
WHITE PAPER
Rethinking Network Security
Stopping Today's Sophisticated Cyber Attacks
Requires a Review of Essential Security Technologies
portnox™
www.portnox.com

Executive Summary

The proliferation of devices requesting access to the network, driven largely by the adoption of BYOD policies and utilization of IoT devices, has forced network security teams to be more diligent about setting and enforcing effective access control policies.

Despite best efforts, attempts to address this evolving problem are akin to putting a finger in the dike — rogue devices inevitably slip through the cracks, leaving corporate networks vulnerable to ransomware and countless other cyber threats.

What's more, network complexity complicates the issue. Today, networks consist of an ever-increasing number of WANs, LANs, VLANS, SD-WANs, MPLS, VPNs, employees' homes, coffee shops, hotels, airports — wherever authorized devices can connect to gain access to company resources. As if the industry needed another acronym — some are calling it Bring Your Own Network (BYON). Regardless of how we define the trend, access to everything (from everywhere) has changed the security dynamic.

The impact on corporate bottom lines is tangible. The risks and costs associated with network breaches are growing larger by the year. It seems as if every day a new Fortune 500 company is reporting a costly cyberattack. Data breaches from January through September 30, 2021 (9 months), exceeded the total number of events in the entire year of 2020 by 17 percent (1,291 breaches in 2021 compared to 1,108 breaches in 2020). Adding to the challenge, threat actors are becoming more sophisticated and prevalent, leaving organizations on their heels fighting to catch-up.

To make matters worse, most of the available security solutions and toolkits to combat these interconnected problems are insufficient. Legacy on-premise network security software is often too complex to deploy and maintain, especially as IT teams struggle with staffing shortages, skillset gaps and budget constraints. This is especially true for mid-size companies that are particularly time- and budget-conscious and resource constrained.

To support distributed workforces, diverse device types, and increasingly sophisticated cyberattacks, companies need to employ essential network security technology that is powerful, yet easy to implement and manage. Today, companies are forced to choose between expensive, hard-to-manage systems, or a plethora of specialized tools from hundreds of vendors. Both options can and will complicate IT infrastructures, and hamper IT security operations due to deployment and maintenance nightmares.

There is a better alternative for resource-constrained IT teams needing to protect against cyberattacks: a lightweight, cloud-delivered solution that unifies today's network security essentials—authentication and access control, continuous endpoint risk posture assessment and compliance enforcement.

Cyber Threats: Rise in Prevalence, Rise in Costs

Cyber threats have become alarmingly prevalent, with malware increasing 358% overall and ransomware increasing 435% in 2021 compared with 2019.

All threats, from phishing to attacks on Internet of Things (IoT) devices and supply-chains, have grown exponentially. Attacks on IoT devices tripled in the first half of 2019 and supply chain attacks were up 78%.

Costs have escalated in tandem. The average ransomware payment rose 33% in 2020 over 2019, to $111,605. The total cost of cybercrime for each company increased 12% from $11.7 million in 2017 to $13.0 million in 2018. Data breaches cost enterprises an average of $3.92 million annually.

In an attempt to mitigate these costly risks, many companies have opted to deploy niche solutions and tools such as network and host intrusion detection, various threat intelligence feeds, and mobile device management. While useful in isolation, these disparate tools (e.g., Network Performance Management, SIEM, XDR, SOAR, etc.) create many different panes of glass, leaving gaps in network security and complicating IT infrastructures.

All this means extra work for already thinly-stretched IT teams. In this sense, less really is more.

The cybersecurity software market is oversaturated with tools that have been designed for very siloed tasks. Many of these have been developed in direct response to new threats, and require a certain focus and sophistication that doesn't lend itself to the average IT professional's chaotic daily life. Instead, companies need to develop a simple, yet solid security foundation that consists of three essentials:

1. **Firewalls** to monitor incoming and outgoing network traffic

2. **Network access control** to enforce access policies, assess connected device risk and remediate non-compliant devices

3. **Endpoint protection** like antivirus to prevent, scan, detect and eliminate malware and other viruses from devices

Winning the War Against Hackers in the Face of Device Proliferation

With the advent of COVID-19, an enormous push to hybrid work changed the threat landscape.

Many more activities have become remote, and therefore more reliant on and demanding of secure remote network connections. As more organizations expand their hybrid workforce models, the network edge continues to push out and the number of potential entry points for attackers increases. BYOD is exacerbating the trend. As of 2021, 67% of employees use personal devices at work, and 59% of organizations have adopted BYOD.

