FORTINET

# Protecting Plant and Manufacturing Operations from the Expanding Attack Surface

## Critical Elements of a Sophisticated Security Architecture

# Table of Contents

# Executive Overview

Plant and manufacturing operations that rely on operational technology (OT) are increasingly finding themselves in the cross hairs of cyberattacks. Nearly three-quarters of OT organizations experienced at least one malware intrusion in the past year.[1] As they work to thwart these attacks by improving the security of plant and manufacturing operations, organizations that rely on OT technologies should evaluate prospective security solutions using several key criteria.

To begin, plant and manufacturing operations leaders need to be sure their security technologies effectively control network access, while preventing lateral movement among and between network segments. Second, they should look for security solutions that integrate to eliminate information silos and reduce the amount of staff time that security management consumes. Third, they need to make sure that every solution on their shortlist is specifically designed to support the protocols and capabilities utilized in their plant operations and manufacturing environment.

# Introduction: Manufacturing Organizations Need to Modernize Security Solutions

Even by the standards of technological change, plant operations and manufacturing organizations are experiencing an unprecedented rate of evolution. Many use supervisory control and data acquisition (SCADA) systems to keep industrial processes on track. These systems collect data from sensors, then incorporate that data into industrial control systems (ICS) used to manage the company's operational systems that typically include a complex array of generators, fans, industrial robots, and other devices.

SCADA and ICS have rapidly become more sophisticated in their ability to leverage data from different types of sensors. They are also increasingly being used by third-party firms; 64% of OT organizations give third-party IT vendors either complete or high-level access to their SCADA or ICS.[2] As a result of these trends, many manufacturers now connect their OT systems to the corporate IT network. Linking ICS and SCADA devices to network IT resources, such as high-end processors and data storage, facilitates more efficient management of plant and manufacturing data.

In addition, increasing numbers of plant operations and manufacturing leaders are putting control systems online. In a recent webinar, 35% of participants said that more than half of their OT systems and devices are connected to the internet, and almost 1 in 10 said all of their OT systems and devices are internet-connected.[3]

Nearly two-thirds (64%) of OT organizations struggle to keep up with the pace of change in OT technology.[4] Security is front and center as an area that needs attention. Fortunately, the right combination of security technologies can enable plant operations and manufacturing leaders to manage these risks.

Following are five considerations plant operations and manufacturing leaders need to keep in mind:

**"When IT and OT work together, organizations are able to deliver more efficient, cutting-edge solutions."[5]**

**Unfortunately, only 55% of organizations that use SCADA and ICS systems have role-based access control for all employees.[6]**

## Deploy Effective Controls Over Network Access

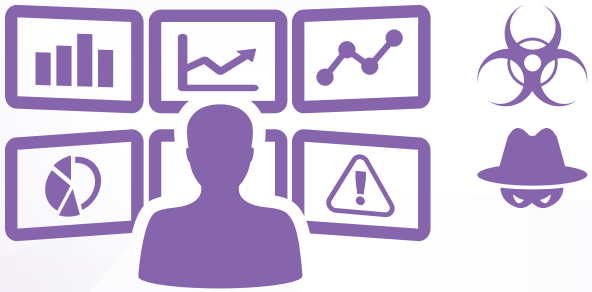
OT devices and systems are becoming increasingly attractive targets for attackers who want to disrupt business operations, steal trade secrets, and collect ransoms.[7] Nearly 60% of organizations using SCADA and ICS have experienced a breach in these systems within the past year, while only 11% have never been breached.[8] This is enormously problematic because the security that comes built into ICS and SCADA solutions is often lacking.

Many OT systems now in use were designed decades ago—when companies maintained an "air gap" between their IT networks and their OT environments, including plant operations and manufacturing systems. Cyberattacks were not even a consideration in the development of such devices. As a result, many OT systems are missing modern capabilities that would make them more secure as the air gap evaporates.

The first line of defense in preventing cyber criminals from reaching SCADA, ICS, and other plant operations and manufacturing systems is to know everything that is connected to or attempting to connect to the corporate network. This is where network access control (NAC) is critical. With many OT systems headless and thus unable to accept patches and upgrades, traditional endpoint security approaches are inadequate.

Plant operations and manufacturing leaders should also employ role-based access control to ensure that users can access only the devices and applications they are authorized to access. Trust needs to be continuously monitored and verified by a trust engine that is integrated into the broader security platform. Taking a least-privilege approach to network access—part of the zero-trust access security model—helps prevent unauthorized access to OT systems.

Research shows that it is important to ensure that users access networks—IT and OT—securely. This is where a private virtual private network (VPN) using multi-factor authentication ensures that users are protected when accessing areas of the corporate network.



**“ICS [systems] are not designed to ensure resilience against concerted attacks … As ICS systems/ components were designed prior to consideration of cyber threats, securing these systems will be a growing area of cyber warfare and engineering research.”[9]**

## Minimize the Attack Surface

The recent increase in connectivity between OT and IT systems creates risk in both directions. Successful attacks on IT systems can give criminals access to OT data and applications, potentially putting plant operations and manufacturing equipment and processes at risk. An attack on an ICS or SCADA system has the potential to alter the motions of equipment, which could result in damages to the equipment or injury to workers.[10] In the most extreme cases, malware that attacks plant operations and manufacturing could put lives at risk.

At the same time, hacked ICS, SCADA, and other OT systems may provide a backdoor for access to network resources. Some plant operations and manufacturing equipment operating systems cannot run standard security-client software and do not provide a means of patching security holes. Even among those plant operations and manufacturing systems that can run security software, patching vulnerabilities is usually difficult because the OT systems need to run 24x7; they cannot be taken offline for security updates.

