portnox™

WHITE PAPER

The Importance of a NAC Solution

Executive Summary

This document presents reasons why the value proposition of network access control (NAC) solutions has shifted in recent years due to the onset of wireless networks, coupled with technological advancement that has brought BYOD and IoT devices into the enterprise. It presents the benefits and hence the importance of a NAC solution in the current convoluted network and device environment, referring to Center for Internet Security (CIS) "First 5 CIS Controls" and additional research resources. It presents the key benefits of deploying a NAC solution namely: visibility into connected devices, control over network security posture, management of risk to the network and company data, and Internet of Things manageability. Not unlike firewalls in the 1990's, NAC today is a **must have** part of a robust network security posture.

Introduction – The Growing Demand for NAC Solutions

Since network access control (NAC) was first introduced in the early 2000s, a great deal has changed in the enterprise security landscape. If companies used to use only desktops and laptops, connected and authenticated over a wired network, nowadays wireless networks and mobile technologies have introduced personal devices (via BYOD) and Internet of Things (IoT) to the workplace. In addition, increasingly stringent compliance standards, such as PCI-DSS, SOX, and ISO standards, require companies to openly communicate their security controls to external auditing authorities. As a result, the demand for NAC solutions has rapidly grown over recent years, with Research and Markets predicting the NAC market to be worth $4.39 billion by 2022.

However, the value of NAC solutions extends far beyond answering specific device, network and compliance concerns. NAC solutions can effectively answer the "First 5 CIS Controls", or the top security requirements recommended by governmental and private sector security research organizations that can eliminate approximately 85% of organizational security vulnerabilities. When implemented together with existing security infrastructure, such as SIEM, IPS, MDM, and others, NAC solutions can provide actionable intelligence that makes it easier to react to changes on the network. These benefits and more are outlined below explaining why now, more than ever, enterprise networks need to put NAC at the top of their priority list when it comes to securing the organizational network.

Full Coverage of Top CIS Controls

Those familiar with the cybersecurity vendor market know that due to the proliferation of solutions, many organizations are overwhelmed with what is known as a "Fog of More", or a constant stream of new information and problems that they need to address. As a result, the Center for Internet Security (CIS) came up with the list of top controls to help organizations focus their cybersecurity needs and choose solutions that will address the largest number of vulnerabilities. While specific solutions aren't mentioned, NAC addresses the majority of the 20 controls, and provides complete coverage for the critical Top 5, namely[1] :

CIS Control 1: Inventory of Authorized and Unauthorized Devices

"Actively manage (inventory, track and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access."

- **How NAC Helps:** NAC solutions can see all hardware devices on the network to allow for total inventory and control of all devices accessing the network. There are a number of ways of achieving this, such as port mirroring, IP scans or real-time event driven methods depending on the specific solution.

[1] "Guide to the First 5 CIS Controls," Center for Internet Security.

CIS Control 2: Inventory of Authorized and Unauthorized Software

“Actively manage (inventory, track and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.”

- **How NAC Helps:** NAC solutions gather information on the software installed on endpoints and based on the network security policy can perform actions to notify the user of violations in the policy, force remediation or block unauthorized software. Depending on the vendor solution, this can be achieved with or without an agent installed on the supplicant.

CIS Control 3: Secure Configurations for Hardware and Software

“Establish, implement and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.”

- **How NAC Helps:** NAC solutions can inspect configurations on any endpoints connected to the network. Software can be pre-configured with some NAC solutions, but room can be left for the administrator to add their own configuration inspections as needed.

CIS Control 4: Continuous Vulnerability Assessment and Remediation

“Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attacks.”

- **How NAC Helps:** Most NAC solutions allow for continuous compliance validations and remediation measures for connected devices in the event the device’s risk posture changes post connection.

CIS Control 5: Controlled Use of Administrative Privileges

“The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks and applications.”