IoT is also broadening the threat surface, adding to the list of endpoints not only in the office, but also in the operating room, the factory floor and the shipping warehouse. There may be some 21.5 billion IoT devices by 2025 - a number that keeps IT security professionals up at night. From security cameras to connected multifunction copiers, IoT devices open the real potential for breaches.

With so many diverse, dispersed devices requesting network access, security teams must be more diligent about setting and enforcing access control policies. To maintain vigilance, security teams need to focus their efforts on the second security essential we covered above: network access control (NAC).

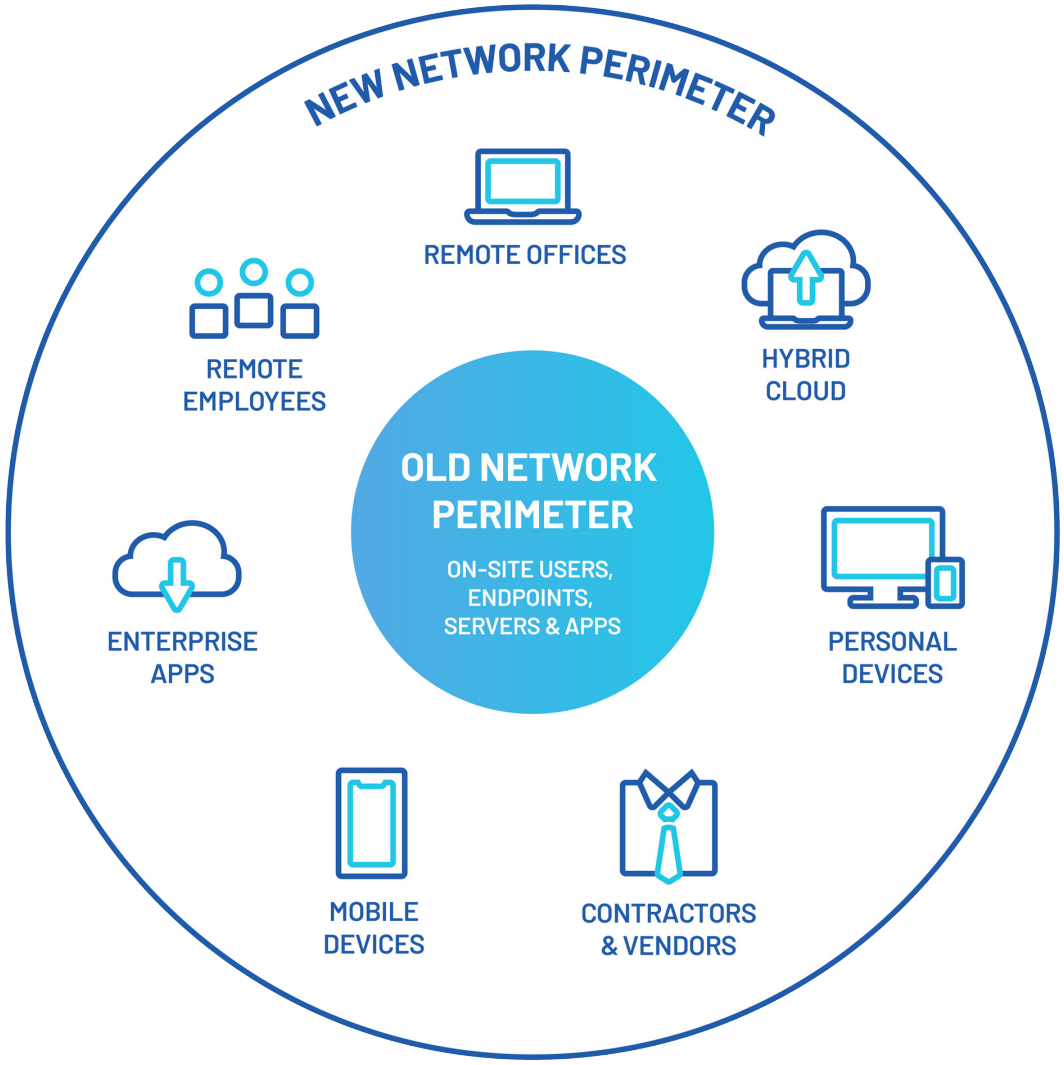
In a perfect world, this means deploying a NAC that offers cloud RADIUS services, a variety of authentication methods, as well as 24/7 endpoint risk assessment and remediation across all prominent access layers — wired, wireless and VPN.

Simple, yet powerful — a NAC that's easy to use while providing the extensive security coverage needed to confront these challenges head-on is required.

Have Our Networks Become Too Complex to Secure?

