CASE STUDY

BRADFORD NETWORKS

From Concept to Reality: Designing Security Automation and Orchestration Technology into a Smart Building

Bradford Networks helps a large financial organization obtain full network visibility, network lockdown and automated quarantine to secure IoT devices.

As IoT technology continues to advance at a frenetic pace, smart buildings appeal to a wider audience. IoT devices simplify operations and enable organizations to create advanced physical, wired and wireless security solutions. So when a multi-national financial company decided to build a new smart building from concept to execution, Bradford Networks was excited by the invitation to join the project.

Planned by a long-time client of Bradford Networks the smart building complex includes adjoining structures that take full advantage of today's IoT enabled devices. Impressive building plans and operations designs enables the new complex to allow for 10,000 endpoints — approximately 6,000 for employee or corporate devices plus another 3,000 for IoT building devices. There are built-in panels with sensors that detect when to let air in and out, elevators without buttons that only take you to the destination floor coded into your badge and numerous other measures that streamline operations and security.

The Challenge

This financial company has a very simple rule: on the wired network, no access is granted unless it's on a known, trusted company device. The company is taking advantage of numerous IoT devices in its new smart building so its tradition of strict network security must be designed from the ground floor up. Each device on the network will be cataloged, provisioned and controlled before employees first enter the building. During construction, the network will remain locked down so vendors must use a separate temporary network to provision devices.

Bradford Networks is part of the foundational network installation … helping provision and create profiling rules that validate every corporate device, every time it connects.

NETWORK PROFILE

» A Cisco Network with Network Sentry supporting microsegmentation to the edge

CHALLENGES

» Build network access security into the entire greenfield installation – securing over 10,000 endpoints

» Detailed installation and project management – requiring 60 days of work timed over 1.5 years of construction

» Support and enforce over 200 microsegment VLANS

SOLUTION

» Network Sentry, Bradford Networks' Security Automation & Orchestration Solution

RESULTS

» Full visibility of all network connections (all users and devices)

» Wired network lockdown that only allows company devices to connect

» Validate each device every time it connects for a strong security posture

» Automatic quarantine of non-compliant devices

» Simplified and automated "moves, adds, and changes" throughout the network

» Detailed logging and reporting of all network access activity

» Comprehensive network inventory of all endpoints to track build progress

The company is using Network Sentry to provide full visibility and network access control of every wired endpoint. Bradford Networks is part of the foundational network installation at this site, helping provision and create profiling rules that validate every corporate device, every time it connects or re-connects. For example, if a hacker attempted to spoof a printer, Network Sentry would detect this during device re-validation and block access. Only company-owned desktops and laptops running a Network Sentry agent can successfully pass the multiple validations necessary to connect to the network. These processes are designed to secure the company data and ensure that they meet and exceed industry compliance requirements.

The size of this installation and the number of IoT devices is staggering. It features over 1,300 cameras alone as part of 3,000 plus IoT devices secured by Network Sentry. Using microsegmentation, the company employs Network Sentry to enforce rules, control interaction, limit cross-talk, and minimize device communication. The company is configuring every switch as multiple separate sets of user, operational and control microsegments, so nothing spans the systems. Microsegmentation will create over 200 VLANS, taking segmentation to the very edge, reducing the size of the threat landscape, and securing the network against hackers and the spread of malware in an east-west infiltration.

The Network Sentry Difference

The financial company chose Network Sentry not only because of its history of success with Bradford Networks, but also because they wanted a network access control solution that did not need a .1x configuration requiring certificate or user-based authentication. Network Sentry was the perfect choice. Plus, Network Sentry leverages the agent technology to access serial numbers of each provisioned device, compare it to the network asset inventory database and automatically isolate the device if it does not match. Finally, the Network Sentry inventory tool enables the company to track installation progress during the construction phase. Bradford Networks generates weekly reports so the company can track its progress as 10,000 devices are installed and provisioned.

This project is a prime example of Bradford Networks serving as a trusted business partner, providing precise, detailed implementation in a very complex environment.

BRADFORD NETWORKS

374 Congress Street, Suite 502, Boston, MA 02210, USA
Toll Free +1 866.990.3799 | Phone +1 603.228.5300
Email info@bradfordnetworks.com
Web vwww.bradfordnetworks.com

Bradford Networks is leading the transformation of network security by providing visibility, control and response to minimize the risk and impact of cyber threats. The company's patented Network Sentry solution continuously assesses the risk of every user and endpoint, and automatically contains compromised devices that act as backdoors for cyber criminals. Through its SmartEdge Platform, Network Sentry seamlessly integrates with firewall, threat detection and endpoint security solutions to enhance fidelity of security events with contextual awareness. This unique triaging process bridges the gap between the SOC and the NOC by replacing error-prone manual interventions with automated threat to reduce containment time.