

NAC-as-a-Service eBook

As organizations move to the cloud, the next evolution of Network Access Control takes shape to meet business demands

Controlling Access Across a Digitally Transformative Network

Network access control solutions have been around since the early 2000s, serving the important purpose of authenticating and authorizing access to the corporate network. These legacy solutions excelled at making access decisions based on authentication credentials and endpoint compliance, but were largely limited in the scope of devices they could see and control. Thus, with the onset of digital transformation, Bring-Your-Own-Device (BYOD) and the Internet of Things (IoT), a new era of NAC was ushered in, which is why the sector has seen consistent growth in recent years (about 20% YoY, according to most estimates).



Even the definition of network access control by market shapers like Gartner has been altered to impart the central role NAC solutions have in securing digitally transformative enterprise networks. According to Gartner's definition¹, "network access control (NAC) technologies enable organizations to implement policies for controlling access to corporate networks by devices such as the Internet of Things (IoT) and by users". Therefore, if the focus used to be on who to let in and who to keep off the network, with digital transformation, NAC's focus has shifted to establishing normal patterns of network behavior so that access can become a more fluid, yet inherently secure process. To put it briefly, NAC solutions are key in making the transition to digital transformation smooth and secure.

Some of the challenges arising from digital transformation that NAC solutions address:

- Encouraging workforce mobility and productivity while maintaining control over network security
- BYOD and the move to mobile – controlling more endpoints than ever before
- Internet of Things and the connected enterprise
- Integration and on-boarding process

¹ Gartner Market Guide for Network Access Control, Claudio Neiva, Lawrence Orans, May 9, 2017

2 WHAT IS NAC-AS-A-SERVICE?

Securing Digital Business Risk Starts with Knowing What's on Your Network

NAC-as-a-Service makes the traditional capabilities of NAC solutions – authentication, authorization, and endpoint security assessments – available from the cloud as a service. Not only does the pricing model change – shifting from port-based pricing and one-time fees in legacy solutions to the “as-a-service,” subscription-based model – but the capabilities and extent of the network view dramatically expand.

In addition, NAC-as-a-Service is part of a trend within digital transformation to control business risk, as opposed to just IT risk, and serves the growing demand from CIOs to move to cloud services and solutions that will differentiate their company from the competition. Indeed, this round of digital transformation is really the first time that IT is being valued strategically in overall corporate strategy, and decisions on company architecture are made not only by CIOs/CISOs, but CEOs and board members too. Gartner² further predicts that by 2021, 40% of IT staff will be versatilists, or hold multiple roles that will be business, rather than technology related.

Which technological areas do you think are most important in helping your business differentiate itself and achieve your organization's mission?

Technologies expected to help businesses differentiate themselves from their competitors

Percentage of Respondents	Total (n = 2,834)	Top (n = 165)	Typical (n = 2,476)	Trailing (n = 193)
BI/Analytics	26%	28%	26%	20%
Digitalization/Digital Marketing	14%	17%	14%	12%
Cloud Services/Solutions	10%	15%	9%	8%
Mobility/Mobile Applications	6%	7%	6%	5%
Internet of Things	6%	6%	6%	6%
Customer Relationship Management	5%	1%	5%	6%
Artificial Intelligence	5%	7%	5%	1%
Enterprise Resource Planning	5%	1%	5%	9%
Infrastructure/Data Center	5%	3%	5%	4%
Automation	4%	2%	4%	3%

These factors and more place NAC-as-a-Service solutions at a critical juncture where they must prove their added value in securing the digitally transformative network, while creating the utmost flexibility and instilling a feeling of user-friendliness that many legacy solutions lack.

² Gartner Press Release “Gartner Reveals Top Predictions for IT Organizations and Users in 2018 and Beyond”, October 3, 2017, <https://www.gartner.com/newsroom/id/3811367>