Even a decade ago, the operations, systems and digital footprints of most medium to large companies had become overwhelmingly complex. Over the last ten years, these digital corporate footprints have expanded to reach and capture growth from previously untapped corners of the world. More recently, the business imperatives of the COVID-19 pandemic spurred faster adoption of enterprise software solutions — (SaaS) — that pushed data beyond the organization's physical perimeter.

The truth is that IT teams have to reassess and realign their priorities. This means leveraging technical security essentials in a way that eases the burden on them. In practice, the first step is to begin adopting network security solutions that accommodate today's most common networking hardware; provide out-of-the-box integrations with critical security tools such as InTune, MFA, and popular SIEM solutions; and work in conjunction with firewalls and endpoint security solutions.



Unlocking Value in Network Security Products

Events like the recently exploited Log4j vulnerability continue to keep IT security teams on their toes.

Little can be done to plan for, let alone prevent, such wide-reaching software flaws — hundreds of Cisco, VMWare, IBM and Oracle products were affected in this instance, including more than 120 different configurations of Cisco Identity Services Engine (ISE).

The unfortunate reality is that these events ultimately mean lost weekends patching systems, as well as assessing the damage done to the network and the devices. In many cases, it means bringing in more skilled professionals to investigate, diagnose, and implement—a costly endeavour you likely would not have budgeted for. Other on-going IT priorities are also inevitably pushed to the side with mitigation underway.

Such exploits and subsequent critical system fixes are particularly hard felt by the mid-market. This segment is often considered the backbone of the economy, yet they're underserved when it comes to having purpose-built network security essentials, including network access control technologies.

For resource-strapped IT teams, these unpredictable security incidents can seem insurmountable, especially when the onus is on the customer to patch their own software.

Constant fire drills lead to stress, burnout and turnover—something many organizations simply can't afford. Instead of helping alleviate IT stress, traditional on-premise network security vendors make the problem worse. Their solutions require extensive, ongoing integration and maintenance. Complicating matters further, specialized point solutions don't mesh easily to provide a holistic view of the network.

This then brings us to the question of value.

Wouldn't it be more valuable to bring in IT security essentials that can reduce this stress and anxiety by eliminating the need for heavy systems maintenance? Wouldn't it be valuable to free up that time spent putting out fires and use it to modernize your IT security stack?

In practice, this means adopting and deploying network security solutions that deliver the essential functionality and capabilities we laid out earlier. It also means turning to SaaS for security. And for network security, it means choosing the right cloud-native NAC.

Key Requirements of Effective Network Access Control

To effectively combat today's network threats and support distributed workforces utilizing a variety of device types, organizations must employ network access control.

But what specifically should an organization look for in a NAC solution? Well, we've laid out some operational necessities to consider:

- Lightweight & Easy-to-Use — A cloud-delivered SaaS solution for network access control—a cornerstone security essential—is ideal because it can be deployed across even the most complex, distributed networks in a fraction of the time compared to legacy on-premise solutions. Unlike NAC appliances that are hosted on public cloud instances and paid for and managed by the customer, cloud-native NACs are delivered as a service. Cloud delivery eliminates the need for IT teams to handle time-consuming and sometimes risky deployment, as well as system maintenance like upgrades and patching. It also takes the need for physical hardware out of the picture. Cloud-native NACs that are delivered as a service provide the latest and greatest access control functionality, and leave the product improvement to the vendor. A cloud-delivered SaaS should also provide a clopud-native PKI as part of the solution, or it should allow customers to use their own PKI if desired.
- Automated Protection, 24/7 — At a minimum, the right NAC should provide 360-degree protection, from device discovery and authentication, to risk posture assessment and remediation. It should allow administrators to easily set access, risk and remediation policies that can be enforced automatically without manual intervention in order to maintain compliance 24/7.
- Universal Endpoint Accommodation — If a device can connect to the LAN, the NAC should be able to authenticate it and enforce the aforementioned security policies. This applies to managed corporate devices like laptops and desktops, as well as BYOD, IoT and operational technology (OT) - no matter whether agentless or agent-based.
- Network Ubiquity — A NAC should accommodate today's most leading networking hardware and architecture, and be deployable across all major access layers - wired, wireless and VPN. Based on in-depth contextual analysis and policy management, a proper NAC solution should be capable of dynamic VLAN assignment and access control policies based upon the roles and permissions granted to the user or device authenticating to the network.

