

## Access Layers' portnox™ for Improved Network Access Control



### Table of Contents

Introduction	2
Network Access Control (NAC)	3
Access Layers' portnox™	4
portnox™ Management Environment	6
portnox™ Architecture and Deployment	7
Summary	8
About Access Layers	8



# Introduction

**Efficient network security can be achieved only when all network elements are identified, monitored and secured properly at all times. It is no longer effective to secure the perimeter only, since the unmonitored internal network still remains vulnerable. Common defenses are usually not applicable for achieving "internal" security, unable to protect thousands of different systems originating from various vendors.**

Over the past few years, corporate network environments are subjected to many new threats, having to address the needs of a fast growing, diverse user community. Increasing amount of mobile devices, diversity and amount of endpoints other than PC's and laptops (for example: IP Telephony devices), and managed and unmanaged users constantly entering and leaving the network, all raise the network's vulnerability in terms of information and infrastructure security.

As user communities expand and access methods proliferate, networks become more and more heterogeneous and flexible to allow proper productivity, making it almost impossible to maintain the required level of network security. It is no longer effective to secure the perimeter only, since the unmonitored internal network still remains vulnerable and under constant threat. Common defenses are usually not applicable for achieving "internal" security, unable to protect thousands of different systems originating from various vendors.

Companies have suffered tremendous financial losses due to incomplete network security, which caused sensitive information leak and intended or unintended corruption of information and infrastructure. In some cases the damage occurred due to access of a single, "unhealthy" or "unknown" endpoint, causing crashes and disruption of critical operational processes.

Today it is clear that efficient network security can be achieved only when all network elements using the network, managed or unmanaged, are identified, monitored and secured properly. Nonetheless, identifying all network elements, monitoring their actions at all times and enforcing granular security policies without harming users' productivity, network performance or infrastructure, is not trivial.

Analysts suggest that the best way to protect networks, considering their current status and future expected growth, is by using Network Access Control technology (NAC), which has gained industry attention over the last years. According to their forecasts, most companies will be forced to implement some sort of NAC solution within the next 2-3 years, and ones which will not succeed to do so will suffer business insufficiency due to network malfunctions.

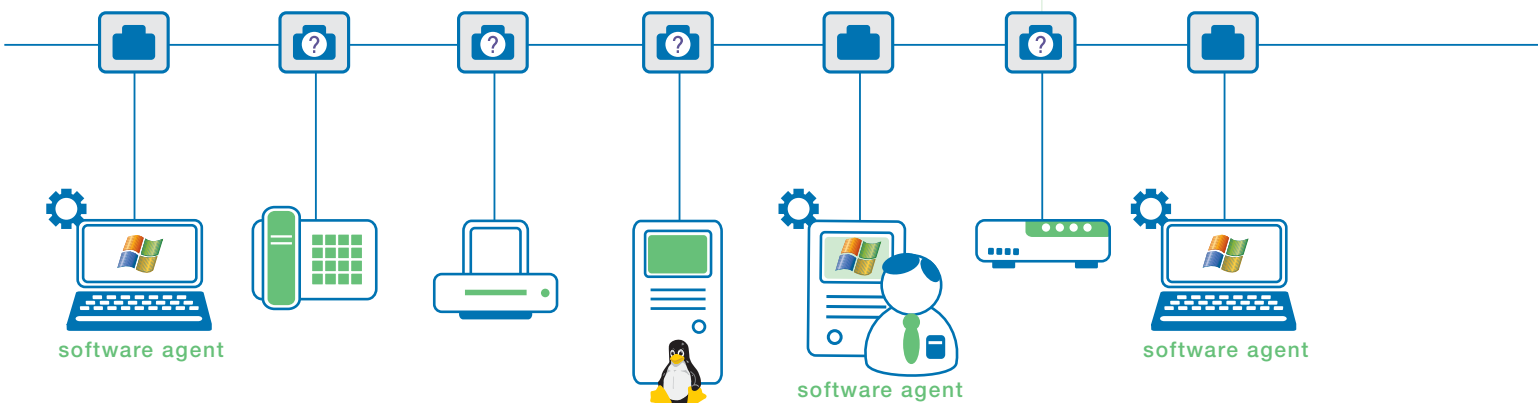
# Network Access Control (NAC)

Network Access Control (NAC) technologies generally require users and endpoints to prove their identity and "state of health" before gaining network access. Most available NAC solutions stop users or endpoints trying to access the network, evaluate their health and match to corporate security policies (using different methods such as designated protocols, software agents or data scanning), and activate remediation and other processes according to the test results. In most cases, such processes relate to the installation and running of anti-virus, patches, service-packs and latest versions of common applications, as well as prevention of use of unauthorized applications and software.