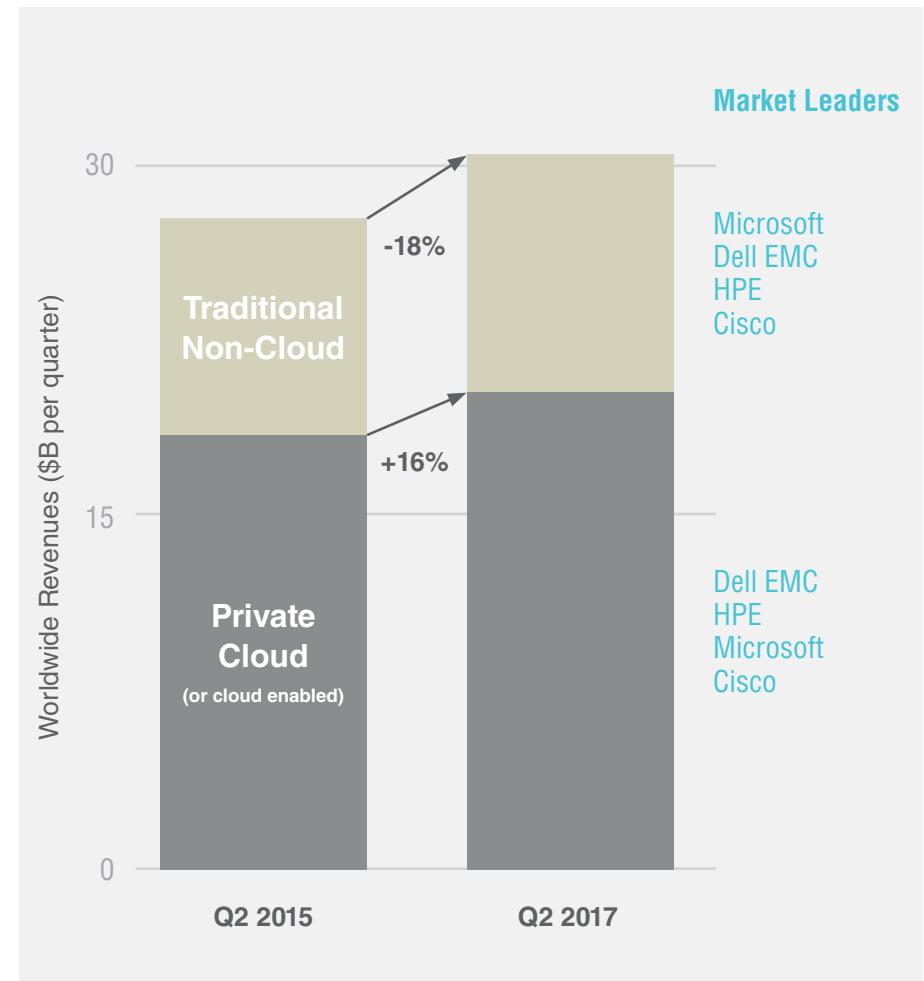
2 WHAT IS NAC-AS-A-SERVICE?

Growing Cloud Investments

While there has been hesitance in the security community over the adoption of cloud, a survey of IT spending shows that investments are increasingly being made in the cloud. According to a Synergy Research survey of IT professionals, spending on traditional, non-cloud data center hardware and software dropped 18% between the second quarters of 2015 to 2017. During that same period, however, private cloud/cloud-enabled solutions grew by 16%.

To summarize, as enterprise moves into a digitally transformative landscape, “digital security will continue to be the number one barrier to entry to digital business,”³ creating a unique opportunity for NAC-as-a-Service solutions to protect complex corporate networks.