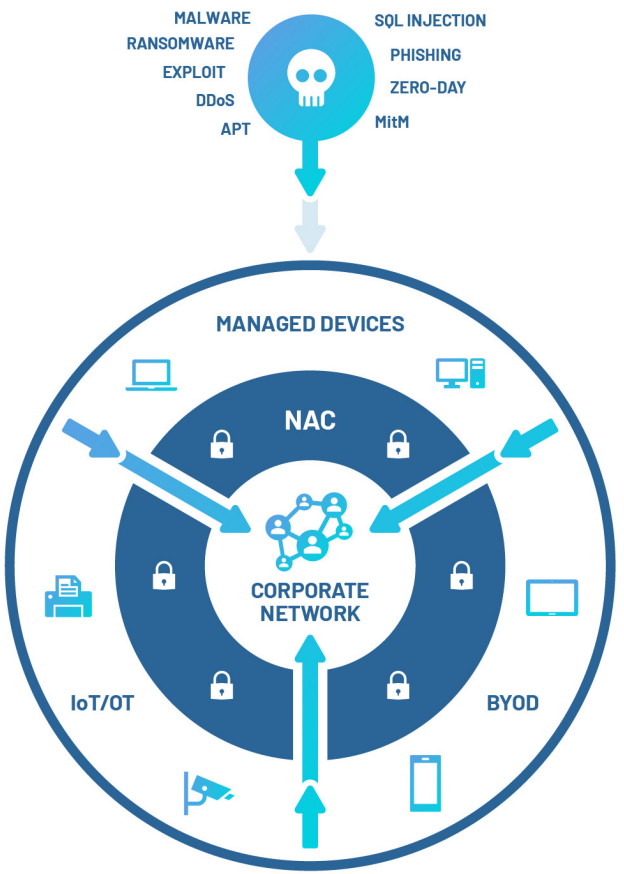
Portnox: Cloud-Native Network & Endpoint Security Essentials

The State of NAC Today

Network access control enables organizations to enact its own unique policy for how and when endpoints (desktops, laptops, smartphones, etc.) can connect to their corporate networks. NAC solutions are typically designed to allow IT security teams to gain visibility of each device trying to access its network, and specifically the type of device and access layer being used (i.e. WiFi, wired ports, or VPN).

Today, NAC provides a number of powerful features on top of what it was originally designed for years ago. These include security posture assessments for endpoints, which pinpoints any associated endpoint risks, allowing network security administrators to control network access based on their organization's risk tolerance threshold. With the rise of cloud computing, remote workforces, bring-your-own-device (BYOD) policies, and the internet of things (IoT), network access control has become a much more critical part of the larger cybersecurity technology stack at most companies. The technology itself has also evolved quite drastically in response to these emerging trends and their impact on networking and ensuring network security.

Legacy on-premise NAC solutions are too complex to deploy and maintain with the internal resources at hand. Either through personal experience or through word of mouth, our core audience is aware of the operational challenges these systems pose. Mid-market organizations have turned to lighter point solutions that focus only on network authentication, leaving them without two critical pieces of the access control pie, specifically device risk monitoring and remediation.



Unlocking Value with Portnox NAC

Portnox NAC provides a variety of unique operational, financial and strategic values to organizations from an IT security perspective. Portnox customers are able to unlock values such as time savings and cost optimization, to IT innovation enablement and executive-level security posture visibility, from the moment they sign up online.

This rapid time-to-value is driven by Portnox's robust feature set:

