SOLUTION BRIEF

FortiNAC Simplifies Comprehensive IoT Security

Executive Summary

The risk exposure presented by Internet-of-Things (IoT) devices is perhaps the most challenging part of a network to secure. With an estimated 75 billion IoT devices being connected worldwide by 2025,[1] and attacks targeting IoT devices continuing to rapidly evolve as cyber criminals seek and find new vulnerabilities to exploit, protecting these devices is becoming crucial to a business's overall viability.[2] In response, FortiNAC provides IoT endpoint visibility, network access control (NAC), and automated threat responses to suit the security needs of any organization. Features work with all firewalls and integrate seamlessly with other security solutions, enabling organizations to leverage existing security investments while building a strong security posture.

IoT Vulnerabilities Increase Data Breach Opportunities

According to recent Ponemon Institute research, 97% of risk management professionals indicate that a data breach caused by unsecure IoT devices could be catastrophic for their organization. At the same time, only 15% of respondents had a comprehensive inventory of their IoT applications.[3] Cyber criminals are constantlyscanning networks for vulnerabilities. IoT products and other headless devices are an easy target because most firewalls cannot see or protect these sorts of endpoints.

There are two main use cases for these device-based risk exposures:

Unwitting Accomplices and Shadow IT. Most employees are still unaware of the potential network security risks that come with common office equipment such as internet-enabled coffee makers, refrigerators, printers, and projectors. But these devices are designed to automatically send information to manufacturers and/or share information with other devices over the internet—sometimes without owners even realizing these devices are connecting outside the network.

It's very common for a staff member's legitimate attempt to simplify a business challenge to result in additional connected technologies without the involvement of IT. This subsequently opens a new, unprotected pathway for cyberattacks. It also contributes to something known as shadow IT—user-administered applications and endpoint management that is neither authorized nor overseen by the organization's security experts. While it's not done with any malicious intent, shadow IT describes a widespread trend—comprising as much as 50% of IT spending at large enterprises.[4] And it exposes organizations to significant risks.

Unsecured Headless Devices. When organizations add security cameras, HVAC sensors, medical equipment, and thousands of similar connected or smart devices, many are IoT-enabled to help deliver better operational efficiencies for the business. But these devices also have little to no built-in security by design. Headless devices lack memory and processing. They don't have a traditional interface or operating system like those of a laptop or phone; therefore, they can't run meaningful built-in security. And some IoT devices can't even be patched or updated due to hard-coded PINs in the firmware.

Additionally, without an associated user, IoT devices cannot be authenticated and secured by most existing firewalls or other security solutions that determine access via user-based criteria. Often, security teams don't even realize that these devices are IoT-enabled or that the existing security infrastructure can't protect them. And these same problems exist with other headless devices, such as industrial control systems (ICS) and programmable logic controllers (PLCs).

You Can't Protect What You Can't See

Real-time visibility into all connected endpoints is a crucial first step toward closing security gaps; it's impossible to secure a device if an organization does not know it exists. As an integrated part of the Fortinet Security Fabric, FortiNAC provides real-time visibility via a live inventory of all devices connected to the network.

FortiNAC offers an easy-to-use, one-step solution specifically designed to close security gaps resulting from absent or outdated access controls. It enables network lockdown, simplifying IoT device onboarding and management, while filling a crucial defensive gap by controlling device access. The following are some of FortiNAC's core capabilities:

1. **Endpoint Profiling and Classification.** To help manage the growing numbers of IoT and bring-your-own-device (BYOD) endpoints within most organizations, FortiNAC automates device discovery and classifies each as either corporate- or employee-owned. It provides "what and where" information for all devices. Profiled devices can then only access those assets they need for their function. For example, an Internet Protocol (IP) camera is granted access to the network video recorder (NVR) server, but not the organization's finance or legal servers.
2. **Control of Unsecured/Headless Devices.** FortiNAC can configure third-party network devices to implement segmentation policies. It can change the configurations on switches and wireless products from more than 70 vendors. These dynamic controls extend the reach of the Security Fabric in heterogeneous environments. The use of existing network infrastructure also helps save money and time.

