# UNDERSTANDING 802.1X AND NAC: 3 PROBLEMS TO AVOID

WHITE PAPER

## EXECUTIVE SUMMARY

**To enable control over network access, security architects typically turn to the 802.1X standard and/or commercial network access control (NAC) solutions. Each option has security limitations to consider, however, especially as networks rapidly expand with bring-your-own-device (BYOD) and Internet-of-Things (IoT) systems. This guide reviews the limitations of each approach and identifies three major problems to avoid when designing a NAC solution: lack of visibility, lack of control, and lack of automation.**

## SPOTTING THE RISKS

Who and what is on your network? These were simpler questions to answer back in the days of wired-only connections and company-owned devices. Now, the defined and hardened network perimeter has virtually disappeared. Employees want wireless and remote access to company resources, as do guests and partners. More than half of companies favor a BYOD policy.[1] At the same time, 1 million IoT devices such as temperature sensors and building controls are being added to networks daily.[2]

The result is that network access is more difficult to protect than ever, and the increased risk exposure is substantial. In a 2018 SANS Institute survey, 42% of respondents reported that their endpoints have been exploited in the past year—and 20% don't even know if they've been breached.[3] A network's endpoint devices represent the most common targets for cyber threats. In addition, 25% of all attacks are projected to target IoT devices by 2020.[4]

Security architects typically draw on two approaches for securing network access. One is 802.1X, a standard created in 2001 for authenticating users and devices that wish to attach to a network. It is a fundamental component of any comprehensive NAC solution. But it is not comprehensive access control in itself. It has a number of limitations that will be delineated below.

The second approach is to use a NAC solution. Vendors brought the first NAC solutions to market a few years after the release of the 802.1X standard. The first generation of solutions authenticated endpoints (primarily managed PCs) using simple scan-and-block technology. The second generation evolved to support guest access to networks. This guide compares NAC capabilities with 802.1X and identifies three of the biggest problems to avoid when designing any NAC solution.

**1 million**
IoT devices are being added to networks daily.

**42%**
of respondents report their endpoints have been exploited in the past year.

## 1) LACK OF VISIBILITY: WHAT'S ON YOUR NETWORK?

You cannot secure what you cannot see on your network. The 802.1X framework can serve as a gatekeeper for entry to both wired and wireless networks, but it has shortcomings in the visibility and protection it provides. Figure 1 offers a high-level view of how 802.1X works.

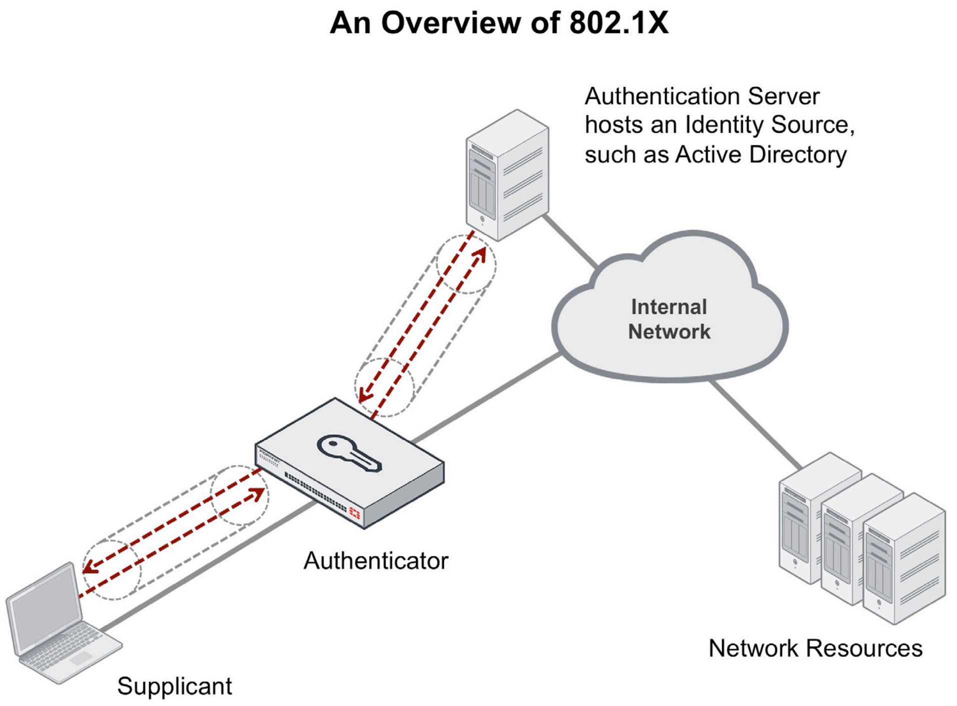

FIGURE 1: USING THE 802.1X FRAMEWORK, AN AUTHENTICATOR CHECKS A SUPPLICANT'S ID AND PASSWORD AGAINST THE AUTHENTICATION SERVER AND ITS IDENTITY SOURCE, SUCH AS ACTIVE DIRECTORY, BEFORE ALLOWING ADMISSION.

