SOLUTION BRIEF

Helping To Ensure OT Security Using FortiNAC

Executive Summary

Securing operational technology (OT) systems is a crucial concern in manufacturing and critical infrastructure. While industrial control systems (ICS) and its supervisory control and data acquisition (SCADA) subset systems have been around for many years, greater connectivity and an increasingly sophisticated threat landscape have amplified their susceptibility to attack. One of the areas where Fortinet helps protect OT environments is network access control (NAC). Fortinet's FortiNAC can be implemented as a stand-alone solution or as part of the larger Fortinet Security Fabric to provide visibility and control across OT networks.

Understanding SCADA vs. ICS

ICS are often managed via SCADA systems that provide a graphical user interface for operators to observe the status of a system, receive alerts, or enter adjustments to manage processes.

The ICS market is expected to grow to $81 billion by 2021.

The SCADA market is expected to grow 6.6% annually to reach $13.43 billion in 2022.[4]

Interconnectivity Increases SCADA/ICS Risks

Originally, OT environments and more specifically ICS and SCADA systems were secure because of their isolation from public networks and the internet. And as attacks were virtually nonexistent, there was no reason to incorporate security technologies like Programmable Logic Controllers (PLCs). But this has all changed in recent years as the wall between OT and information technology (IT) systems came down. Per a recent survey, most organizations report connections between traditional IT and their OT systems, introducing the potential for outside hackers to penetrate these control systems.[1]

After the Ukrainian power grid failure of December 2015, when a multi-faceted SCADA attack shut down electrical services for 80,000 customers, organizations quickly concluded these systems are now accessible targets.[2] This is a reality today due to network changes—largely driven by digital transformation—that connected many SCADA systems to the internet and cloud. Further, OT systems have incorporated things like smart environmental controls (e.g., lighting, fire suppression, HVAC) with connected capabilities. And each of these new connections creates a pathway for threats into systems that have historically had no meaningful security built in.

Managing the security of OT systems is a challenge—especially for energy providers, distributed manufacturing facilities, and other critical infrastructure organizations. While exposing these systems to the internet offers great benefits, it also introduces a new set of risks that may be unfamiliar to OT management teams. As these networks begin to weave a complex web of internet-connected ICS, SCADA systems, and PLCs, they now require centralized management and compensating security controls. Organizations must be able to lock down their networks to ensure they know everyone and everything connecting to their OT network.

The Challenging of Securing IoT

OT systems represent a very large attack surface. In a study by Forrester Consulting, nearly 60% of organizations using SCADA or ICS experienced a breach in those systems in the past year. And 97% of respondents acknowledged security challenges because of the convergence of IT and OT.[3]

Because of their historical isolation, ICS and SCADA 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 present particularly appealing targets for attack. First, they can offer access to valuable network data. Second, these systems are frequently part of a nation's critical infrastructure (e.g., electrical, oil, gas, water, transportation).

As the intersection of IT and OT increases, vulnerabilities fall into three main problem areas:

1. Lack of visibility

Lack of 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 must be able to see all devices seeking to connect to their network across many different locations, including the extreme edges of the network.

As ICS sensors, HVAC systems, and controllers become increasingly smart and connected for greater functionality, this introduces new entry points for attacks on OT systems. Specifically, IoT devices lack security standards and are frequently unsecured. IoT devices also do not have an associated user and therefore cannot be authenticated by most existing firewalls or other security that determine access via user-based criteria.

2. Lack of control

A flat and 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 IP to exfiltrate. Therefore, organizations need the ability to apply and enforce access policies based on who and what is connected to the network. Dynamic role-based network access controls logically create network segments that group appli¬cations, link data together, and limit access to specific groups, all of which enhances internal network security.

Control of users and devices is an especially important consideration for maintaining compliance. Many existing industry regulations and privacy laws require strict network access control and data protection—such as the General Data Protection Regulation (GDPR), Health Information Portability and Accountability Act (HIPAA), U.S. Securities and Exchange Commission (SEC), Sarbanes-Oxley (SOX), and Payment Card Industry Data Security Standard (PCI DSS). Organizations can face fines that can reach millions of dollars per violation.

3. Lack of timely situational awareness

When an individual device is being attacked, an organization must be able to share threat information automatically to mount a coordinated defense across the organization. But security teams can receive and triage thousands of security alerts each day. When notified of suspicious activity on a specific IP address, a security administrator might spend hours investigating and manually tracking down a suspect device as well as all of the other relevant information surrounding the event to even determine if it was an attack or an anomaly.