The described conventional NAC approach will not apply for long, though. It is already clear that it takes a lot more than identification and remediation to achieve optimal network security. Based on installation of components (such as software agents and computer certificates) on endpoint devices, the conventional NAC approach is not applicable to hundreds to thousands of non-PC endpoints (such as mobile devices, Unix Servers, phones, printers, IP cameras, legacy systems, etc.), leaving significant parts of the network breached at all times. In addition, it doesn't deal with the identification and handling of events other than an endpoint trying to access the network.

There are many NAC solutions available, most requiring installation of components on endpoints, upgrade of existing network elements or structural network changes. Implementation and deployment processes are usually costly and complex, and may cause decrease of normal business productivity. Despite the complex deployments that conventional NAC solutions require, they still do not address the real IT security threats organizations are facing, due to their inability to support the full spectrum of endpoints, network elements and events.

**Dependent on installation of components on endpoint devices, conventional NAC solutions do not address the real IT security threats organizations are facing, due to their inability to support the full spectrum of endpoints, network elements and events.**



# Access Layers' portnox™

Access Layers' portnox™ is a natural extension to conventional NAC solutions. It represents an innovative approach by which optimal network security can be achieved only by cross-checking information derived from three different IT organizational arenas - networking, security and infrastructure.

portnox™ allows maximized, real-time control over all endpoints and other network elements through infrastructure-based monitoring and handling. It allows the definition and enforcement of unique access control policies for each physical and logical network port, securing those parts of the network which no other solution succeeds. The system is responsible to identify endpoints and network elements and check whether they are authenticated. When authorization is decided upon, the system enforces specific policies which were defined for the actual port the network element is trying to use".

Through continuous real-time network monitoring, portnox™ cross-checks information from various resources to decide which events represent threat and require handling. Such events include any irregular or suspicious network behavior, as well as conventional events such as endpoint access attempts. It uses multiple authentication schemes to identify the network element that initiated the event, all of which are fully transparent and do not require any interference with endpoints and other network elements.

Assessment and validation are based on a unique, patent pending scoring mechanism. Various parameters are matched to decide whether the identified network element is authorized to use the network in the manner it attempts to. Such parameters include the activity's nature, the actual physical location where it was initiated, time of day, the "state of health" of the element's particular Operating System or any installed software it is trying to use, and many others. A grade is assigned for each parameter checked, and a general score is calculated based on all parameters' grades and weight. Authorization is decided upon if the general score reaches a pre-defined level.

portnox™ allows for granular security policies to be dynamically enforced. Through VLAN Steering, endpoint remediation, or interference with specific physical ports, network managers can now decide which endpoints and network elements are allowed to access the network, how, when and where.

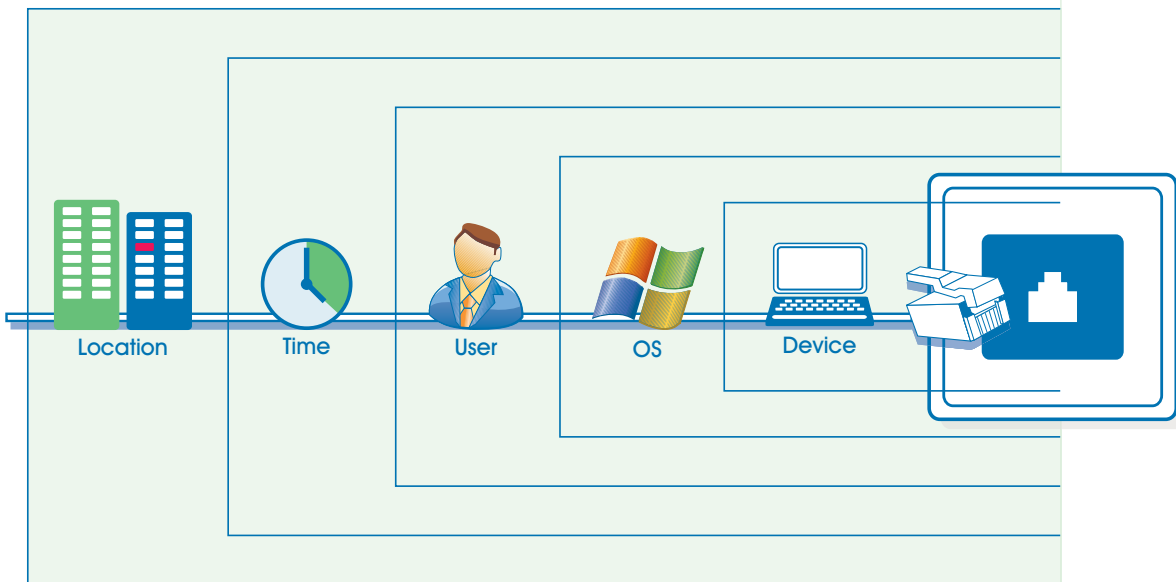
**Through VLAN Steering, endpoint remediation, or interference with specific physical ports, network managers can now decide which endpoints and network elements are allowed to access the network, how, when and where.**



