WHITE PAPER

Cloud-Native Network Access Control

Why Moving NAC to the Cloud Enables Organizations to Combat Today's Biggest Network Security Challenges

portnox™

www.portnox.com

The Shortcomings of Legacy NAC

Network Access Control (NAC) sits within the larger field of cybersecurity, and more specifically network security.

It is a technology that 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. The use cases for NAC today are constantly expanding.

Network security professionals leverage NAC solutions for network visibility, the discovery of endpoints, security profiling, compliance enforcement, remediation ... the list goes on.

The problem, however, is that traditional legacy on-premises NAC products have evolved into massive, monolithic systems that are very heavy to deploy and often require extensive professional services agreements to get off the ground. What's more is that because these traditional NAC systems are on-premises or merely cloud-managed, they require on-going upgrades, patches and on-site appliances across each site. This can be backbreaking work,that many lean IT teams simply are not equipped to manage on a regular basis. It would come as no surprise that many organizations that choose to deploy these feature-rich, yet difficult to manage solutions experience vendor lock-in. This can persist for years.

Today's Top Network Security Challenge

Increase in Network Complexity

Today, corporate networks are expanding and evolving in true Darwinistic fashion thanks to architectural advancements, new networking protocol standards, device proliferation, hybrid work policies...you could write a dissertation on this topic alone. The point is: the corporate network now extends to wherever authorized devices can connect to gain access to company resources. All of this proprietary, confidential or merely sensitive data being accessed across these parts of the network is no longer safe behind your castle walls. The physical headquarters still exists, but it's basically just a "fat" branch like any other satellite office or employee working from home.

Increase in Devices

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.

Increase in Cyberattacks

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.

Increase in Vendor Complexity

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:

Why NAC is Essential to Combatting these Challenges

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 definition, "NAC technologies enable organizations to implement policies for controlling access to corporate networks by devices such as 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 is a critical technology when it comes to strengthening your network's security posture.

Common NAC Use Cases

A NAC solution's primary function is to deny access to unauthorized devices or users while allowing authorized devices and users appropriate access. Additional functionality of NAC solutions includes the following:

- Authorization of users and devices
- Discovery of all devices on the network
- Device posture checking
- Quarantine of unsecured devices
- Policy lifecycle management
- Overall security posture assessment
- Automatic policy enforcement for incident response
- Guest networking access
- BYOD enforcement
- Device posture check during remote access (VPN)
- Enforcing time and geography access policy

In the modern world, physical and virtual devices often repeatedly join and leave a network, and the devices themselves can vary greatly in their risk profile. Understanding the different use cases for this technology informs a more comprehensive NAC solution. Common use cases include:

- IoT — The use of IoT devices only continues to grow. This includes their use in Operational Technology (OT) settings and connections to enterprise networks from home networks. Such devices can go unnoticed or unmonitored by older NAC solutions, making them a prime source of exploitation for cybercriminals. The right NAC solution will identify and monitor IoT devices, in addition to traditional devices.
- BYOD — With employees working remotely from personal computers or accessing the corporate network from personal phones, a proper NAC solution must also be able to handle permissions and authentication of unfamiliar devices attempting to access the network.

- Incident Response — In addition to simply controlling network access, a robust network access control solution should be able to respond to threats quickly and effectively. This is where automation comes into play. Automation in a NAC solution enforces security policies, shares contextual information, and isolates insecure devices at the point of connection to the network before they can do any damage.
- Contractors — Often, companies want to allow contractors, partners, or temporary workers access to only certain parts of the network. NAC can be used to maintain access privileges and prevent unauthorized access to certain parts of the network while ensuring guest users have smooth connectivity and a good experience.
- Medicine — In the world of healthcare, there is a growing reliance on the Internet of Medical Things (IoMT) devices. But healthcare is a highly regulated industry, and network compliance is vital. Properly structured NAC solutions can provide the necessary protection of sensitive personal data and medical records in a network with multiple users and IoMT devices.
- Compliance — Organizations can be fined if they do not meet regulatory requirements for their respective industries. NAC solutions can be considered a form of risk mitigation that helps enforce compliance controls under regulations such as HIPAA, SOX, or PCI-DSS.

