BRADFORD NETWORKS

KHIPU

Network Sentry is Part of a Stronger Cyber Fence around Iceland's Airports

Isavia identifies devices and controls network access with Bradford Networks' Security Automation and Orchestration solution.

Headquartered at Reykjavík Airport, Isavia is the national aviation authority for Iceland, dedicated to ensuring that flight operations are safe, secure and in accordance with international standards.

Isavia's nationwide network is critical to operations at Iceland's airports and air traffic control facilities serving vast areas of the northeastern Atlantic. With the number of visitors to Iceland coming through the international airport rising every year and on-track to double in 2016 from 2015, the need for increased network security continues to grow. Many different devices depend on access to the airport's network, including laptop and desktop PCs and a wide range of security and infrastructure devices. Network managers need to know what devices are on the network, where they're located and that each is limited to its intended access. Given the need for heightened airport security, Isavia recognized that these challenges could best be addressed using Network Sentry from Bradford Networks.

With on-site assistance and integration provided by one of Bradford Network's leading channel partners, Khipu Networks, Isavia installed Network Sentry to provide real-time network visibility and automated access control at airports across Iceland as well as at Isavia headquarters and satellite offices. The solution identifies all devices on the network and allows access to resources based on pre-defined policies. Access decisions are made before the device connects so if a device is unauthorized, the connection is automatically blocked. Network Sentry also simplifies the day-to-day logistics of configuring network devices. It automatically identifies devices and assigns access based on easy-to-manage profiles, providing plug-and-play provisioning in a fraction of the previous time.

isavia

NETWORK PROFILE

» Wired Cisco network that supports computers, security devices and infrastructure equipment at airports and other Isavia facilities across Iceland

CHALLENGES

» Monitor and control access to a nationwide network with many remote locations cost efficiently

» Identify devices on the network and only allow access to resources for which they are authorized

» Keep unauthorized devices off the network (rather than try to track them down later)

» Streamline network provisioning for technicians installing or moving devices

» Reduce the burden on network administrators, who had to configure ports manually in disparate locations

SOLUTION

» Network Sentry, Bradford Networks' Security Automation and Orchestration solution

RESULTS

» Provides a real-time view of network activity at all Isavia facilities

» Ensures that only authorized devices can access the network

» Automatically places devices on the correct VLAN based on predefined policies

» Blocks unauthorized devices before they can get on the network

» Plug and play provisioning saves time for network administrators and on-site IT staff

"Using Network Sentry, we have great oversight into which stores and companies are connecting, how many ports they are using and what kind of equipment they have"

— *Axel Einarsson,
IT Manager, Isavia ohf.*

Automatically Enforces Access Policies

"Network Sentry is part of the security fence for our airports," Axel Einarsson, IT Manager at Isavia, explains. "We use it to control device access to ports according to their role. If an unauthorized device tries to connect, Network Sentry shuts down the port immediately." New devices are sent to a registration VLAN where IT captures the MAC address and a few other details. "After that, we can plug a device in anywhere, and Network Sentry automatically assigns it to the correct VLAN according to predefined policies. It's a big time-saver," Axel adds.

The solution supports all Isavia facilities, including Kefkavik International airport, fifteen domestic airports across Iceland, Isavia's headquarters in Rekyavik and branch offices. Network Sentry provides visibility and access control for thousands of devices, including staff PCs and headless devices like printers, badge readers and security cameras. It also provides access control for companies and stores that use the Isavia network.

Improved Oversight and Control

Network Sentry is now an integral part of Isavia's security perimeter that is used to protect Iceland's aviation infrastructure and the flying public who depend on it. It provides complete visibility into all devices that access the network, and Network Sentry's automatic quarantine of unauthorized devices has significantly improved Isavia's security posture. This increased security addresses major concerns for Isavia and the flying public.

Isavia needed a solution that offered the most efficient oversight and access control on a nationwide network.. "Isavia has locations all around Iceland, and we need to protect the ports in those remote locations. We wanted a solution that would enable us to know what was connecting to our networks and shut down unauthorized access."

"We can plug a device in anywhere, and Network Sentry will assign it to the correct VLAN. It's a big time-saver."

— Axel Einarsson, IT Manager, Isavia ohf.

Axel and his colleagues explored the market for a comprehensive security solution, looking for a combination of functionality, ease of use and price. "Network Sentry was a better fit than the competition and integrated smoothly into our network environment," Axel says.

Isavia has greater control over its network while reducing the workload for network administrators at Isavia headquarters and IT staff at remote sites. Since Network Sentry places each device on the correct VLAN, IT can install a device and have it network ready instantly without assistance from administrators to configure ports. "The whole process has become smoother and faster," Axel observes.

What's Next

Continually improving the security posture is a key focus for Isavia. Isavia plans to extend Network Sentry in a number of new directions, including its wireless network, to enable secure BYOD for employees and guests. Network sentry offers real-time visibility and policy-based access control. Network Sentry enables simplified security and antivirus compliance checks when devices connect to the network. Adding this requirement will ensure that devices have an up-to-date operating system and anti-virus software before being allowed access to the network. If users do not meet the requirements, Network Sentry provides a link for users to self-remediate and limits access until they do. "Network Sentry has given us better oversight and control over our network, Axel adds. "Now we look forward to taking it further."