Simplified Deployment of IoT Devices

FortiNAC simplifies the deployment of IoT devices by automating most of the authentication process using a sponsor. When a new IoT device tries to connect to the network, FortiNAC automatically places the device in an isolated network, profiles the device, and sends the information and the suspected type of device to the appropriate department for review and authorization. Once the device is confirmed, FortiNAC notifies the firewall of the type of device and where to place it in the correct network segment. The solution is also easy to upgrade and scale across organizations of all sizes and industries.

With features that work with all firewalls and that integrate seamlessly with other security products, FortiNAC solutions help organizations maximize existing investments while fortifying the organization's defensive posture. FortiNAC offers a variety of options to suit the needs of any organization:

- **FortiNAC Base** for organizations that need to secure IoT/headless devices and enable network lockdown without more advanced network controls or automated threat responses
- **FortiNAC Plus** for organizations that want complete endpoint visibility and a flexible NAC solution with granular control, but do not require automated threat responses
- **FortiNAC Pro** for organizations that want complete endpoint visibility, a flexible NAC solution with granular controls, as well as accurate event triage and real-time automated threat responses

Product	Requirements	Visibility	Control	Response
FortiNAC Base offers an entry-level product designed specifically to close device access security gaps, eliminate common audit failures from shadow IT, and enable network lockdown.	Works best for organizations that do not require more advanced user/network controls, persistent agents, or automated threat responses.	◔	◑	○
FortiNAC Plus adds more advanced NACs as well as automated provisioning and controls for users, guests, and devices. Users automatically receive only the required amount of access based on their role or device. FortiNAC Plus also offers pre-connect and post-connect scans to ensure all devices meet the minimum network security requirements before enabling access; it can even direct users to self-remediate certain issues. In addition, it provides policy-driven, automated quarantine for noncompliant devices or if a device falls out of compliance while connected to the network.	Works best for organizations that want complete endpoint visibility and an advanced NAC solution with granular control, but do not require event triage, event correlation, or fully automated threat responses.	●	●	○
FortiNAC Pro provides real-time endpoint visibility, comprehensive access control, and automated threat responses while delivering contextual information with triaged alerts. It integrates with the broader Fortinet Security Fabric to ingest logs and data from other solutions. It then uses a correlation engine to triage alerts by severity, improve the accuracy of event triage, and present the alert (along with all contextual data) to an analyst.	Works best for organizations that want complete NAC functionality in one solution. As the premium FortiNAC product, FortiNAC Pro delivers the ultimate in visibility, control, and automated responses.	●	●	●

Product	Requirements	Visibility	Control	Response
By presenting all the information in one comprehensive alert, FortiNAC Pro automates much of the manual security review process. This dramatically reduces the time IT analysts spend sifting through alerts and researching event information—shrinking containment time from days to seconds. Automated rules in FortiNAC trigger containment settings across the security architecture (such as FortiGate, FortiSwitch, FortiAP, or integrated third-party solutions).				

[1] Ludovic F. Rembert, "Connected Devices Will Generate 79 Zettabytes of data by 2025," IoT Business News, August 10, 2020.

[2] "Threat Landscape Report for Q2 2018," Fortinet, August 2, 2018.

[3] "Second Annual Study on The Internet of Things (IoT): A New Era of Third-Party Risk," Ponemon Institute, March 2018.

[4] Peter Bendor-Samuel, "How to eliminate enterprise shadow IT," CIO, April 11, 2017.

December 8, 2020 2:50 AM

858995-0-0-EN

D:\Fortinet\Solution Brief\Purple Solution Brief\FortiNAC in IoT\sb-fortinac-simplies-comprehensive-iot-security-V1-1282020\sb-fortinac-simplies-comprehensive-iot-security-V1-1282020