CASE STUDY

Construction & Property Investment Powerhouse Gains Greater Network Visibility & Control with Cloud-Delivered Portnox CLEAR

McLAREN

Executive Summary

London-based McLaren Construction Group had been facing endpoint and network security challenges. In particular, the company found automated device authentication, compliance checks and visibility consistently difficult.

As such, McLaren went in search of a simple-to-deploy and operate NAC solution that could be delivered in the cloud. Having examined a variety of different NAC technologies on the market, the company selected Portnox CLEAR.

The decision was driven by CLEAR's ability to adapt to McLaren's security requirements, as well as the solution's ease-of-deployment. As a SaaS product, CLEAR required minimal manpower, no training and zero TCO (Total Cost to Ownership) from McLaren. Also fueling McLaren's decision was CLEAR's scalability, management centralization, and limited maintenance.

Today, McLaren has established a 360-degree view of the devices connected to its network, and has added new layers of security since implementing CLEAR.

Overview – McLaren Group

McLaren is a privately-owned construction, property investment and development company with operations in the United Kingdom and the Middle East. The company's core areas of focus include commercial offices, mixed-use buildings, residential, retail and more.

Daniel Blackman, McLaren's Head of IT, together with his team, completed a company security posture analysis that included the top 20 CIS controls. Their analysis concluded that they required visibility of devices and network components connected to their networks.

INDUSTRY:
Construction, Property Investment & Real Estate Development

SOLUTION IMPLEMENTED:
Portnox CLEAR

NUMBER OF DEVICES:
1,000

BENEFITS:

Rapid Deployment – Enterprise-grade wifi security in minutes with pre-set infrastructure requiring no prior training.

Seamless Authentication – Individual user-credentials or auto connect via certificate.

Zero-Touch Management – Cloud-delivered RADIUS server and no on-premises hardware/software maintenance / upgrades. CLEAR always runs the latest version.

Flexible Access Controls – Device posture assessment drive policy with Dynamic VLAN or ACL assignments. Blocks or diverts unknown devices, including BYOD.

Device Visibility & Accountability – All devices on the network are seen and easily search to locate users and devices.

No Vendor Lock-In – CLEAR works with any wireless, wired, cloud or VPN infrastructure.

Additionally, Blackman and his team needed the ability to control which devices could gain access to the network in accordance with company policies, security regulations and best practices. McLaren turned to Portnox CLEAR to successfully secure their networks and automate security processes.

The Challenges

McLaren faced a common challenge associated with large and geo-distributed organizations: limited network and device visibility, leading to a variety of security and compliance issues, including device discovery, user authentication and more.

“Our IT team was in charge of responding to network access requests, but it took us too much time to handle each request and people struggled with the complexity of integrating with our existing infrastructure. We couldn’t control the devices that were connecting to our wireless networks, including IoT devices. Furthermore, we couldn’t be sure that the connected devices were compliant with company policies before they were permitted access to key resources,” said Blackman. “We also had to deal with problems related to software and security updates. We were often forced to handle this manually for all devices, which was extremely time-consuming.” Blackman continued.

> *At McLaren Group we needed to find a cloud-delivered NAC solution with no resource overhead and no added complexity – particularly in terms of introducing new hardware or infrastructure changes. We examined a a number of products, and decided to go with CLEAR because of its ease-of-deployment. We were set up within half an hour, which exceeded expectations. We are very satisfied with how easy it is to use this centrally managed solution. We now have complete device visibility and discovery capabilities, which we previously didn’t have access to. With Portnox, it’s been easy to scale to other locations quickly.*
>
> ***Daniel Blackman***
> *Head of IT @ McLaren Group*

“Resolving issues became tiresome and required more and more skilled personnel,” recalled Blackman. “We became aware that we had no rogue device detection or easy access for IoT devices on our sites. We have CC TV’s, audio conferencing devices, security biometric readers, video conferencing equipment and more – and we really wanted to be able to see what was connected to the network on a single pane of glass."

Why Portnox CLEAR

The security team at McLaren needed a solution that would be simple to deploy and operate, while providing full device visibility and network access enforcement capabilities.

