WHITE PAPER

Network Access Control in ICS/OT Using FortiNAC

Secure IT/OT Convergence with the Fortinet Network Access Control Solution

Executive Summary

As digital transformation and Industry 4.0 take hold in operational technology (OT), many organizations have started to converge IT and OT networks to streamline workflows, centralize controls, and optimize operations. In fact, 58% of manufacturers say the Industrial Internet of Things (IIoT) is a strategic necessity for digitally transforming industrial operations,[1] and about 60% of healthcare establishments have already implemented Internet of Medical Things (IoMT).[2] This growing interconnectivity of things extends from IT into previously air-gapped OT environments. While bringing value to businesses, this also causes attack surfaces to increase and makes once-isolated business operations and critical infrastructures more exposed and vulnerable.

Businesses must take advantage of digital transformation while keeping security risks at bay. This is where network access control (NAC) solutions play a key role. The fundamental function of NAC is to control the access of all connected devices based on set criteria to the network that would otherwise be open for access upon connectivity. NAC has been helping control device access to the IT network for 20+ years. Now, as the network expands, NAC needs to extend its visibility, control, and enterprise-grade security policies to OT devices and operational networks.

The Fortinet network access control solution, FortiNAC, provides visibility across the network for all connected devices, including IT, OT, Internet of Things (IoT), IIoT, and IoMT. FortiNAC extends control of the network, including configuration and segmentation. It also automates event responses and risk remediation in seconds.

80% of OT environments experienced a ransomware attack in 2021, with 47% reporting an impact on their OT/ ICS environment.[3]

The average security breach costs more than $4M in the industrial sector.[4]

Increased Security Risks Hinder IT/OT Convergence

Originally, OT environments—specifically industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems—were secure because of their isolation from external networks and the internet. But this has all changed with IT/OT convergence. While exposing OT systems to the external network or the cloud offers great benefits for operational intelligence, it also introduces a new set of risks. It leads to real-world attacks that can significantly degrade business continuity and operational performance.

As the security risks are clear and present, many organizations are deploying centralized security management tools as foundational components for bridging the IT/OT gap to facilitate contextualized OT security. According to IDC FutureScape's Worldwide IT/OT Convergence 2022 Prediction, by 2024, 30% of industrial organizations will incorporate these security tools to tighten their OT security.[5]

The Challenge of Securing OT

As IIoT devices keep getting added to the network, they create large and fast-growing attack surfaces. However, because of their historical isolation, OT and ICS systems were not included in most existing IT cybersecurity designs. On top of that, many of these legacy systems cannot be patched or updated. And these unsecured endpoints are particularly appealing targets to attackers.

Clearly, there are challenges to securing OT devices while businesses undergo their IT/OT convergence. As the intersection of IT and OT increases, security issues will exhibit themselves in these four main areas:

1. **Lack of visibility:** Not having comprehensive and centralized device visibility leaves OT networks vulnerable to attack. The vast proliferation of all network-connected devices (including IoT and BYOD personal devices) multiplies endpoint-based security vulnerabilities by increasing the number of potential access points for lateral attacks.

   Security teams not only need to see all devices seeking to connect across many different locations, including the extreme edges of the network, but they also need to get more accurate identification of these devices beyond MAC and IP addresses and into types, locations, and functions. It's not an easy task due to the diversity of OT devices, their specializations in different OT verticals, and their unique functions in specialized operations. To make things worse, OT devices tend to have a much longer life cycle than IT equipment—making it harder to have a comprehensive, accurate device database.

