FORTINET

# Network Access Control (NAC) in the Era of IoT and Remote Work

# Table of Contents



FORTINET

# Executive Overview

As Internet-of-Things (IoT) and mobile devices continue to proliferate, the enterprise attack surface grows broader. New gaps and vulnerabilities in the network perimeter are exposed. And at the same time, zero-day exploits and advanced persistent threats grow more sophisticated in their endpoint attack strategies. Security architects need improved access controls to protect devices and the broader network from threats and meet increasingly strict compliance standards. To address these challenges, network access control (NAC) solutions must evolve to provide more robust capabilities that support current needs—threat awareness, containment, and mitigation.

# The Evolution of Access Control

Widespread office adoption of IoT products and work-from-home policies deliver new business capabilities. However, at the same time, they create new challenges. For one, there is virtually no device configuration standardization for IoT. Across any single organization, there are potentially hundreds of device types, brands, and operating systems in active use, of which many lack enterprise-grade security. Additionally, with the new work-from-home policies requiring more employees to use virtual private networks (VPNs) for secure connectivity back to the office, difficulty understanding and providing appropriate access to those devices is precisely why endpoints remain a leading target for sophisticated attacks.

And with the shift to remote work due to the pandemic, employees are connecting back to the corporate networks over secure VPN connections, but with devices that might be anything but secure. From unpatched machines to personal devices, all types of devices can access the network during remote work, opening up all kinds of security issues.

From early on, security leaders focused on controlling device access to the network in order to secure endpoints. The first generation of NAC solutions functioned to authenticate and authorize endpoints (primarily on-premises PCs managed by IT) using simple scan-and-block technology. But when demand for managing guest access to corporate networks arose, NAC capabilities had to evolve. In this case, second-generation NAC solutions facilitated limited internet access for external users (e.g., visitors, contractors, business partners).

But now, with intense changes happening both within network infrastructures and beyond in the threat landscape—and additionally, the pressures of increasingly strict industry regulations and data privacy laws—NAC solutions must evolve again. To fully secure BYOD and IoT endpoints, security architects must be able to see where each device is, what it does, and how it connects to other devices across the network topology. In this case, third-generation NAC solutions must coordinate all endpoint visibility, controls, and automated responses.

**By 2025, there will be 41.6 billion connected IoT devices worldwide—generating 79.4 zettabytes (ZB) of data.[1]**

## Networkwide Visibility

When it comes to NAC, the adage, "You cannot protect what you cannot see," is apropos. Lack of endpoint visibility leaves networks vulnerable to unseen risks. A majority (83%) of organizations report that they are at risk from mobile threats—and two-thirds (67%) say that they are less confident about the mobile asset security than other devices.[2]

Security leaders must be able to track all network infrastructure gear across many different locations, including the extreme edges of the network. Strong defenses start with a complete view of internal devices (PCs, smartphones, laptops, servers, IoT devices, medical devices, POS terminals, HVAC controllers, badge reads, IP cameras) as well as any other IP-based device through a single, integrated network topology view.

A third-generation NAC solution's risk-assessment capabilities must identify the device type and the software configuration (including, where possible, whether antivirus and malware protection is up to date). This endpoint vulnerability assessment must cover both wired and wireless devices, as well as when those devices are connecting over VPN links. It should include headless devices that cannot support built-in security due to their limited capabilities, with many IoT devices falling into this bucket. Innocuous connected appliances—such as refrigerators, gaming consoles, and smart speakers, as well as nonsanctioned network gear such as switches, access points, and wireless routers—that are added to the corporate network without the knowledge of the IT department present risks that can directly lead to a network breach.[3]

Organizations must also be able to automatically discover and categorize all potential users associated with their devices before granting network access—for example, what devices they have registered with the network and even the location/time of day of the connection request. In addition, a NAC's visibility and risk assessment duties should continuously scan for erratic user behavior or signs of endpoint compromise post-connection.

## Enforcement of Policy-based Controls

Once the user and device have been identified, a third-generation NAC solution must then help to implement granular, policy-based microsegmentation of the network with a minimal access approach. A flat and open internal network offers unrestricted access across the organization for hackers, malicious users, or automated malware to exploit sensitive data and IP. Network segmentation dynamically regulates where devices and users can go within the network, when they can go there, and which assets each can access—all based on predefined control policies.