After considering several network access control solutions across the marketplace, the group decided to implement Portnox CLEAR. “We decided to go with CLEAR because it was only pure cloud solution, allowing for simplified implementation, scalability and licensing. Plus, there was no need to invest in new infrastructure,” Blackman explained. “We were literally set up and ready to go within half an hour, and it’s worked as intended from that moment on.”

There were a variety of important business considerations driving McLaren’s decision-making process, most of which spoke to Portnox's robust security capabilities and platform flexibility:

1. Cloud-Delivered – McLaren is gradually becoming a “Cloud First” company and looking to implement more SaaS solutions wherever possible. What McLaren especially likes: CLEAR is always running the most up-to-date version on all endpoints, complete with the latest features and functionality...meaning its IT team can focus on network security and not worry about time-consuming software upgrades.

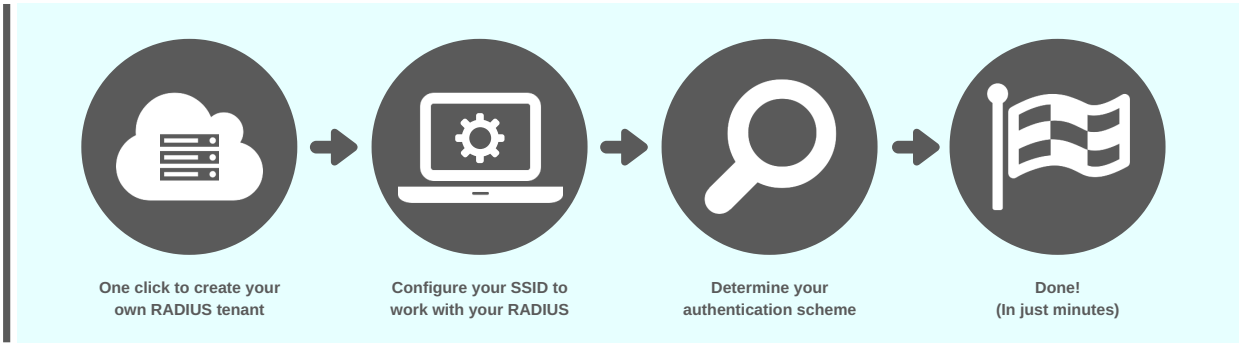
2. Vendor Agnostic – McLaren was able to keep their existing multi-vendor infrastructure, while receiving all the security benefits from Portnox without having to invest in new network equipment or struggle with complicated configurations. CLEAR includes built-in integrations with Azure AD, Microsoft Intune, Palo Alto Networks and more. This ensures that access management, threat response and the prevention of lateral movement is not interrupted. Additionally, CLEAR integrates with native and existing architecture, without the need for port mirroring or span port.

3. Stronger Security – Now that the solution has been fully implemented, McLaren’s security team has successfully handled all challenges associated with device visibility, network access control and compliance enforcement. This includes the ability to see all endpoints on the network, and ensure that they are properly secured according to company policies, privacy standards and regulatory compliance.

4. Automation – As risk-monitoring and enforcement actions are automated, McLaren’s IT team can devote their time to more important tasks that would otherwise have to be done manually, thereby increasing efficiency and productivity.

The Impact

Simple Set-Up



Simple Control

CLEAR controls access to the network based on the 802.1X protocol. It can block rogue devices, quarantine non-compliant endpoints or limit access to specified resources using access control lists (ACLs) or VLAN changes. CLEAR displays a captive portal to explain the next steps that the user should follow. It also assists with the remediation of devices and brings them back into a healthy security state.

Simple Operations

McLaren now has CLEAR's operational console, and is providing role-based access for administrators. This includes the network admin, security admin, IT admin and support team. McLaren's devices are authenticated quickly, and the IT staff can now handle exceptions - such as granting temporary access - with the simple click of a mouse. Automated response actions are in place to remediate devices that do not meet McLaren's security standards.

Simple Management

Day-to-day maintenance is now much more simple. McLaren's enforcement actions are automated as part of a location-based rule, eliminating the need to write a variety of complex rules. Now, anyone using CLEAR will be able to understand why a specific action was taken. Lastly, there is no need for hardware appliances, hardware malfunction handling or future EOL replacements.