FROM CONCEPT TO REALITY: DESIGNING NETWORK ACCESS CONTROL TECHNOLOGY INTO A SMART BUILDING COMPLEX

Building owners and developers are turning to IoT technologies to turn their structures into smart buildings. IoT devices simplify operations and enable organizations to create advanced physical, wired and wireless solutions. However, with the deployment of IoT devices, there is a risk of cyber-attack leveraging these notoriously non-secure devices. So, when a multi-national financial company decided to build a new smart building from concept to execution, they implemented Network Access Control (NAC) to obtain full network visibility, network lockdown, and automated quarantine to secure IoT devices.

The smart building complex includes adjoining structures that take full advantage of today's IoT enabled devices. Impressive building plans and operational designs enable 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. The IoT devices include 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.

COMPLETE NETWORK VISIBILITY AND CONTROL, EVEN DURING CONSTRUCTION

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. Since the company has deployed numerous IoT devices in its new smart building, its tradition of strict network security had to be designed from the ground floor up. Each device on the network was cataloged, provisioned, and controlled before employees first entered the building. During construction, the network remained locked down so vendors had to use a separate temporary network to provision devices.

DETAILS

COMPANY: Anonymous

INDUSTRY: Financial

BUSINESS IMPACT

- Full visibility of all network connections (all users and devices)
- Wired network lockdown that only allows company devices to connect
- Validates each device every time it connects for a strong security posture
- Automatic quarantine of noncompliant 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

DEPLOYMENT

- Network Access Control

The company used Fortinet's NAC solution to provide full visibility and network access control of every wired endpoint. NAC is part of the foundational network installation at this site, provisioning and creating profiling rules that validate every corporate device, every time it connects or re-connects. For example, if a hacker attempted to spoof a printer, NAC would detect this during device re-validation and block access. Only company-owned desktops and laptops running a NAC 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.

THROUGH ITS PLATFORM, NAC SEAMLESSLY INTEGRATES WITH FIREWALL, THREAT DETECTION AND ENDPOINT SECURITY SOLUTIONS TO ENHANCE FIDELITY OF SECURITY EVENTS WITH CONTEXTUAL AWARENESS.

The size of this installation and the number of IoT devices is notable. It features over 1,300 cameras alone as part of 3,000 plus IoT devices secured by NAC. Using microsegmentation, the company employs NAC to enforce rules, control interaction, limit cross-talk, and minimize device communication. The company configured every switch as multiple separate sets of user, operational, and control microsegments so that 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 NAC DIFFERENCE

The financial company chose Fortinet's NAC solution not only because previous successful experience with it, but also because they wanted a network access control solution that did not need an 802.1x configuration requiring certificate or user-based authentication. Fortinet's NAC solution was the perfect choice. Plus, the solution leverages the agent technology to access serial numbers of each provisioned device, compares it to the network asset inventory database, and automatically isolates the device if it does not match. Finally, Fortinet's NAC inventory tool enabled the company to track installation progress during the construction phase. The solution generated weekly reports so the company could track its progress as 10,000 devices were installed and provisioned. This project is a prime example of NAC serving as a trusted business advocate, providing precise, detailed implementation in a very complex environment.

Fortinet's NAC is leading the transformation of network security by providing visibility, control and response to minimize the risk and impact of cyber threats. This patented solution continuously assesses the risk of every user and endpoint, and automatically contains compromised devices that act as backdoors for cyber criminals. Through its platform, NAC 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 assessment to reduce containment time.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

287363-0-0-EN
Sep 26, 2018 6:36 AM
D:\Fortinet\Work\September 2018\092518\cs-smart-building-nac.indd