A third-generation NAC solution should also support intent-based network segmentation by providing critical device details—such as user groups and tagged information—to assist with firewall policy enforcement. Access can then be limited to ensure that users and devices may only reach the applications and files that are appropriate to the defined business needs.

In support, an effective NAC solution must also be able to integrate with other best-of-breed security solutions—including products from third-party vendors. This is a critical capability for protecting modern multi-vendor networks. The solution must be able to leverage existing switches, routers, and access points across the infrastructure to establish a live inventory of connections and enforce segmentation control over network access.

**Breaches caused by system glitches ($3.24 million) and inadvertent insider errors ($3.5 million) are still costly to organizations, many of which can be prevented with the right network access policies and controls.[4]**

## Automated Threat Responses

According to a recent study, it takes more than nine months (279 days) on average for an organization to discover a security breach—at a cost of nearly $4 million in damages per event.[5]

Integration also supports the ability for security solutions to send and receive real-time threat intelligence for coordinated actions across the entire organization. This kind of automation is the "holy grail" of a connected security architecture. Third-generation NACs should include an orchestration level that aggregates all security data in order to automatically triage threats according to priority and then set coordinated mitigation responses in motion.

Devices or users in violation of a set network policy should instantly trigger a unified containment response across the security architecture. This might include automatic termination of a connection, restrictions placed on network access, quarantine isolation, and/or a range of security operations center (SOC) notification actions.

These sorts of automated threat responses can reduce containment time from days to seconds to protect sensitive information and IP—while at the same time supporting compliance with increasingly strict regulations, standards, and data privacy laws.

**One primary goal of a well-designed NAC is to make tasks easier by automating the process of restricting network access and providing context-sensitive remediation guidance.[6]**

# What To Look for in a Third-generation NAC Solution

In the face of changing network infrastructure, sophisticated endpoint attacks, and increasingly rigid compliance requirements, security architects need third-generation network access controls to help secure mobile and smart connected devices. Here, NAC should meet the following criteria:

- ☐ **Visibility.** A NAC solution should be able to see and evaluate a full array of endpoints (including IoT) before they connect to the network. It should also be able to categorize the device's user, if applicable. Risk awareness of device and user should continue post-connection.
- ☐ **Endpoint vulnerability assessment.** The solution should also be able to determine critical device vulnerabilities, such as outdated software versions or uninstalled patches, including scanning devices on VPN connections.
- ☐ **Granular control policies.** Once the device and user are identified, the solution should support intent-based segmentation to automatically enforce security policies based on defined device/user information.
- ☐ **Integration.** NAC should seamlessly integrate with other solutions across the broader security architecture—including third-party products—to actively share relevant information about potential threats and enforce controls across the extended organization.
- ☐ **Real-time threat responses.** For endpoints that may be compromised, organizations need a NAC solution that facilitates automated, real-time threat responses to help immediately contain suspect devices before major damage or infection can occur.
- ☐ **Workflow automation.** The solution should enable user self-provisioning, automated device onboarding, as well as self-remediation prompts if a device does not meet minimum security standards.
- ☐ **Scalable and flexible.** A third-generation NAC should provide a scalable architecture that can affordably support multiple locations across the enterprise and unlimited devices. It needs to offer flexible deployment with physical, virtual, and cloud options.

[1] "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast," IDC, June 18, 2019.

[2] "Mobile Security Index 2019," Verizon, March 2019.

[3] "In the Rush to Join the Smart Home Crowd, Buyers Should Beware," The New York Times, January 22, 2019.

[4] "2019 Cost of a Data Breach Report," Ponemon Institute and IBM Security, July 2019.

[5] Ibid.

[6] Kirk Anderson, "NAC: Usability and Security for Users," Security Boulevard, October 3, 2019.

www.fortinet.com



574193-0-0-EN

December 8, 2020 2:40 AM

eb-FA-network-access-control-nac-in-the-of-iot-and-remote-work-1282020