CASE STUDY

UK's largest mutual life, pensions & investment company gains network visibility & control with Portnox CORE

Executive Summary

Like many financial institutions, Royal London had been facing endpoint and network security challenges. Automated device authentication, compliance checks and visibility were particularly difficult to achieve within a large and geo-distributed organization. Having examined the different NAC solutions in the market, Royal London chose Portnox CORE.

The decision was primarily driven by CORE's ability to adapt to Royal London's security requirements, as well as the solution's ease of deployment, which required minimal manpower and low TCO (Total Cost to Ownership).

Other criteria that played a crucial role in the decision-making process included having an agentless, vendor agnostic, software-based, centralized and simple-to-maintain technology. Today, the company has full and continuous visibility into every component on the network, along with an upgraded level of information security thanks to implementing CORE.

Overview – Royal London

Royal London is the largest mutual insurer in the United Kingdom, providing around nine million policies with group funds under management of £100 billion. The group employs over 3,500 people, and has offices in London, Wilmslow, Edinburgh, Bath, Glasgow and Dublin.

INDUSTRY:
Financial Institution

SOLUTION IMPLEMENTED:
Portnox CORE

BENEFITS:

Rapid Deployment – CORE is agentless, centralized and works with any existing equipment and vendors.

Simple Operations – CORE's operational console provides a unique network-focused view (from bare metal to endpoint) as well as endpoint listings and the ability to filter the information easily.

Vastly Improved Visibility – a real-time view of endpoints connecting to the network, including state of security, compliance status and user activity.

No Vendor Lock-In – CORE is vendor agnostic, and works with Royal London's existing equipment and vendors.

Ross Cargill, Cyber Engineer at Royal London, and his team performed security analysis and concluded that they required visibility of devices and network components connected to user access. Additionally Cargill 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.The company turned to Portnox CORE to successfully secure their networks and automate security processes.

The Challenges

Royal London was faced with a similar challenge encountered by many large financial institutions: having limited network and device visibility, leading to a variety of security and compliance issues.

"We couldn't control the devices that were connected to our user access network, or be sure that the devices that were connected were compliant with company policies before they were permitted access to key resources," said Cargill. "We have large sites across the UK with lots of visitors, and we needed the ability to secure access to the user switch ports," Cargill continued.

Unfortunately, financial institutions have the constant challenge of being prime targets for cyber offenders. This requires that their security requirements and risk control mechanisms be optimized. To achieve this, these organizations need a solution that is not only simple to implement, operate and manage, but also highly secure. At the end of the day, such a solution must ensure that confidential client information must remain protected and private, security regulations are adhered to, and the network itself is readily available for onboarding by employees and contractors alike.

> *At Royal London we needed to find a fully comprehensive NAC solution that didn't add complexities in terms of excessive additional hardware, agents and change of current infrastructure. We examined a few products, and after testing, we couldn't be happier with the ease of deployment and ongoing management of the Portnox solution. We were able to discover devices we didn't know about so were able to either remove them from the network or approve them via the Portnox platform. With the Portnox solution there is nothing we cannot authenticate using one of the built-in authentication mechanisms and whenever we needed additional assistance, Portnox's support was fantastic. The fact that it is centralized, agentless and completely vendor agnostic, made it a no brainer for us!*
>
> ***Ross Cargill, Cyber Engineer @ Royal London***

Why Portnox CORE?

The security team at Royal London was looking for a solution that would be simple to deploy and operate, while providing full visibility and enforcement capabilities. After testing several NAC solutions by publicly-traded companies, the group decided to implement Portnox CORE. "We decided to go with CORE because it was easy to deploy, agentless, offered a simple licensing model and had a low requirement for new infrastructure," said Cargill.

There were a variety of important business considerations driving Royal London's decision-making process:

1. Implementing a Vendor Agnostic Solution – This allows financial institutions to keep their pre-existing and multi-vendor infrastructure, while receiving all the security benefits without having to invest in new network equipment or to deal with complicated configurations.

2. An Automated, Centralized Solution – Instead of having to deploy appliances in every single location, Royal London now has a system setup that is centrally controlled and performs network monitoring and enforcement across all locations. This has directly lowered security costs in the short-term (and will continue to do so over time), and has significantly reduced TCO.

3. An Agentless Solution – As with all financial institutions, Royal London must never place data and assets at risk while it constantly adds new types of endpoints and services to its networks. Being agentless, CORE allows the financial organization to maintain a strong security posture while avoiding the impediment of business operations caused by having to load and maintain agents on endpoints. In addition to a much faster deployment, non-managed endpoints - such as IoT devices that can not have an agent deployed on them - are also supported.

4. Adherence to Security Compliance Regulations – Connecting and already connected endpoints need to meet basic compliance requirements. This is made possible thanks to CORE's ability to prevent non-compliant devices from accessing the network. This also allows for the preservation of customer trust by protecting data privacy.

The Impact

CORE rapidly provided a complete view of the user access network and every device that was connected or trying to connect to it in real-time. This included identifying and categorizing all devices, such as company-issued computers, IP phones and other miscellaneous devices. This was achieved without having to install agents or appliances. As access is based on device and user identities, company devices and contractors were quickly accounted for, taking into consideration their location and which part of the network they were on. In-depth insights became available, such as user currently logged on, types of endpoint, operating systems, AV versions and more.

Endpoints that did not have the most up-to-date AV signatures were automatically updated using Portnox actions to remain compliant with company policies.

"We are now reassured in the knowledge that rogue devices cannot connect to our network. Our IT support has improved because it's so easy for our support technicians to find users and their devices via the NAS view," Cargill added.

Now that the solution has been fully implemented, Royal London's security team has successfully handled all challenges associated with visibility, 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.

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

Simple Deployment

While adjusting to Royal London's equipment, CORE used standard management protocols which are already defined on the network equipment. Therefore, no preparation work was required. Being software-based, there was no need for appliance installations or infrastructure changes. There was also no need to position CORE inline to pass the traffic through it, or to perform port mirroring. CORE was deployed on Windows servers and at a single centralized location, providing comprehensive access management and control across the entire enterprise, including remote branches.

Simple Operations

Royal London now has CORE's operational console, and is providing role-based access for administrators. This includes the network admin, security admin, IT admin and its support team. There is now a unique network-focused view (from bare metal to endpoint), as well as an endpoint-focused view (endpoint listings) and the ability to filter information as needed.

> ***What is Portnox CORE?***
> *Portnox CORE is a simplicity-focused Network Access Control solution, making deployment, operation and maintenance easier and faster. It provides fully actionable network and device visibility, thereby allowing IT and security teams to handle security risks and compliance challenges in a methodical and easy way. Enforcement actions are automated, thereby reducing the time and manual labor once associated with them.*

Simple Management

Designed by network practitioners, the day-to-day maintenance is now quite simple. At Royal London CORE is configured to "fail open," so if outages or power failures occur, company productivity is not effected. Enforcement actions can be automated as part of a location-rule base, without the need to write complex Boolean rules. Anyone will be able to understand why a specific action was taken. Clustering CORE is easily done at the software and IP level by installing a new server and adding it to a cluster without the need for complex architectures. Additionally, there is no need for hardware appliances, hardware malfunction handling or future EOL replacements.