingly digital business systems. But it would first need to address technical deficiencies that had accumulated over the years. The food manufacturer's legacy systems and applications, for example, were incompatible with modern cloud computing and cybersecurity platforms. Its disparate networks and virtual infrastructure couldn't accommodate critical data analytics and artificial intelligence technologies. And inadequate cybersecurity awareness and training programs for employees contributed to a culture of poor security hygiene.

The CPG manufacturer asked Rockwell Automation to help modernize and unify its IT and OT systems, implement automated monitoring and management of the new network, and update cybersecurity capabilities across 44 sites in North America; without tapping into capital expenditure (CapEx).



**61%**

**of all factories surveyed experienced a security incident in 2021**

SOURCE: TRENDMICRO, THE STATE OF INDUSTRIAL CYBERSECURITY, MAY 2021

## WHAT WAS DEPLOYED

Rockwell Automation created and deployed a modern cloud-based solution using our Infrastructure-as-a-Service (IaaS) offering. Our team collaborated with the CPG company to design the IaaS network and implement cybersecurity capabilities to include network segmentation, patch management for operating systems, and antivirus solutions. A Rockwell Automation ecosystem partner, World Wide Technology, managed the delivery of hardware for the initiative. All network and compute infrastructure were then migrated to a managed service in OT. The company also deployed Rockwell Automation's TechConnectSM Support and Application Support services for improved 24/7 help desk support for applications and infrastructure, and to dispatch on-site field labor for 'hands-on keyboard' support. While service level agreements (SLAs) mandated a response to IaaS alerts in 10 minutes or less, actual response times averaged just 3.5 minutes.

## OUTCOMES

This secure digital transformation solution **closed large cyber-risk gaps** by implementing a modern network infrastructure using Infrastructure-asa-Service offering, as well as effective OT patch management – a notoriously complex security requirement to solve – and antivirus safeguards.

Using the Rockwell Automation's Application Support service, the company **improved response time for critical alarms and alerts by 90%**, which in turn diminished downtime. Funding for the initiative came from the company's operating expenditures, which enabled it to fund digital transformation without tapping into CapEx reserves. The globally-supported, services-ready support model **helped address staffing shortages** for skilled IT and cybersecurity workers in their newly digital operations, and **prepared the company for future scaling**.

## SOLUTIONS

- Infrastructure as a service (IaaS) >
- OT patch management >
- Antivirus >
- TechConnect™ and application support >

# Are you ready to solve your cybersecurity challenges?

To find out more about how Rockwell Automation can support your business  to adapt to the major trends and transformations discussed in this paper, visit: **rockwellautomation/cybersecurity**

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) 2663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, No. 2 Corporation Road, Singapore, 618494, Singapore, Tel: (65) 6302 8686, Fax: (65) 6302 8787
UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44) (1908) 838-800, Fax: (44) (1908) 261-917



Publication FOOD-SP035A-EN-P - June 2023