

# THINK YOU KNOW YOUR NETWORK?

Think again.



## Portnox Platform

While the promise behind traditional NAC solutions such as those provided by the large networking and software giant's has been strong, the delivery on that promise has fallen short and deployments have been largely unsuccessful. At this stage, most enterprises have already gone through at least one attempted NAC deployment and have very little additional control or security to show for it leaving large swaths of the network and many devices out of reach. Moreover, the enterprise network is continuing to evolve faster than ever, constantly introducing new layers and platforms to manage and control.

Through recent years we've seen the introduction and growth of wireless, virtualization, cloud and lately BYOD initiatives that have repeatedly challenged traditional offerings. Common phrases heard during NAC post-mortem discussions are: "too complicated", "extremely cumbersome", "inadequate". In short – they just don't work!

portnox is leading the change on a new way of achieving effective and comprehensive control by providing an easy to deploy solution that covers access control for all IP devices across all access layers, providing unsurpassed network integrity and compliance.

---

## Portnox Platform Solutions

Portnox is a proven server software solution that works with your existing networking infrastructure and deploys on any server. A single portnox software instance can manage up to 20,000 ports across all access layers, multiple sites, network vendors and physical locations.

The Portnox Platform provides complete control of all network elements; 100% network coverage, from initial authentication and compliance assurance to enforcement and remediation.

Portnox is a truly unique 100% 'agent less' server software solution that supports heterogenic environment while providing a complete network/device/user coverage. All that with no MAC addresses nor inventory management; the 802.1x 'standard' is not required and there are no network changes, upgrades or updates called for.

Portnox makes NAC an achievable reality. Upon its deployment, Portnox assumes control and security of any network entry point (access layers) to the enterprise's network from the standard Ethernet to wireless to virtual servers, even to a cloud based service. With Portnox deployed and prior to gaining access to your network, an IP device must be identified as a legitimate, authenticated and authorized device.

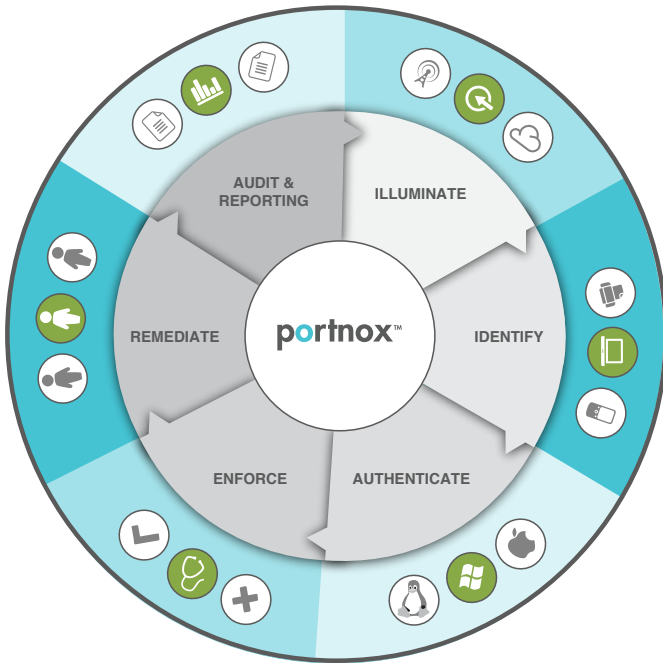
---

### KEY FEATURES:

- A centralized and horizontal management framework
- Seamless clustering & high availability
- Role based access control
- Deployment driven (residents, vouchers)
- Flexible licensing based on port, device & user
- 100% network coverage
- Real-time, visual access control
- Network (BI) analytics
- 100% software, also available as SaaS

Portnox authenticates and authorizes access by providing a robust authentication mechanism and granular NAC policy supported by a unique visualization interface with strong management and access control tools.

## How it works?





### KEY FEATURES:

- Fail open architecture
- Granular 'connection model' and policy options
- Single server manages 20,000 ports
- No traffic mirror / tap / bridge / poison
- True agent-less solution
- Granular 'connect model' and policy options
- Rapid deployment
- 20 different authentication profiles
- Corporate directory, domain & BPX integration
- No MAC address or inventory management
- Scoring based authentication

### With Portnox you can:

- Monitor any access attempt and identify each device and user at the access layer level
- Enforces corporate security & ensures regulatory compliance
- Maintain corporate identity and ensure compliance
- Regain the control of your virtual domain
- Enforce location based access policy
- Get to know who, when, how and where devices and users are taking part of your network
- Protects against the 'unknown-unknowns'
- Maintain granular access control at the level of the access layer
- Contain infected and rogue devices
- Achieve comprehensive network hygiene

### Minimum System Requirements:

 SOFTWARE	 HARDWARE*
<p><b>Operating System:</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows Server 2008 R2</li> </ul> <p><b>Database:</b></p> <ul style="list-style-type: none"> <li>• Microsoft SQL server 2005</li> <li>• Microsoft SQL server 2008 R2</li> </ul>	<p><b>1 CPUs Dual Core Xeon 3.x</b></p> <ul style="list-style-type: none"> <li>• Min of 4GB RAM</li> <li>• 72 GB of disk space</li> <li>• Single network adapter 100/1000</li> </ul> <p>* Available also as virtual appliance</p>