NAC Functionality “Must-Haves”

- Network Visibility & Device Discovery - A NAC solution discovers and identifies all devices/users in the network before they are granted network access, requiring continuous monitoring of the network and devices connected to it. The system enables the discovery, classification and assessment of every device connected to the network. Configuration and security state of every device is monitored, ensuring that the network and devices are compliant to the organizational security policy.
- Full Access Layer Coverage - As today’s networks explode in size and scope, particularly with remote workforces on the rise, it’s imperative that your NAC solution can manage access control across all existing access layers. This includes the obvious – wired ports and WiFi. It also must be able to manage the various remote access methods used within your organization. These may include VPN, Teleworker Gateways, and beyond.
- Authentication Services - Traditionally, enterprises have enabled network authentication via usernames and passwords. As we now know today, this method of authentication can be easily compromised by bad actors, making it no longer sufficiently secure for enforcing network access control. Any NAC worth its salt should offer several methods for authentication, including: role-based, MAC authentication bypass (MAB), and certificate authority.
- Device On-Boarding - Business units and even departments (think Finance & Accounting, for example) often have their own VLANs since they’re dealing with very sensitive, confidential data. The task of setting up such VLANs and onboarding new devices is just one of dozens of tasks overseen by frequently overburdened IT teams. So, if not done correctly at first, it can open the door to potential network vulnerabilities, such as a person gaining access to a part of the network he/she

should not have the privileges for. At a small scale, managing access manually is often sufficient. For larger organizations, however, this just isn't sustainable. As a result, many large organizations that don't have a secure onboarding process will often compromise on network security hygiene.

- Policy Configuration — Network security teams define and activate access control policies to control device access to the corporate network, which is ultimately based on the device authorization state. Once a device is authorized for network access, a network access policy determines which specific virtual LAN (VLAN) that device or user is directed to. On top of that, the policy also defines, for each type of authorization violation, whether to deny entry or whether to quarantine the device by assigning it to a specific VLAN or apply an access control list (ACL).
- Endpoint Risk Monitoring — Your corporate network is only as strong as its weakest security link. This means continuous risk posture assessment is paramount. By continually monitoring the network, your network and security teams can stay ahead of cyberattacks with the ability to identify new risks in real-time, react to these risks, and take action. In a world with ever-expanding boundaries and an exponential increase in types of endpoints, continuous risk posture assessment must function no matter location, device type, or the type of data being transferred.
- Device Remediation — Having a rapid remediation plan in place will not only help prevent further damage or the lateral spread of attacks but also allow for business continuity. Effective endpoint remediation consists of:
    - *Automated Patch Updates Across the Network* — Enforce necessary patch, anti-virus, operating system, and application updates across managed and unmanaged endpoints.
    - *Immediate Incident Response* — Contain ransomware events by remotely disconnecting endpoints from the network without the need for manual intervention.
    - *Armed Incident Response Teams* — Arm IT professionals and network admins with the ability to remotely take actions on employees' devices. The proliferation of IoT devices over the last decade has prompted a growing number of network security concerns. With all of these devices — printers, CCTV cameras, ATMs, MRI machines, etc. — now connected to their respective networks, it's exponentially expanding corporate threat surfaces.
- Compliance Enforcement — NAC is used to enforce regulatory policies and maintain compliance across the organization. In practice, this typically means:
    - Understanding how mobile, BYOD, and IoT devices will affect and transform not only the organization but the industry and implementing the right processes and tools control them.
    - Tracking any network related device or program in real-time via a centrally secured platform providing full and actionable visibility.

- Controlling access to the network and to cloud applications, even based on the geographical locations of users.
- Ensuring that the business is in compliance with governmental regulations like SOX, PCI DSS, HIPPA, FINRA, FISMA, GLBA among others. Strict compliance will provide legitimacy with clients and partners.

Cloud-Native vs. Cloud-Managed

For IT and security teams with limited staff and tight budgets, cloud-native software-as-a-service (SaaS) security products offer tremendous value. Some CIOs have even mandated that new security tools be delivered in the cloud where possible. Some vendors with older on-premises products have tried to sneak in their products by claiming they are now "in the cloud," but the truth is that that is a façade.

Let's call these products "faux" cloud security to contrast against products that are truly "cloud native." Vendors of faux cloud products hope that with a little marketing smoke and mirrors, they can use some "cloudy" language and potential buyers will not know the difference. When we say faux cloud, technically speaking, we mean that the vendor is just allowing the customer to host their on-premises product in the customer's public cloud account. This means the customer still must install, configure, deploy, maintain, update, and eventually decommission that product.

In other words, you as the customer must do all the work. The only "cloud" aspect of this arrangement is that you can do all the work on a server you are renting (that is, paying for) from AWS, Azure, Oracle, Dell, etc.