By 2025, 70% of asset-intensive organizations will have converged their security functions across both enterprise and operational environments.[6]

2. **Lack of control:** A flat, open internal network makes it easy for hackers, malicious users, and automated malware to roam freely across the organization in search of sensitive data and intellectual property (IP) to exfiltrate. A modern IT/OT converged network needs to meet the resiliency requirements of the OT operation, shield it from other IT segments, and protect security risks from spreading to other areas of the network. Granular network segmentation and purposefully designed security and access policies would do this. Dynamic role-based access controls logically create network segments and limit access based on the roles and functions of IIoT and OT devices.
3. **Lack of situational awareness:** OT security differs from IT security, and very few teams have members that possess the appropriate knowledge in both arenas. For OT, maintaining control of all physical assets to ensure their safe operation is always the primary objective. To do so, security processes and vulnerabilities from OT devices need to be handled differently from IT. For example, IT security updates are so frequent that many IT vendors have a designated update day. However, patching vulnerabilities is not an option in many industrial environments as these systems must operate nonstop.

   Because OT components are rarely updated, they may have many more public vulnerabilities when compared to IT computers. To better secure OT, the awareness of the OT environment and real-time monitoring of OT devices through the connected routers, switches, and firewalls become critical. Security teams must have situational awareness of what's attempting to communicate with the OT systems as well as what traffic is passing through. When an individual OT device is attacked, security teams have to know how critical the device is and what actions to take. Also, identifying the location of the device under attack will help determine the type of action(s) required.
4. **Compliance:** OT compliance requirements are different than IT compliance. Network access control solutions targetting IT and OT convergence should comply with regional and international regulatory requirements.

Access Enforcement with FortiNAC

Solving the challenges associated with securing ICS, SCADA, IoT, BYOD, and other endpoints requires advanced NAC to be part of a comprehensive security architecture. Fortinet FortiNAC can be implemented as a standalone product or as an integrated part of the larger Fortinet Security Fabric to protect network access for unsecured endpoints. With extensive third-party switch and wireless support, FortiNAC extends the Fortinet Security Fabric to over 2,700 non-Fortinet products.

In coordination with additional Fortinet solutions, FortiNAC enables organizations to secure highly distributed networks from SCADA-seeking threats by detecting endpoints with unpatched vulnerabilities. For non-critical endpoints, it can instantly and automatically remove them from the network until they are sufficiently patched. It can also automatically bring these endpoints back into the network from a central dashboard.

For customers concerned about automated enforcement, FortiNAC can alert and notify administrators at their network operations center (NOC) or security operations center (SOC) when such conditions are detected. Specifically, as internet connectivity increases in industrial environments, FortiNAC serves as an important complement for protecting unsecured ICS and SCADA systems, helping to ensure that no unapproved entities connect to an OT network. FortiNAC provides three main capabilities that enhance network security: visibility, control, and automated threat notifications.

Complete Visibility into Every Endpoint Device

A recent survey found that 42% of OT security professionals believe that lack of visibility is the biggest challenge for managing OT risks.[7] Because it is impossible to protect the network from a threat you cannot detect, complete real-time visibility across the organization is a crucial first step in securing endpoint devices. FortiNAC profiles every endpoint connected to the network, including the physical location and type of device. Leveraging 21 active and passive profiling methods, including FortiGate session data and flow data from third-party devices, FortiNAC automatically classifies every endpoint seen on the network. Revalidating these methods each time a device connects to the network also detects and prevents MAC address spoofing attacks.