To use a simple analogy, the supplicant in an 802.1X solution is like a guest waiting outside a nightclub. The authenticator performs the role of a security guard and checks the guest's ID against a list approved by the club manager (authentication server), before allowing entry. When authentication is complete, the supplicant joins the network and the role of 802.1X is essentially finished.

NAC solutions were introduced to provide security capabilities that the 802.1X framework alone lacks. NAC solutions not only authenticate a device but also scan it for threats and check that it complies with security policies before it is allowed to connect. Some NAC solutions perform authentication without needing an 802.1X solution, while others are designed to work with 802.1X elements such as a Remote Authentication Dial-In User Service (RADIUS) server.

There is no standard or agreed-upon architecture for NAC solutions, and they have evolved with different architectural approaches. Some lack the comprehensive visibility and inclusiveness needed for rapidly evolving enterprise networks. Their defensive shortfalls, and additional 802.1X security concerns, are noted below.

### BYOD DEVICES

BYOD adoption continues to grow: 87% of companies rely on their employees using personal devices to access business applications, up from 74% in 2015.[5,6] Employees are more productive with their own devices, saving 58 minutes a day.[7] But BYOD also presents security teams with a tough challenge: how can unmanaged devices be controlled and secured?

Connecting devices using an 802.1X solution can be challenging:

- Each site needs access to an authentication server connected to a central directory, and supporting this requirement can be a burden to the IT team.
- There is unacceptable risk if users can attach their own devices to the network using only usernames and passwords.
- It can be complex for users if they must install 802.1X supplicant software on their devices. This enhances authentication, but requires increased IT support.
- NAC solutions vary in their ability to automate BYOD onboarding.

### IoT DEVICES

The volume of IoT devices attached to networks, such as security cameras, recorders, temperature sensors, and light controls, is increasing quickly. Many of these devices do not support supplicant software, so they cannot participate in 802.1X authentication.

One option is to deny them access to the network, but this is not realistic. Another option is to put them on a whitelist (approved list), but this is resource-intensive and not secure. A third option is to register their media access control (MAC) addresses and restrict network access to those addresses. This is risky because it is resource-intensive, plus savvy users and hackers can spoof MAC addresses.

Some NAC solutions have their own limitations when it comes to managing IoT devices. For example, some solutions require agents on devices in order to scan them, which presents problems because many IoT devices cannot accommodate software agents.

### GUESTS AND PARTNERS

802.1X solutions can assign nonemployees, such as guests, partners, or contractors, to virtual LANs (VLANs) that allow web connectivity, but limit or prevent access to corporate resources. As with BYOD users, however, there is increased risk in allowing unmanaged and unscanned devices on any part of the network. Requiring supplicant software to be installed on devices enhances authentication, but it also increases the demands on users and IT support.

### WIRED LANS

Wired LANs present a number of challenges that make 802.1X deployment complex and costly. Many legacy endpoints and some legacy switches do not support 802.1X supplicant software. Other switches from different manufacturers are inconsistent in how they handle 802.1X. Further, it is challenging and resource-intensive to configure a switch to support a mix of 802.1X and non-802.1X endpoints, and this can limit visibility and increase risk exposure.

Whether you're managing a wired or wireless LAN, the limitations of 802.1X and/or first- and second-generation NAC solutions make it difficult or impossible to get complete visibility of the users and devices on your network.

Employees using BYOD personal devices save **58** minutes per day.

## VISIBILITY CHALLENGES

| Need | 802.1X | NAC |
|---|---|---|
| Authenticate username/ password | X | X |
| Authenticate device | If supplicant software installed | X |
| Automate BYOD onboarding | Complex: may require IT support | Varies: may require agent software |
| Support IoT | Most IoT devices don't support supplicant software | Varies: may require agent software |
| Guests and partner VLANs | If supplicant software installed | X |
| Wired LANS | Complications and exceptions | X |

## 2) LACK OF CONTROL: WHAT CAN YOU DO TO MINIMIZE RISK?

802.1X solutions can authenticate a user and device, but they do not scan the device to assess and remediate its security posture before giving it access to the network. That's like having an airport security agent check passenger IDs and let passengers board the plane without scanning them and their baggage for threats.