- **How NAC Helps:** With possibilities for role-based access control, based on the company’s user repository, most NAC solutions allow for controlled use of administrative privileges based on pre-defined roles and responsibilities.

Features and Benefits of NAC Solutions

NAC solutions can address the necessary above-mentioned controls by providing the following features and benefits:

- **Visibility into the Network:** NAC solutions are a “one-stop-shop” when it comes to gaining visibility into connected devices on the network and in providing network management tools. NAC solutions are able to see which devices are connecting to the network when, and provide information to network and security admins regarding suspicious behavior or connections. By gaining visibility, organizations in effect gain access to actionable intelligence and information on the state of their network security posture.
- **Access Control:** At the heart of any NAC solution is the ability to control access to the organizational network. By controlling access, organizations are able to keep rogue or compromised devices off of the network and better understand the state of endpoint and software inventory that has access to their network and its resources. It allows for the enforcement of pre-defined security principles (policy) and requires the endpoints to meet certain criteria in order to connect such as: device type, patching updates and anti-virus software. This is particularly important for distributed organizations with different types of devices.
- **Unified Management:** By providing the ability to both see and control devices connecting to the network, NAC solutions offer a unified management console that simplifies key tasks for network and security administrators. Within the unified management console, NAC solutions provide the opportunity to effectively implement network security policies by setting automated controls and remediation procedures. By collecting information on network endpoints and their security posture, while also controlling where they access the network (which can also be based on organizational roles when tied to a repository), NAC solutions provide new information to help identify vulnerabilities and minimize the attack surface.
- **Addresses the Internet of Things:** Together with the proliferation of mobile technologies, Internet of Things (IoT) are entering the enterprise at breakneck speed. However, there are a number of security challenges with such devices, namely that they are designed with weak processing systems that cannot accommodate anti-virus or other security software. NAC addresses security issues by allowing for IoT visibility in an agentless system. It can see when IoT devices are connecting and transmitting data over the network, as well as control the areas of the network that they can access. For instance, if an

employee comes to the office with an unauthorized hub to connect additional non-authorized devices, NAC solutions will ensure that those devices and the hub itself will be blocked from accessing the network until the employee consults with a network or security administrator.

- **Integrates with Existing Infrastructure:** While NAC solutions aren't a "cure all" for all cybersecurity needs, they seamlessly integrate and share essential data with security integrations such as: MDM, IPS, SIEM, advanced threat detection services, vulnerability assessment tools, next generation firewalls, and more. NAC solutions can use the alerts from integrated systems to formulate a better reaction to threats or changes in network status. They also integrate with user repositories such as Active Directory to control network access based on group policies, ensuring that users only have only the access they need.
- **Achieving Compliance:** NAC solutions are notably able to help organizations meet a growing body of compliance standards across many industries, such as: PCI-DSS, SOX, HIPAA, ISO 27002 and NIST. Some NAC solutions have designated compliance tools to help network and security administrators bring their security policies into compliance, easily perform necessary auditing checks and compile reports. As compliance becomes an increasingly important aspect of business' bottom line, the implementation tools that NAC solutions provide will only increase in value.

Conclusion – Controlled Access Means Controlling Exposure to Digital Business Risk

If the conversation around NAC solutions 10 years ago centered on managing and controlling wired networks, laptop and desktop devices in the enterprise, nowadays the value proposition of NAC solutions has notably increased. Due to the proliferation of wireless networks and mobile devices – through BYOD and IoT – the workplace has become, on the one hand, a more agile and flexible environment, and on the other, a breeding ground for vulnerabilities and cyber risk. As NAC solutions address the "First 5 CIS Controls", while also providing intelligence into network behavior through various integrations and methods for achieving compliance, they are well suited to help meet and address these risks. In summary, by controlling access to the network with a NAC solution, organizations control their exposure to a wide array of emerging digital business risks, keeping their organizational network healthy and secure.

NAC today is a **must have** part of a robust network security posture.