Data Center Infrastructure Market



³ Gartner Hype Cycle for Cloud Security 2017, Jay Geiser, July 17 2017

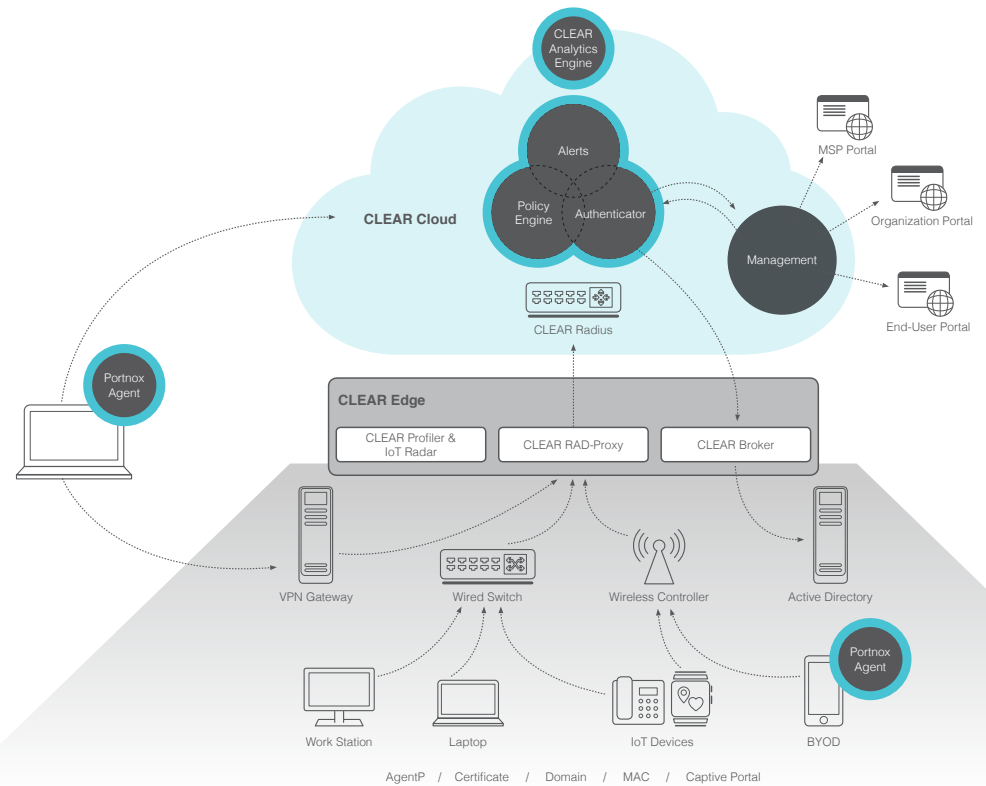
Source: Synergy Research Group

3 HOW DOES IT WORK?

NAC-as-a-Service eliminates the need for appliances by deploying them from the cloud – RADIUS servers, certificate authority, databases, analytical engine and management, all of that already deployed and ready for use. The cloud service is connected to the on-premise organization infrastructure using an optional broker. For example, using an Active Directory broker to connect the enterprise directory to the cloud, or using an optional radius proxy which connects to the switches, wireless controller and VPN gateway. Those optional brokers are managed and upgraded seamlessly from the cloud and can provide access when there is an internet outage.

The solution also consists of endpoint risk-assessment. This can be done either without an agent, by utilizing the broker scanning capabilities, or by deploying agents to mobile endpoints, such as BYOD and laptop devices. With persistent agents, NAC-as-a-Service is able to provide both on and off premise visibility, control and management of these edge devices, in all locations and at all times.

The same goes for IoT devices that are connected to wired and wireless networks, allowing IT staff to set specific security policies for these devices and enforce them any time and from any place.



4 WHY DO NAC AS-A-SERVICE CAPABILITIES MAKE SUCH A DIFFERENCE TO BUSINESSES?



What are the Capabilities of a NAC-as-a-Service Solution?

In our current times of digital transformation, the capabilities of network access control solutions have widely expanded. If they used to be the authenticators and authorizers for users and devices accessing the corporate network, their capabilities have expanded to include advanced and automatic endpoint compliance checks, robust guest access policies, and controlled access for IoT devices.

4 WHY DO NAC AS-A-SERVICE CAPABILITIES MAKE SUCH A DIFFERENCE TO BUSINESSES?

In this context, NAC-as-a-Service solutions expand on these capabilities providing:



Instantaneous Deployment

If legacy NAC solutions can get tied up in deployment (depending on if the solution is agent-based or agentless), NAC-as-a-Service solutions have no such problem. Similar to other cloud computing solutions, there is no need for additional hardware or software and the solution is deployed as-a-service over leading cloud storage services, such as Microsoft Azure. For highly-secure industries, NAC-as-a-Service also offers the options of keeping Active Directory and RADIUS servers on-premise.



Complete Visibility

A key feature of any NAC solution, NAC-as-a-Service extends the visibility of existing NAC solutions across all endpoints and cloud applications. Together with the easy method of deployment, system admins gain seamless visibility into all endpoints without the use of an agent. In addition, it's possible to filter the Network Access Server (NAS) view according to a number of different parameters, including geographic location (both on campus and remote), time of last login, and level of endpoint risk. This data and more can be used to create a complete map of network behavior.



Automate Controls

With cyber threats increasing at an unprecedented pace, it no longer makes sense for IT professionals to manually track threats on managed endpoints. Instead, with NAC-as-a-Service solutions, they have automated controls based on a device's unique risk score. Devised from machine learning of endpoint behavior, the risk score is clearly marked for endpoints that are placing the network security at risk, and for those that can be allowed to conduct their business without disturbance. After defining company policy, system admins can decide the level of risk score that denotes quarantining, blocking or conditioning patching a certain endpoint.



Easy 802.1x

A NAC-as-a-Service solution allows for simple deployment of 802.1x authentication, without compromising on security across the enterprise and allowing admins to embrace the trustworthy method of authenticating devices on the corporate network.