This new approach allows network managers to constantly monitor the network, receive a real-time view of what and who is active within the network, be alerted on any unusual event (such as access attempts, violations, access problems or irregular network behavior), and apply different access control rules in different physical locations, on an ad-hoc or policy basis.

portnox™ addresses both network security and management issues in an efficient, dynamic manner. Complete network coverage, centralized monitoring of physical network access switches and elements, direct switch management and audit capabilities, and real-time alerts on any unusual network behavior - are only part of the portnox™ management offering.

- ▶ Complete network coverage
- ▶ Centralized monitoring of physical network access switches and elements
- ▶ Direct switch management and audit capabilities
- ▶ Real-time alerts on any unusual network behavior



portnox™ illuminates a standard physical ethernet port

# portnox™ Management Environment

**portnox™ unique management GUI "shows security" like no other available solution. It presents data in a clear, summarized manner that informs, illustrates, and illuminates the organization's real-time security status.**

Through its rich management capabilities, portnox™ allows for dynamic operation of network security and administration. It provides network managers with a real-time view of all network members, activity and access attempts, allowing them to identify threats and prevent violations or damage before they occur. At the same time, it provides the ability to easily and quickly perform complex administrative actions and efficiently control network performance and resource allocation.

**Examples for tasks performed using portnox™ management environment include:**

- ▶ Configuration and maintenance of detailed scoring policies
- ▶ Configuration and management of granular access policies based on physical locations or organizational role definitions
- ▶ Real-time configuration and management of access parameters for each physical network port, including the ability to disable ports on an ad hoc or policy basis
- ▶ Disconnection or isolation of systems, users or endpoints in case they generate threatening or unusual security events
- ▶ Handing execution of simple administrative actions over to the IT Helpdesk
- ▶ Efficient resource allocation according to systems, users or endpoints usage profiles
- ▶ Filtered view of valuable statistic network information
- ▶ Rich reporting capabilities

## Benefits

- ▶ Real-time view of all network members, activity and access attempts
- ▶ Identification of threats and prevention of violations
- ▶ Easy and rapid performance of complex administrative actions
- ▶ Efficient control over network performance and resource allocation





# Summary

**Network managers are struggling to maintain a sensitive balance between maximized network security and proper business productivity. portnox™ creates a new context by using the physical port location as a new dimension to network security, allowing it to secure parts of the network that no other solution can protect. Supporting switches, network components and endpoints of all major types and vendors, portnox™ deployment is fully transparent and therefore does not risk performance or productivity at any time.**

In a corporate world in which the amount and variety of network elements expand constantly, network managers are challenged to find and maintain a sensitive balance between maximized network security and proper business productivity.

Analysts suggest that the most effective way to secure networks is using Network Access Control (NAC) technologies. But most NAC solutions available today require significant adjustments to be made to network elements, structure or work procedures, and do not offer complete security coverage which includes all network elements.

portnox™ is a natural extension to available NAC solutions, allowing maximized, real-time control over endpoint network access, through the definition and enforcement of unique access control policies for each physical network port.

Adding the physical port location as a new dimension to network security creates a new context, allowing network managers to decide which users or endpoints are allowed to access the network, when and where. In addition, portnox™ offers centralized monitoring of physical network switches and elements, direct switch management and audit capabilities, and real-time information on any unusual network behavior.

Supporting switches, network components and endpoints of all major types and vendors, portnox™ deployment is fully transparent, does not require any special adjustments and therefore does not risk network performance or business productivity at any time.

Offering complete network coverage, portnox™ secures parts of the network that no other solution can protect, and therefore is a must component within any NAC suite.

## About Access Layers

Access Layers was founded in 2005, with a vision to respond to the pressing need in the security market for systems that will complement traditional LAN security solutions and provide the market with true network control and management capabilities.

Access Layers is headquartered in Hertzlia, ISRAEL.

More information is available at [www.accesslayers.com](http://www.accesslayers.com)