Why is this important? To begin, 63% of companies do not monitor endpoints when they are taken off the network and then reattached.[8] They could easily have been compromised. At the same time, the average cost of a single endpoint breach reached $5 million in 2017.[9]

Letting a device onto the network without scanning it is obviously unwise. In addition, 802.1X solutions do not monitor devices **after** they've been authorized to connect. The solutions cannot:

- Spot and block compromised devices on the network or lock down the network when they are detected.
- Limit lateral movement (segmenting the network through dynamic assignment of VLANs) if compromise is detected **after admission**. (802.1X **can** only be used to assign a VLAN **during** admission.)
- Enforce granular role-based access policies after admission (e.g., an IP camera should have access to the video server, but not other parts of the network).
- Monitor ongoing policy compliance, or provide logging, reporting, and audit trails to enhance compliance.

Some NAC solutions can be combined with an 802.1X solution to scan devices and check their security posture before admission. If the device is not compliant with security policies, the NAC can send it to a remediation VLAN where its access is restricted until it complies (malware removed, patches updated, etc.).

In addition, some NAC solutions can scan devices **after** admission to perform some or all of the bulleted capabilities above. NAC capabilities vary, however, and some NAC solutions require agents or client software to enable post-admission scanning. This can make the inclusion of BYOD and IoT devices complex or not possible.

**63%** of companies cannot monitor endpoints when taken off the network.

## CONTROL CHALLENGES

| Need | 802.1X | NAC |
|---|---|---|
| Scan device for threats **before** admission | — | X |
| Scan device **after** admission to spot and block threats | — | Varies: may require agent software |
| Limit lateral movement, assigning VLANs **before** admission | X | X |
| Enforce access policies **after** admission | — | Varies: may require agent software |
| Provide logging, reporting, audit trails | — | Varies |

## 3) LACK OF AUTOMATION: NOT ENOUGH RESOURCES TO ADDRESS THREATS

Today's security teams are typically overstretched. More than 1 million cybersecurity roles are unfilled globally, a total that could grow to 3.5 million in a few years.[10] Meanwhile, teams are receiving security alerts each day that extend into the thousands, with many lacking the bandwidth to manually intervene in every potential network threat. An 802.1X or NAC solution that does not have robust automation capabilities cannot keep up with the need to detect and mitigate threats, therefore increasing the risk exposure of an organization.

Some NAC solutions can also drain team resources and increase risk if they lack integration and interoperability with other security solutions. Specifically, when a NAC solution detects a targeted, risky behavior, it may not have the ability to:

- Share information, such as user identify, security posture status, and device location, with other security solutions, such as intrusion detection and prevention systems (IDS/IPS), data loss prevention (DLP) systems, and security information and event management (SIEM).
- Gather information from enterprise mobility management (EMM) solutions to determine whether or not a device belongs to an organization.
- Be automated to trigger configuration changes in other solutions and quarantine the threat.

Already-burdened security teams face substantial added risk if their NAC solution cannot integrate with other security solutions, for coordinated and automated responses to threats.

More than
**1 million**
cybersecurity roles are unfilled globally.

## AUTOMATION CHALLENGES

| Need | 802.1X | NAC |
|---|---|---|
| Share threat details with other security solutions | — | Varies |
| Gather details from EMM to know if device is company-owned | — | Varies |
| Provide automated, coordinated response with other security solutions to targeted behavior | — | Varies |

## IN SEARCH OF CONTROL

802.1X-based solutions by themselves, or even when combined with many NAC technologies, are not adequate to protect networks that are expanding with BYOD and IoT devices, and new demands for guest and partner access. But NAC solutions are not the same, as they have varied architectures and authentication approaches.

When vetting NAC solutions, security architects need to look for advanced-capability, third-generation NAC solutions that:

- Complement the security gaps of 802.1X
- Address the challenges of including BYOD and IoT devices
- Avoid the problems of a lack of visibility, control, and automation

[1] Josh Bouk, "Top BYOD Trends for 2018", Cass Information Systems, Inc., November 14, 2017.

[2] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed September 6, 2018.

[3] Lee Neely, "Endpoint Protection and Response: A SANS Survey," SANS Institute, June 12, 2018.

[4] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed September 6, 2018.

[5] "BYOD Usage in the Enterprise," Syntonic, Summer 2016.

[6] Teena Maddox, "Research: 74 percent using or adopting BYOD," ZDNet, January 5, 2015

[7] Melanie Turek, "Employees Say Smartphones Boost Productivity by 34 Percent: Frost & Sullivan Research," Samsung Insights, August 3, 2016.

[8] "The Cost of Insecure Endpoints," Ponemon Institute, accessed November 1, 2018.

[9] Charlie Osborne, "Fileless attacks surge in 2017, security solutions are not stopping them," ZDNet, November 15, 2017.

[10] Steve Morgan, "Cybersecurity Jobs Report 2018-2021," Cybersecurity Ventures, May 31, 2017.

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

November 15, 2018 12:59 PM
253941-0-0-EN
wp-understanding-nac-111518-1259pm