CASE STUDY

A Major European Bank Establishes Comprehensive Network Access Control from Heaquarters for All Branches & Offices

MAJOR EUROPEAN BANK

This major European bank with headquarters and branch offices throughout Luxembourg, manages over €150 million in assets. The bank faces a constant balance of priorities to keep their financial data secure, meet various regulatory and compliance requirements, whilst simultaneously provide customers in bank/branch wireless guest network access.

The Objective and Challenge

- Preserving their customer's trust by protecting their privacy on the network
- Providing customers required and expected access while maintaining full compliance
- Immediate awareness and control the instant devices attempt to access the network regardless of entry port, access point or VPN.
- Management, visibility and control from HQ for all branches and other bank offices.
- Assurance that customer wireless or other access is limited to specific established and appropriate VLAN(s)

> *The visibility, control and dynamic VLAN capability Portnox was able to bring not only to our headquarters, but across all branches and remote sites from a central management location was unique from the solutions we evaluated and made our decision in favor of Portnox easy.*
>
> ***Director of Network Operations***

The Solution

The Bank selected and deployed Portnox for its ability to deliver constant and real-time control of all devices actively connected to any part of the network from a single centrally deployed location. In addition, with limited availability of IT staff at remote branch locations, Portnox was able to provide remote branch networks access and use of HQ guest network, quarantine and other VLANs with no local configuration or IT resources.

Additional values realized with the Portnox deployment include:

- Apply compliance policies based on type of user/type of device/time based/ location/IP/ use of bandwidth/ fingerprint etc.
- Pinpoint rogue access to the network at all locations, so that administrators could instantly be aware of a device/ user that was rogue, or had failed one of the compliance checks, based on policies the Bank had set.
- Block a rogue device which was connected to the network on the same port that an authenticated device was connected (in a converged setup), without disrupting the legitimate devices' session.
- Shut down the port in an employee's office, once that employee had swiped his card on the time attendance machine on his way out, and then reactivate the port on his return.