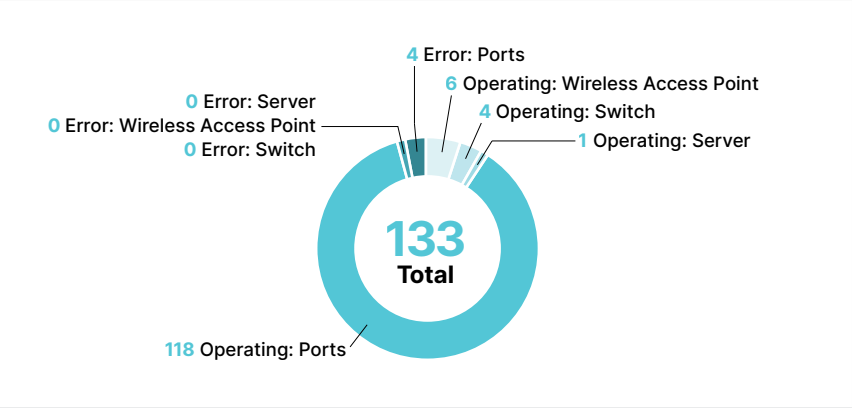

Figure 1: An example of real-time visibility: FortiNAC overview dashboards

Unparalleled Control of Unsecured Devices

As each endpoint device is classified, a least-privilege access policy is applied at the access layer switch and the firewall to ensure proper north-south segmentation rules are in place. In a Fortinet access layer switch or third-party environment that supports private VLANs, microsegmentation capabilities ensure that good east-west communication is also limited. FortiNAC also helps those responsible for managing ICS and OT systems to maintain complete control of their network by managing new devices that want to connect or communicate with other parts of the organization's infrastructure.

> Asset owners frequently require support from third parties such as industrial original equipment manufacturers (OEMs) and system integrators. As these expert technicians come on-site, the asset owner has little control over what's on their laptops, phones, or USB sticks. FortiNAC plays an important role in limiting what networks they have access to when they connect these devices and provide additional security to the industrial enterprise.

FortiNAC can put potentially suspicious requests on hold until administrative approval is given and the network connection is free of spurious traffic. This enables organizations to avoid disruptions to critical systems.

FortiNAC can change the configurations to implement segmentation policies on switches and wireless products from a wide array of vendors. These dynamic controls extend the reach of the Fortinet Security Fabric in heterogeneous environments. Automated rules in FortiNAC trigger containment settings in other Fortinet Security Fabric elements such as FortiGate, FortiSwitch, and FortiAP. It extends to all Fortinet Security Fabric-ready features, including third-party solutions.

Control features are accessed via a highly customizable, easy-to-use web-based administrative dashboard. Potential threats are contained by isolating suspect users and vulnerable devices or enforcing a range of containment actions. This reduces containment time from days to seconds. It also maintains compliance with increasingly strict industry regulations and protects critical data and IP.

Supported Authentication Protocols

FortiNAC supports both legacy and modern authentication protocols and mechanisms. Legacy support includes: CHAP, MS-CHAP, 802.1x, RADIUS, and more.

Control Industrial Switching Platforms

FortiNAC natively supports control of industrial switch platforms from vendors such as Siemens Ruggedcom, Belden/ Hirschmann, Rockwell Automation, and Cisco Industrial Ethernet. There are several management information bases (MIBs) from industrial automation and control system platform vendors available in FortiNAC out of the box.