A real-world example of this software sleight-of-hand is Cisco's Internet Security Engine (ISE). Cisco delivers ISE as a virtual appliance to handle network access control (NAC) – a critical component of any effective cyber security stack. As of ISE's latest version, a customer can deploy the software in their own AWS or Azure accounts. That is the long and short of it, however. The well-known challenges of setting up ISE – or any other network security appliance – remain. It is difficult to get your ISE server configured properly, ensuring it communicates with all your network equipment, even after having committed over 1,200 pages of ISE documentation to memory.

As a potential customer, how can you distinguish cloud-native from faux cloud?

There are a few telltale signs. The table below summarizes some of the most salient differences. When you evaluate a new vendor, be sure to ask questions such as who is paying for the infrastructure? Who is responsible for updates and upgrades?

	Cloud-Native	Cloud-Managed
Infrastructure	Provided, paid, and managed by the vendor; mostly invisible to anyone utilizing the service	Provided, paid, and managed by you through your own AWS or Azure account
Implementation	Quick time to value; much of the work is invisible to you	Depends on the complexity of the app, but it is your responsibility to do the work or pay someone else to do it
Pricing	Subscription with lower up-front cost	Perpetual license with expensive up-front cost that is amortized over time. *(Note: many vendors are moving away from perpetual licensing for on-prem or faux cloud products, but as they do, their customers are getting the worst of both worlds – paying more annually while still being responsible for on-going maintenance of the product)*
Total Cost of Ownership	The price of the product reflects the genuine cost of ownership	The price of the product is only one (and sometimes only a small) part of the total cost that is reflected in the staff time and public cloud expenses; in many instances, you may not even know what it is going to cost you until it is too late
Vendor Lock-In	Easy to switch to another vendor should your business needs change	Expensive license, deployment and maintenance costs make switching prohibitive, often for years
Access	Access anywhere via browser with internet connection	On-premises model often requires access via VPN *(Note: what happens when your solution has a problem there is a problem with your solution and your VPN is configured to use your on-premises system? It sSounds like someone is driving into the office!)*
Scalability	Automatically scales with usage	Depends on the complexity of the app, but it is your responsibility to do the work or pay someone else to do it
Updates	Vendors regularly update the underlying components such as servers, databases, etc. This process will often be invisible to you.	You are responsible for ensuring that the entire tech stack — components, databases, servers, network — is updated with the latest patches
Upgrades	You seamlessly and transparently reap the benefit of new features, enhancements, and other improvements with zero effort	Any upgrade requires you to install, test, and then deploy the upgrade in production, often during nights and weekends, in case something goes wrong
Accountability	The vendor takes ownership of the uptime and security, performance, and availability of the service	Apart from the infrastructure as a service, you are on the hook for the performance, health, security, and availability of the solution, lock stock and barrel

Portnox Cloud-Native NAC: The New Gold Standard

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:

- Cloud-Native / SaaS — 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.