4 WHY DO NAC AS-A-SERVICE CAPABILITIES MAKE SUCH A DIFFERENCE TO BUSINESSES?



Understand Your BYOD & IoT Ecosystem

One of the biggest challenges of digital transformation for IT professionals is that they want to encourage their employees to use technology, and reap the financial benefits that result, but are concerned about the digital risks they can expose the organization to. That's why gaining visibility of the applications, location, security posture and access permissions for BYOD and IoT devices is more important than ever. NAC-as-a-Service also provides ways to control these endpoints so that if they are "always on," your network security can be too.



Build Tailored Network Security Policies

With the extended network views of a NAC-as-a-Service solution, IT professionals can spend more time on value creation and business critical tasks, such as devising an access policy that suits the needs of their organization. If the company has many remote employees or contractors, the system admin can set up geographic policies that control where the corporate network can be accessed from. For example, if there is a concern regarding threats from a particular OS, policies can be set up by IT professionals to restrict all access for any device using that OS.



Optimized Guest Access

Guests, visitors, consultants and contractors are becoming a central part of the digitally transformative enterprise, however it is often difficult to decide what level of access to give them. With NAC-as-a-Service solutions, you can control access to your file-stored and cloud-based resources with the click of a button, making access decisions based on the needs of each guest. There are options for sponsored access, multifactor authentication access, disclaimer-based access and more.



Powerful Security Integrations

One of the cornerstones of a successful NAC solution has always been the level of communication and integration with other cybersecurity solutions. This is important because with both on-premises and NAC as-a-Service, organizations can use featured tools such as mobile device management for IoT and BYOD; as well as vulnerability and threat detection tools to enhance their access control capabilities and retain clear visibility of all devices on the network. An additional advantage to implementing NAC as-a-Service is that integrations with existing or new security solutions are a breeze, as information is shared freely to create a flawless security stack.

While these are only some of the capabilities of NAC-as-a-Service, as the enterprise transforms, so do access control solutions. Yet it is clear that, at the moment, NAC-as-a-Service is able to effectively cover a number of important bases for the digitally transformative enterprise, namely: network visibility and control – both on and off campus, BYOD and IoT controls, automated actions based on endpoint risk scores, guest access management and more.

How does the Cloud Enhance Control Capabilities?

One of the initial questions asked by nearly every potential NAC-as-a-Service client is, “How does NAC-as-a-Service differ from NAC?” The assumption is that only the method of deployment differs, i.e. from the cloud for one and from the on-premise server, software, or hardware, for the other. But the real difference between NAC-as-a-Service and NAC is far more complex than a deployment and pricing model; it has more to do with making NAC solutions more powerful and essential to security than ever before.



Use Case #1 Controlling the Remote Workforce

Companies from all over the world are allowing their workforce to perform duties outside the office, and from distant locations such as home offices, coffee shops, restaurants, hotels and more. This is possible due to the advancements in mobile technology and network infrastructures. While the benefits to both the organization and employee are clear (increased retention, reduced capital expenditures, and flexibility), it raises major security concerns for IT departments.

The Challenge

The biggest concern today with employee mobility is the potential impact on data and network security. Cyber-criminals have been known to target remote workers, developing malware that identifies programs installed on a remote desktop to determine whether this employee's data is worth gathering. Additionally, immediate access to company documents, emails, and applications creates loopholes for cyber-criminals looking to infiltrate a company's network.

Many companies require remote workers to log in with virtual private networks (VPN), but that could be tough to enforce. For convenience, workers might use

their own Internet connection or set up in a coffee shop and use public Wi-Fi. Employees on business flights or overnight hotel stays typically connect via airport or hotel Wi-Fi, meaning that they are using open connections accessed by thousands of other travelers every day. Using these connections could open gateways for hackers into the enterprise network.

Additionally, the changes to computing infrastructures has made remote employee network security more challenging. Typically, full-time remote workers use company-issued devices, and traveling contract

workers connect on personal devices to carry out work-related tasks. Some industries, such as education, actively support more diverse endpoints since they have an ever-changing roster of students and faculty members relying on BYOD policies. This combination of personal and company devices, each with potentially different operating systems, decentralizes management and increases the challenge to keeping data safe. Compounded with the fact that mobile devices are more easily lost or stolen, having a remote workforce security strategy in place is imperative.