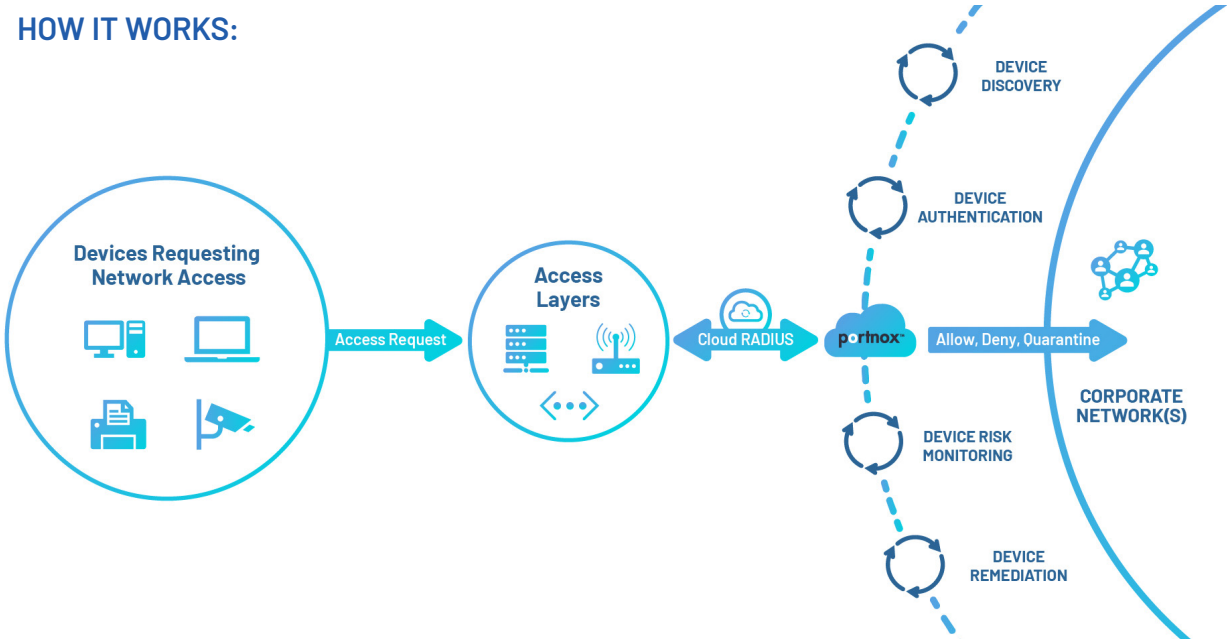
- Network Visibility & Device Discovery — Portnox provides NAC as a true cloud service. This means no on-premises hardware necessary to install on-site and operate, and no on-going systems maintenance such as upgrades and patches. Hosted on Microsoft Azure, Portnox NAC continually delivers the latest and greatest NAC service with unprecedented global scalability and performance.
- End-to-End - Portnox delivers a single source of truth for both network and endpoint security, enabling organizations to enforce powerful network access, and endpoint risk and remediation policies across all primary access layers — wired, WiFi and VPN. Portnox supports network authentication, as well as agent-based and agentless risk posture assessment and remediation for a diverse endpoint set, including managed devices, BYOD, and IoT / OT.
- Ubiquitous - Portnox's cloud-native NAC is available to organizations both large and small, no matter what networking hardware is in use. There is no need to change or migrate networking switches or wireless access points. Simply point your networking appliances to Portnox's built-in cloud RADIUS server, set your policies and move on to the next IT project.

Key Portnox NAC Services

- Authentication Services — Portnox's built-in cloud RADIUS can be stood up with the click of a single checkbox, helping you save time and streamline the deployment process.
- Authentication - Multiple authentication methods are available: role-based, MAC-based, as well as a variety of digital certificate methods, including SCEP. IEEE 802.1X is used universally.
- Account Directories - Roll predefined group policy settings from your Active Directory into Portnox CLEAR to simplify on-boarding. Single sign-on to the network utilizing existing directories and groups from Microsoft's Active Directory, Okta, Google Workspace, OpenLDAP, and Azure AD.
- On-Boarding - Portnox allows for on-boarding of managed devices, BYOD and IoT / OT across all access layers. Unique on-boarding and access control policies can be configured for employees, contractors and guests.

- Microsegmentation - With dynamic VLAN and access control list (ACL) assignment, network administrators can ensure the right people have the right level of access to resources across the network. Automated micro segmentation also helps to limit lateral network movement by potential threat actors, reducing the scope of vulnerability.
- Risk Monitoring - Real-time security risk posturing is available for connected endpoints through the use of Portnox's AgentP or integration with Microsoft Intune. Portnox generates individual risk scores for devices based on critical factors such as the state of antivirus and firewall, open ports, applications in use and more.
- Proactive Remediation - Automatically bring non-compliant devices back to a compliant state by setting unique endpoint remediation policies. Activate antivirus and firewall, remove applications, disable internet sharing and more without any manual intervention for both Windows and OS X devices.
- Multi-Tenancy - Create a single source of truth to manage network security policy enforcement for your entire customer base or individual business entities. Apply unique policies across accounts, or apply universal settings across your entire portfolio.
- Integrations - Leverage integrations with common MFA, SIEM and MDM providers to establish a consistent and operationally efficient security program across your network.
- **Coming Soon: Cloud TACACS+ / AAA** - Secure terminal access to network devices such as switches, routers, firewalls and wireless controllers, and restrict what actions those users can execute while simultaneously providing a full audit trail of who did what when.

HOW IT WORKS:



About Portnox

Portnox offers cloud-native network and endpoint security essentials that enable agile, resource-constrained IT teams to proactively address today's most pressing security challenges: the rapid expansion of enterprise networks, the proliferation of connected device types, and the increased sophistication of cyberattacks.

portnox™

For more information, please visit www.portnox.com.