portnox™

The Importance of a Network Access Control Solution

The enterprise computing landscape has shifted significantly since network access control (NAC) solutions were first introduced. Originally created to control access for devices connecting over the wired network, NAC is effective at knowing when devices connect, and controlling their access based on pre-defined security policies. Rapid innovation in the wireless network over the past decade, together with mobile device technology and Internet of Things, has made it so that the enterprise hardly depends on wired-only systems to achieve its business bottom line, causing the capabilities of NAC solutions to evolve.

Evidenced in the fact that NAC solutions address the Top Five Center for Internet Security (CIS) Controls, it seems that the rapid pace of technological innovation cannot outpace the relevance of NAC solutions. NAC solutions address:

CIS Control 1: Inventory of Authorized and Unauthorized Devices

- **How NAC Helps:** NAC solutions can see all the hardware devices on the network, allowing for total inventory and control.

CIS Control 2: Inventory of Authorized and Unauthorized Software

- **How NAC Helps:** NAC solutions gather information on the software installed on endpoints.

CIS Control 3: Secure Configurations for Hardware and Software

- **How NAC Helps:** NAC solutions can inspect configurations on any endpoints connected to the network.

CIS Control 4: Continuous Vulnerability Assessment and Remediation

- **How NAC Helps:** Most NAC solutions allow for continuous compliance validations and remediation measures for connected devices.

CIS Control 5: Controlled Use of Administrative Privileges

- **How NAC Helps:** Role-based access control makes it possible to control use of administrative privileges based on pre-defined roles.

Network security coverage NAC solutions provide:

Visibility into Network Connections: See and gain insights into every device connecting to the network, and gain actionable intelligence that can be used to optimize network security policies in consideration of threats.

Controlled Access: By setting security policies to control access across the network, organizations can keep malicious devices off the network, thereby controlling exposure to cybersecurity threats and digital business risks.

Unified Management: Simplification of tasks for network and security administrators by providing the ability to both see and control connected devices, set automated controls and remediation procedures.

Internet of Things Security: Gain control over IoT devices and their level of security when connecting to the network with the help of agentless NAC solutions.

Compliance: NAC solutions help organizations meet a growing body of compliance standards such as PCI-DDS, SOX, HIPAA, and more. Easily perform auditing checks and compile reports.

Integrations: NAC solutions can easily integrate with existing architecture and share data with other security vendors such as MDM, IPS, SIEM, and more. Using the alerts from integrated solutions, respond faster and with accuracy to threats or changes in the network status.

Portnox CORE
On-Premise NAC

Request a Demo ›

Portnox CLEAR
Cloud NAC

Try It Now ›

Contact Us

Americas: usinfo@portnox.com | +1.855.476.7866
Europe: dotell@portnox.com | +44.1273.256325

www.portnox.com

www.twitter.com/portnox
www.facebook.com/portnox
www.linkedin.com/company/2526271/
www.youtube.com/portnox

portnox™