For these reasons, plant operations and manufacturing systems are often more vulnerable than the typical IT-procured server, storage system, or endpoint. As security solutions become more effective at blocking malware, some attackers are turning their attention to plant operations and manufacturing systems as an alternative and easier path to access corporate networks.

Plant operations and manufacturing leaders should deploy next-generation firewalls (NGFWs) both at the network perimeter and between internal network segments. The NGFWs' trust verifications should be dynamic: They should continuously update the signature set they use to verify user identity, to inspect and control applications, and to block detected attacks. Further, NGFWs should accommodate multiple form factors, to optimize equipment outlays if the firewalls will be deployed to protect segments of different sizes with different volumes of traffic. One more key consideration is the need to inspect secure sockets layer (SSL)/transport layer security (TLS) encryption without impacting the performance of NGFWs.

**"A cyberattack that successfully targets an OT system, or even connected devices such as valves, gauges, or switches, could result in devastating physical consequences to such things as critical infrastructure and services, the environment, and even human life."[11]**

## Eliminate Silos to Improve Security Effectiveness

Most plant operations and manufacturing organizations utilize security solutions from multiple vendors. They select the best-of-breed option to secure each device, resulting in security silos. But this has several negative consequences. One is that different security elements may fail to communicate with one another about detected threats. If a solution in one area of the network detects or thwarts an attempted attack, the malware may yet have success elsewhere. The problem is exacerbated when OT security does not integrate with protection of email, endpoints, switches, wireless access points, or NGFWs.

OT organizations should look for security solutions that integrate tightly to share information about detected threats and about their response to those threats. Integration can also enhance visibility for staff into threat detection and response across all OT and IT systems throughout the organization, for increased line of sight across the entire network security posture.

# 56%

**of OT organizations have experienced a security breach within the past year.[12]**

## Improve Visibility and Automation

For 45% of OT organizations, shortage of skilled IT and cybersecurity talent is a major challenge,[13] and it is one that can reduce a company's ability to adopt sophisticated security technologies and practices. Plant operations and manufacturing teams need to implement solutions that automate manual activities, to streamline workflows for their already-lean staffs.

When evaluating security solutions, plant operations and manufacturing leaders should look for products that not only integrate with the rest of the security architecture but also automate threat detection and response across both OT and IT. The combination of automation and orchestration can reduce, from days to minutes, a network's time to respond to a particular threat. It can also significantly reduce the amount of staff time required to manage the infrastructure, because staff do not waste valuable time running reports across the various security solutions and then compiling information manually.

Finally, an integrated and automated security infrastructure can simplify audit and regulatory reporting, further reducing the manual workload burden on a lean security staff.

**For 45% of OT organizations, shortage of skilled labor is a major challenge.[14]**

## Ensure That Security Solutions Are OT-compatible

In part because of the air gaps that used to separate ICS and SCADA systems from IT networks, many IT security solutions do not support certain OT protocols. However, plant operations and manufacturing organizations that connect OT systems to their IT networks need to make sure the key elements of their security infrastructure support OT.

As an example, some sandboxing solutions are not compatible with certain OT operating systems. Sandboxing technologies identify unknown and zero-day threats by testing potential malware-infected packets before they are unleashed on the network. However, if they cannot run a particular OT protocol, they will be unable to complete this function for systems using that protocol. Plant operations and manufacturing leaders need to make sure their sandboxing solutions were built to support the specific OT devices they need to protect, such as a Siemens programmable logic controller (PLC) or Schneider remote terminal unit (RTU).

The same type of due diligence, to ensure compatibility, is necessary for every security component on the network.

**Security solutions protecting an OT network need to support all the specific protocols in use among the organization's SCADA, ICS, RTUs, PLCs, and other operational technologies.**

## Conclusion: The Right Architecture Secures Both OT and IT

Plant operations and manufacturing leaders put their organizations at risk when they do not have the right security solutions. With the erasure of the air gap between OT and IT, and a proliferation of OT systems and devices, the challenges—and risks—have never been greater. Traditional security simply cannot protect this expanded attack surface.

In response, plant operations and manufacturing leaders need to modernize their security architecture to one that employs comprehensive network access controls, prevents unauthorized lateral movement through the network, delivers transparent visibility and centralized controls, and is fully compatible with OT environments.

**The air gap evaporated, compounding the risks of the expanding attack surface for plant operations and manufacturers. Plant operations and manufacturing leaders can no longer delay addressing the evolving security threats to their OT environments.**

[1] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[2] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, June 28, 2019.

[3] "Webinar: Securing the Future of Industrial Control Systems," Fortinet, accessed September 9, 2019.

[4] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[5] "Causes and Consequences of IT and OT Network Convergence," Fortinet, July 25, 2019.

[6] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, June 28, 2019.

[7] Joe Weiss, "Industrial control systems: The holy grail of cyberwar," The Christian Science Monitor, March 24, 2017.

[8] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, June 28, 2019.

[9] Joe Weiss, "Industrial control systems: The holy grail of cyberwar," The Christian Science Monitor, March 24, 2017.

[10] John Maddison, "Resolving the Challenges of IT-OT Convergence," CSO, June 21, 2018.

[11] Ibid.

[12] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, June 28, 2019.

[13] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[14] Ibid.

www.fortinet.com



443523-0-0-EN

September 30, 2019 4:39 PM

eb-protecting-plant-manufacturing-operations