Supported Device Classification and Profiling Methods

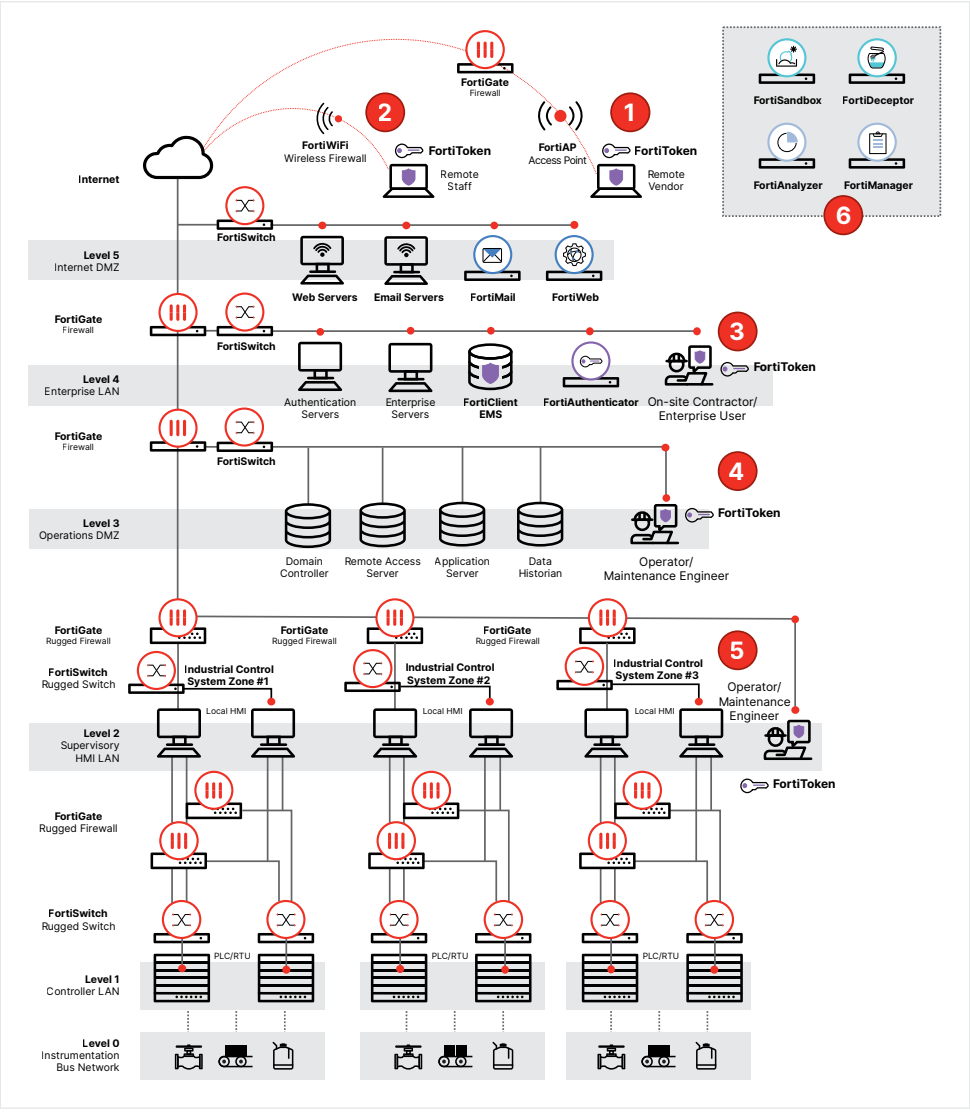

Figure 2: An illustration of how FortiNAC can be deployed to secure the convergence IT/OT environments.

FortiNAC includes a feature called Device Profiler, which is a mechanism to automatically detect and categorize devices as they connect to your network. This process runs continuously. It scans the host database for unknown devices with IP addresses and assigns them a device type based on profiles or rules set up in FortiNAC. Device profile rules use information such as operating system and vendor organizationally unique identifier (OUI) to determine what the connecting device might be. The device profiler is installed with 20+ default rules which can be refined, and new rules can be added. You can evaluate uncategorized devices manually as new rules are added, or existing rules are modified.

OT Platform Integrations

FortiNAC has tight integrations with Security Fortinet Fabric-ready partners Claroty, Nozomi Networks, Ordr, Asimily, and Forescout. These network intrusion detection system (NIDS) vendors extend the Fortinet Security Fabric by taking the rich, granular data they have visibility to and call for the FortiNAC to take action and apply the required response and control. For example, the FortiNAC has considerable vendor data, but the NIDS may flag data flows that identify anomalous patterns. The NIDS can only identify the pattern, but having the FortiNAC integration can create a profile whereby those future flows can be quarantined or stopped. By combining the visibility capability of a NIDS with the response and control of FortiNAC, asset owners can apply critical automation, which is particularly useful in network microsegmentation use cases.

Compliance to Security Requirements

With FortiNAC, asset owners and operators can achieve security control requirements for network access control as specified in IT security control frameworks such as SOX, GDPR, HIPAA, PCI DSS, and OT security requirements such as those specified in NIST CSF, IEC 62443, and NERC CIP.