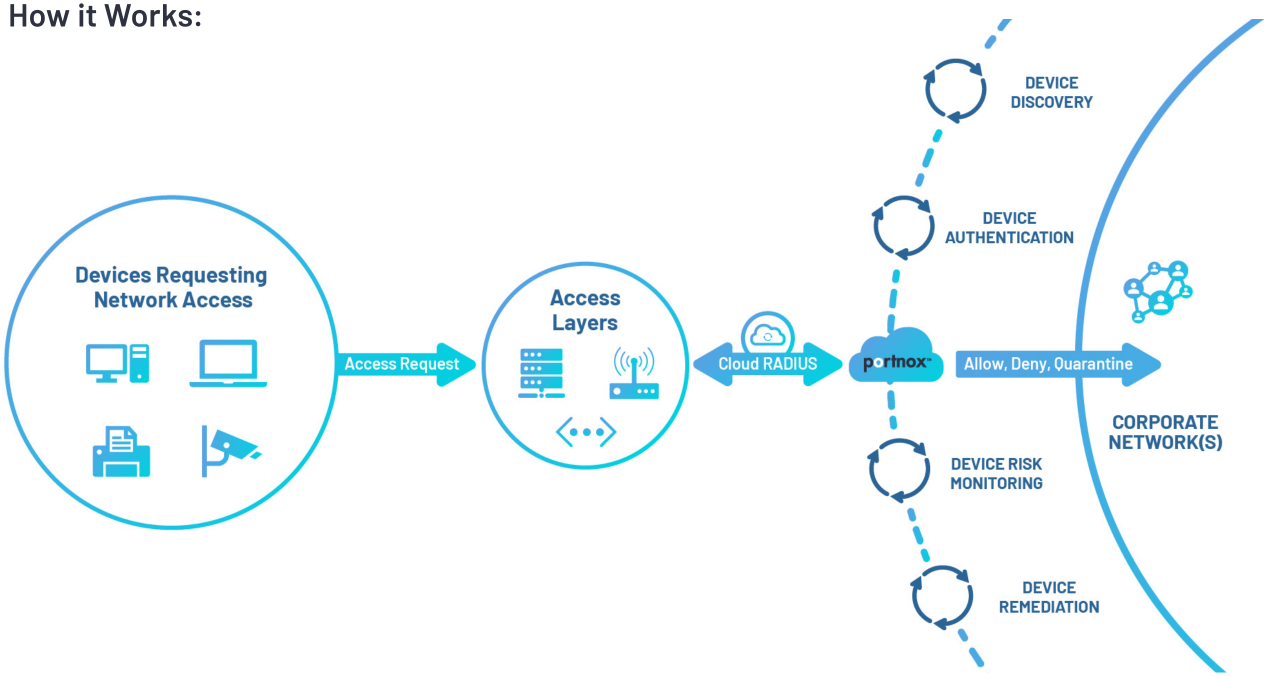
Unique Portnox NAC Services

- Cloud RADIUS — 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,

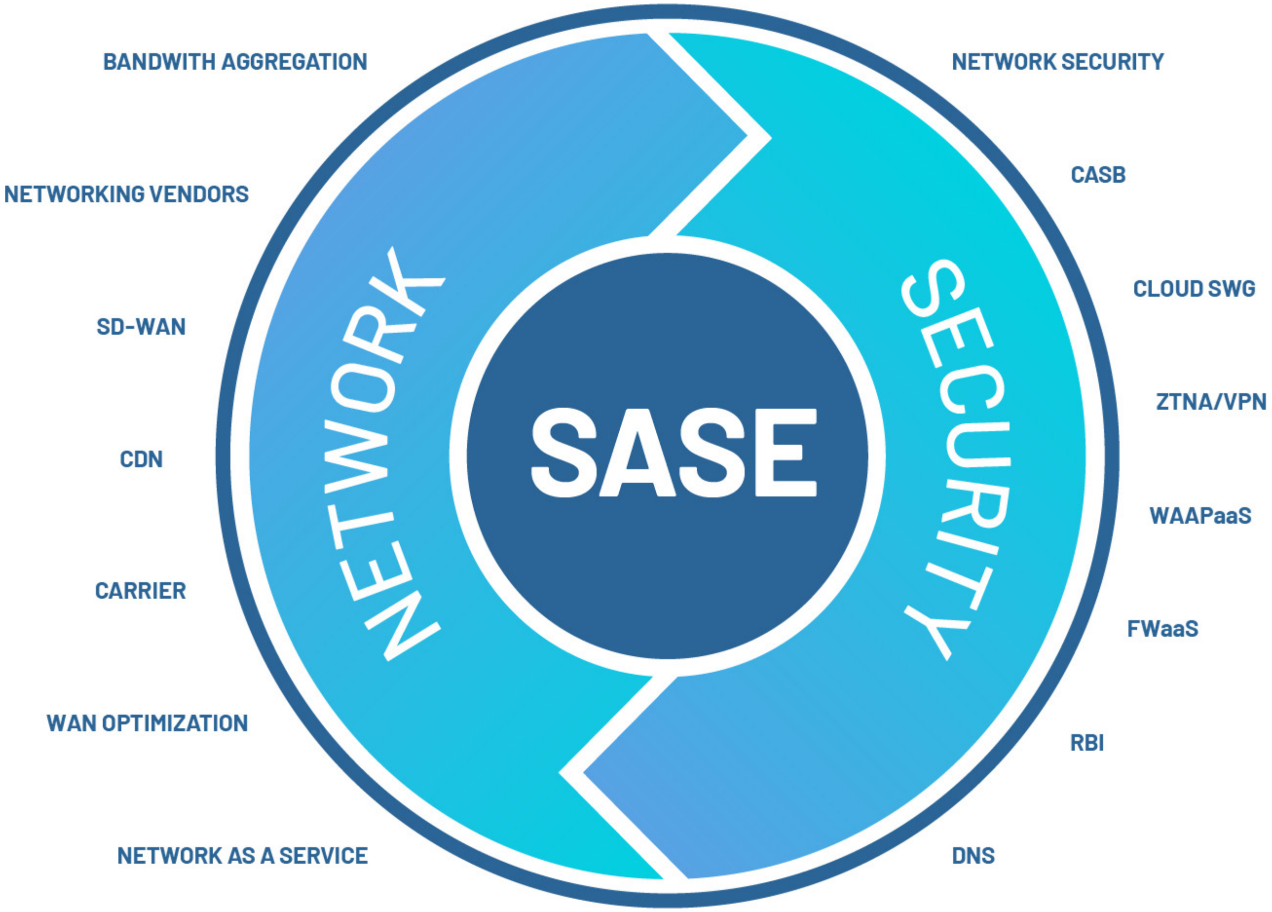
network administrators can ensure the right people have the right level of access to resources across the network. Automated microsegmentation also helps to limit lateral network movement by potential threat actors, reducing the scope of vulnerability.