5 USE CASES

The Solution

With the onus on remote workers to keep their machines and devices updated, there's a lot of room for error. Out-of-date software, plugins, and browsers, plus unpatched and unprotected systems leave remote employees even more vulnerable to attack. With Portnox CLEAR, organizations can gain full visibility of their network endpoints from the cloud, giving IT departments the contextual endpoint knowledge they need in order to know that their data and networks are secure, despite the widespread use of BYOD. They can know where and when endpoints are connecting, if they have been patched for the latest vulnerabilities, and if they are sharing or accessing sensitive information in an abnormal fashion that could raise red flags.

Portnox CLEAR achieves this by enabling risk-based access for all endpoints. Risk-based access means that only devices that adhere to the network security policy will be permitted on the network, significantly minimizing unnecessary exposure to digital business risks and providing network security admins with leverage to enforce their policies. It does so by generating unique risk scores for each device, allowing network administrators to create accurate risk profiles of their networks, and helping them gain an understanding of underlying network vulnerabilities.

Also, as most of today's businesses use SaaS platforms to conduct business, with Portnox CLEAR, it's possible to control access to those applications based on strong authentication credentials – a necessary step in our increasingly connected world— to prevent unauthorized access.



Use Case #2

Minimizing Window of Vulnerability for Global Companies

Often, today's enterprises have a global presence with offices all over the world. For companies doing business on a global scale, regional offices allow for streamlined business operations and reduce the potential for cultural barriers. However, with a global workforce, CIOs and CISOs are faced with the challenging task of securing multiple offices dispersed across the world.

The Challenge

If a vulnerable device is attempting to connect in a regional office, it puts the entire global network at risk. Streamlining security measures is a crucial challenge associated with securing multiple offices across the globe. Many traditional NAC solutions are on-premise, requiring physical installation and securing a network as a defined infrastructure within a physical firewall. This limits scalability and agility,

as installation is required per office. As a result, it's more difficult for IT staff to leverage one solution for network visibility and monitoring.

Furthermore, device authentication and authorization can be challenging in a global company, as transferring data between a regional office and the headquarters can be a slow process. For instance, if a new device in the London office is attempting to

join the corporate network of a US-based company, information about that device needs to reach the US office for evaluation.

Operating without streamlined network visibility, and a potentially unreliable device authentication process, there is greater opportunity to overlook security threats, putting the global network at risk.

5 USE CASES

The Solution

Like other cloud computing solutions, a NAC-as-a-Service product doesn't require any hardware or complex installation, and can therefore be applied across a global network from the cloud. Since deployed as-a-service, it is easier than ever to add new devices and even offices, improving scalability.

With a NAC-as-a-Service solution like Portnox CLEAR, organizations can monitor network activity across the board, monitoring all offices from the cloud in a single platform. With CLEAR, IT staff can filter device information based on various parameters, including geographic location, allowing for a better understanding of device behavior per region.

Portnox understands the need for streamlined and seamless business processes, including device authentication. Portnox CLEAR makes authenticating a new device quick and easy with its Geo-Distribution feature. It does so by authenticating devices from the nearest data center rather than being sent to headquarters, helping customers grow on a global scale by authenticating devices more efficiently.





Conclusion

With the growth of BYOD, IoT and mobile workforces, the need for control over network endpoints is more important now than ever before. The visibility and control offered by NAC-as-a-Service solutions allow CIOs and CISOs to fully embrace the benefits of digital transformation, but as enterprises transform, the solutions should do the same. NAC-as-a-Service is the next generation of NAC, deployed from the cloud as a service, allowing small and large businesses alike to monitor and secure their entire networks with ease.

Portnox CLEAR: Value Proposition

Portnox CLEAR is a NAC-as-a-Service solution that simplifies the management of emerging cyber risks in the enterprise.

Together with its light-weight architecture, built from the ground up in the cloud, CLEAR has all of the benefits of a SaaS solution paired with robust access control and network visibility capabilities.

CLEAR is made up of holistic risk and threat management tools, performing vulnerability assessments, automated patch controls and collecting threat intelligence feeds for all endpoints accessing the network – regardless of their physical or logical location.

Based on detailed risk assessments, CLEAR grants, denies, or limits access to the network while providing full visibility into the state and behavior of network devices.

Drawing on advances in machine learning, CLEAR is armed with a thorough analytical engine to detect emerging digital business risks, cyber breaches and network anomalies in real-time.

TRY IT NOW 



About Portnox

Portnox secures connected organizations' corporate networks utilizing its next-generation network access control and management solutions. Portnox's solutions manage every user, every device – including: Internet of Things (IoT), BYOD, mobile and managed devices – accessing the network, everywhere.

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

portnoxTM