portnox™

WHITE PAPER

# 802.1X IS SIMPLER THAN YOU THINK

A Closer Look at How Easy it is to Implement 802.1X for Stronger Authentication.

## Executive Summary

The following whitepaper dispels the notion that implementing IEEE 802.1X for port-based Network Access Control (NAC) and authentication is prohibitively complex. While previous NAC solutions featured complex deployments, complicated licensing structures, and arduous upgrades, modern solutions to the access control problem have made implementing 802.1X so simple that it has become the de facto standard when securing networks. It will delve into the benefits 802.1X authentication affords, such as ease of use, broad acceptance as a universal standard, and secure encryption. With both the challenges and benefits in mind, this whitepaper presents Portnox Cloud – a turn-key solution for 802.1X from the cloud that maximizes the benefits and applications of the authentication standard.

## Why Consider 802.1X?

### Universal Standard

- Competing standards cause confusion; no sooner is a new standard announced than it is replaced by something that claims to be more secure. Those who choose to move to the new option often find themselves with hardware that can't support it.
- 802.1X was first published in 2001. It has broad, far-reaching support across networking infrastructure and end-user devices. Thus, organizations can implement 802.1X without undergoing a costly hardware refresh; today, even consumer-level devices offer support for this universal standard.

### Ultra-Secure

- Pre-connect authorization: devices trying to connect to your network get no information about the network itself before they are authorized. This prevents potential bad actors from learning about potential exploits on your infrastructure.
- All communication during the authentication phase is encrypted, so there is no chance of someone snooping network traffic to discover usernames and passwords.

### Agent or Agentless

- 802.1X does not require an agent to perform the critical authentication function. This makes it ideal for managing BYOD, where employees may be reluctant to install additional software on personal devices, or in scenarios where there is a need to grant temporary access, such as for a guest or contractor. While more advanced features such as risk posture assessment and automated remediation may require additional software, the core of 802.1X - authentication - does not.

### Easy for End Users

- Management tools you already use - MDM solutions like InTune and Jamf, group policy, and other package management tools make configuring devices easy. Self-onboarding options also take the hassle out of provisioning new devices.
- Implementing certificate-based authentication with 802.1X removes passwords from the equation entirely. This frees your users from having to keep track of a million different passwords and is more secure than password-based authentication.

## Portnox brings 802.1X to the Cloud

Previously, the numerous benefits of 802.1X were overshadowed by the difficulty of deploying an on-premise Network Access Control (NAC) solution. With complex licensing and architecture requirements, many organizations were forced to forego this critical security due to time and resources constraints. Portnox Cloud was created to solve this problem and make implementing 802.1X simple.

### No Physical deployment required

- Deployment and setup are simplified, and no on-premise installation is required. Configure your existing networking hardware for 802.1X authentication, integrate your existing identity provider, and you're ready!

### No ongoing maintenance concerns

- A major benefit of cloud-based software is that administrators do not have to spend nights and weekends performing upgrades or security updates; everything is handled for them.

### Local backup available

- Most people's biggest concern when using a cloud-based provider is, "What if the internet goes down?" Our service is built on Microsoft's Azure Cloud, so you know reliability is a top priority, but nothing is perfect. We offer an optional local RADIUS backup—simple to install via a VM or a container—that will act as a fallback in case your connection goes kaput.

### Certificate-based authentication made easy

- Portnox can simplify everything about certificate-based authentication – from distribution to life-cycle management, ensuring seamless deployment, automated renewals, and secure revocation processes, all while reducing administrative overhead and enhancing network security.

### Automation of Policy Enforcement

- Portnox Cloud characterizes device risk with contextual device information called a "risk score." Risk scores are used to grant or deny access based on compliance with network and cloud access policies, such as geolocation, time of access, active applications, security posture, patching status, and more. With Risk Scores, it's easier to identify, characterize, and address issues with malicious devices, automatically limiting or blocking access if needed.

## Conclusion: It Can Be That Simple!

Though many security professionals know of 802.1X's strengths, deployment has presented significant implementation barriers. By delivering 802.1X as a cloud service, Portnox Cloud simplifies deployment without compromising features, making it an essential solution for enterprises invested in creating the most robust possible security posture. To summarize, obtaining the benefits of 802.1X authentication without the headache of on-premise deployment or compromising on security is what Portnox Cloud is all about.