Stopping Attacks with FortiNAC

Solving the challenges associated with securing ICS and SCADA—as well as IoT, BYOD, and other endpoints—requires advanced NAC as part of a comprehensive security architecture. Fortinet FortiNAC can be implemented as a stand-alone product or as an integrated part of the larger Fortinet Security Fabric to protect network access for unsecured endpoints.

In coordination with additional Fortinet solutions, FortiNAC enables organizations to secure highly distributed networks from SCADAseeking 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 that endpoint back into the network from a central dashboard. Specifically, as internet connectivity increases in industrial environments, FortiNAC serves as an important compliment 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 enhances network security: visibility, control, and automated threat notifications.

1. Complete visibility into every endpoint device

The same aforementioned Forrester survey found that 82% of organizations are not able to identify all the devices connected to their network.[5] Since it is impossible to protect the network from a threat you cannot see, complete real-time visibility across the organization a crucial first step in securing endpoint devices. FortiNAC profiles every endpoint connected to the network, including the physical location and type of device.

2. Unparalleled control of unsecured devices

FortiNAC helps those responsible for managing SCADA and ICS 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. FortiNAC can put potentially suspicious requests on hold until an administrative approval is given.

This enables organizations to avoid disruptions to critical systems. Organizations can also use FortiNAC to establish criteria and enforce policies that control which users access the network and how much access each is given. Here, 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 Security Fabric in heterogeneous environments. Automated rules in FortiNAC trigger containment settings in other Security Fabric elements such as FortiGate, FortiSwitch, or FortiAP. It extends to all Fabric-ready elements, 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 by enforcing a range of containment actions. This reduces containment time from days to seconds. It also maintains compliance with increasingly strict industry regulations and protecting critical data and IP

3. Automated threat notifications

When suspicious event is detected, FortiNAC sends automated threat notifications to the security operations center (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. This level of automation is the “holy grail” of a connected security architecture.

FortiNAC’s orchestration level aggregates all security data in order to automatically triage threats according to priority. FortiNAC then automatically sends an alert to the SOC. It also includes real-time contextual information around the event to help security analysts quickly locate and resolve threats. This can reduce containment time from days to seconds while, at the same time, supporting compliance with increasingly strict regulations and standards.

A Flexible and Scalable Platform for Controlling Access

In addition to FortiNAC, Fortinet offers a comprehensive set of solutions for OT environments.

Using core features from the Fortinet portfolio, organizations have capabilities that include:

- Segmenting and securing communications
- Securing wired and wireless access
- Implementing role-based access control for users, devices, applications, and protocols
- Establishing vulnerability and patch management protocols
- Identifying and profiling assets
- Identifying and blocking malware and zero-day threats

As part of the Fortinet Security Fabric, FortiNAC offers a security automation and orchestration platform that can be deployed as a hard¬ware 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 total cost of ownership (TCO) by not requiring a server in every deployment location. It leverages existing directory, 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 major upgrade, FortiNAC provides a strong security solution that is ideal for protecting increasingly vulnerable OT networks from unauthorized devices or users.

Case Study: Major Oil and Gas Company Secures Critical Infrastructure with FortiNAC

Critical infrastructure and utilities continue to evolve with the demands of their everchanging marketplace. At the same time, these organizations must harden their systems to ensure that delivery is never disrupted by security threats that take advantage of out ofcompliance endpoints. Preserving full network access visibility, control, and response over these systems is crucial. But this can be a special challenge for energy providers that often have highly distributed ICS operations. Using IT staff manually maintain and update these geographically dispersed systems is not practical.

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 difficult hardware installations or complex legacy equipment upgrades.

Because Fortinet’s 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. They gained visibility across their network with a live inventory of all connections—including highly-distributed, remote switches—as well as endpoints and users at all locations.

Case study: Gibson Energy

Gibson Energy specializes in the transportation, storage, blending, processing, and distribution of crude oil and other refined products. Headquartered in Calgary (Canada), 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 IT 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 their infrastructure, FortiNAC can put suspicious requests on hold until an administrative approves it. Since implementation, FortiNAC has saved Gibson thousands of staff-hours on manual device maintenance.

"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," says Richard Hannah, vice president of Information Services at Gibson Energy.

[1] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, May 17, 2018.

[2] "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016.

[3] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, May 17, 2018.

[4] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, May 17, 2018.

[5] "IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices," eSecurity Planet, November 8, 2017.

FORTINET

www.fortinet.com

March 7, 2020 8:01 AM

617953-0-0-EN

sb-FA-helping-to-ensure-ot-security-using-fortinac