Automated Threat Notifications

When a suspicious event is detected, FortiNAC sends automated threat notifications to the SOC. As part of the Fortinet Security Fabric, FortiNAC seamlessly integrates with the broader security architecture to enhance the fidelity of alerts by sending and receiving real-time threat intelligence for coordinated awareness from the entire organization. FortiNAC also acts as the enforcement mechanism when other Fortinet products, like FortiSIEM, FortiEDR, FortiDeceptor, and FortiGate, detect compromised endpoint devices.

Through API integrations with the products mentioned above, FortiNAC can alert the security admin about the compromised OT device without blocking it from accessing the network, which is often done in the IT network. This level of handling is critical to keep operations running while evaluating and deciding on the proper actions to take. The FortiNAC orchestration aggregates all security data to automatically triage threats according to priority. It also includes real-time contextual information around the event to help security analysts quickly locate and resolve threats.

Use Cases

Major Oil and Gas Company Secures Critical Infrastructure with FortiNAC

A leading oil and gas company with 5,000 endpoints across 200 locations in North America chose FortiNAC to manage network access to its distributed endpoints and legacy equipment. FortiNAC provided master control over physically dispersed locations without complicated hardware installations or complex legacy equipment upgrades. Because the Fortinet solution is centralized and has no bandwidth allocation requirement, the customer was able to successfully navigate limited bandwidth concerns without appliance installations at remote sites. The company gained visibility across its network with a live inventory of all connections—including highly distributed, remote switches as well as endpoints and users at all locations.

As part of the Fortinet Security Fabric, FortiNAC offers a security automation and orchestration platform that can be deployed as a hardware appliance, a virtual appliance, or a cloud service. This offers security architects a flexible NAC solution that can adapt to the unique needs of any network environment. Designed with scalability in mind, FortiNAC also helps lower the total cost of ownership (TCO) by not requiring a server in every deployment location. It leverages existing directories, networking, and security infrastructures to protect existing investments and minimize disruption.

With centralized control and the ability to lock down challenging legacy systems without requiring a significant upgrade, FortiNAC provides a robust security solution ideal for protecting increasingly vulnerable OT networks from unauthorized devices or users.

Gibson Energy Uses FortiNAC to Remotely Manage Unsecured Devices in Real Time

A Canadian company, Gibson Energy specializes in transporting, storing, blending, processing, and distributing crude oil and other refined products. Headquartered in Calgary, Alberta, Gibson Energy also offers oilfield waste and water management services. As a midstream energy company, Gibson has thousands of devices in the field. Until recently, device management was done manually—or not at all. But the adoption of IoT devices introduced connectivity to OT networks, requiring more visibility and control of devices to ensure operational integrity.

Gibson's operations teams chose FortiNAC to remotely observe and manage unsecured devices in real-time via a customizable, web-based dashboard. When a new device wants to connect or communicate with other parts of its infrastructure, FortiNAC can put suspicious requests on hold until an administrator approves them. Since implementation, FortiNAC has saved Gibson thousands of staff hours on manual device maintenance.

Gibson Energy's Vice President of Information Services, Richard Hannah, said, "Because we deal in the management and control of critical resources, we needed granular access to firewalls and other security tools to build and maintain a single, unified security posture. That's why we started working with Fortinet."

[1] Bojan Jovanovic, Internet of Things statistics for 2022—Taking Things Apart, DataProt, May 13, 2022
[2] Internet of Medical Things (IoMT): Innovative Future for Healthcare Industry, Cogniteq, January 20, 2022.
[3] Survey Results Reveal Resilience of Industrial Organizations in Face of Ongoing Disruptions, The Claroty Team, February 3, 2022.
[4] Average cost of a data breach worldwide from May 2020 to March 2022, by industry, Cyber Crime and Security, Statista, September 6, 2022.
[5] Worldwide IT/OT Convergence 2022 Predictions, IDC FutureScape, October 10, 2021.
[6] Gartner Says 70% of Organizations Will Shift Their Focus From Big to Small and Wide Data By 2025, Gartner, May 19, 2021.
[7] The 2022 State of Operational Technology, SCADAfence, July 14, 2022.

January 23, 2023 10:16 AM
1838471-0-0-EN