- 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:



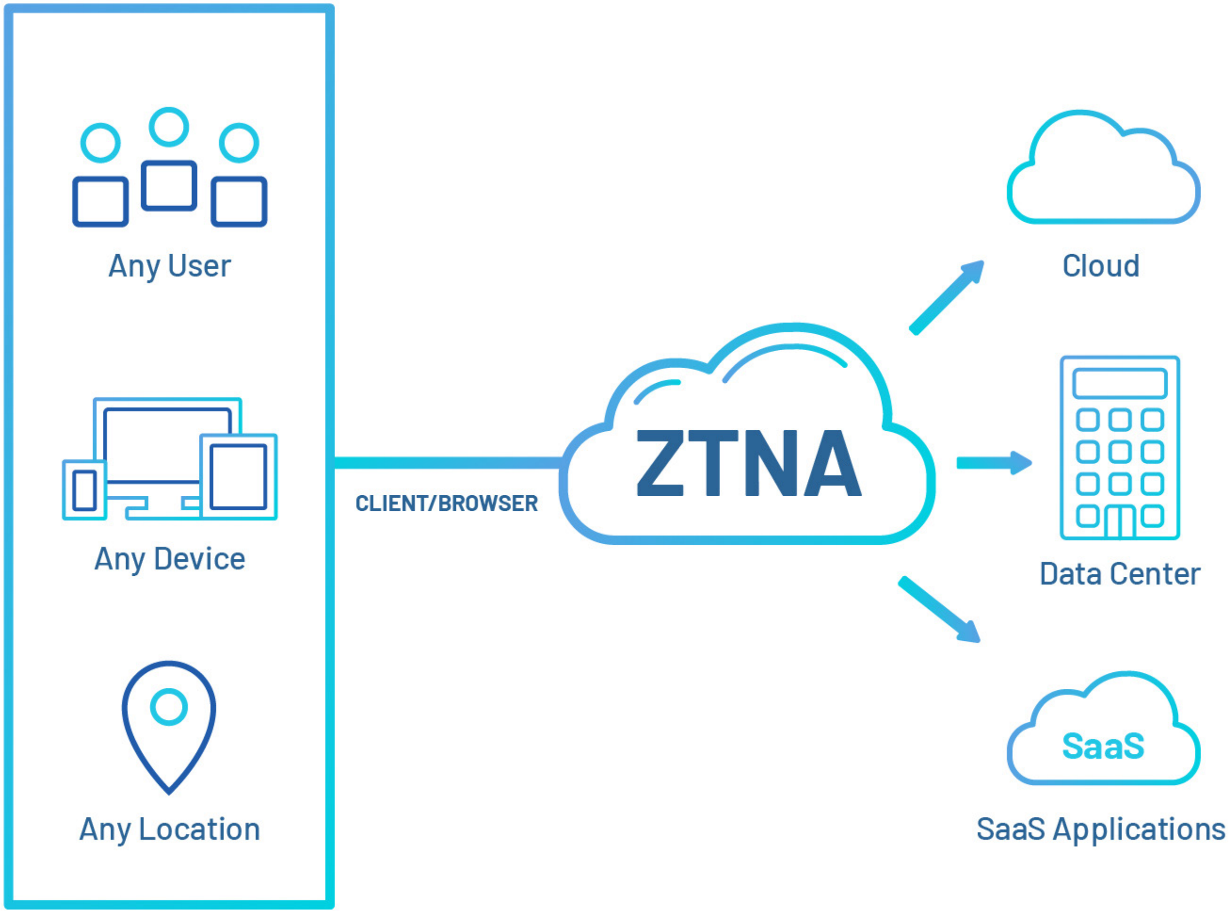
Emerging Networking Concepts Impacting NAC



Cloud Adoption

The adoption of cloud security products is growing faster than ever. Innovations in this arena have enabled organizations to improve business agility and reduce costs; but they've also increased the attack surface as demonstrated by a recent IDC report, which highlights that 98% of organizations suffered at least one cloud security breach in the previous 18-months. Most organizations now understand that with the increased attack surfaces that cloud creates, data security applied directly to sensitive information in the cloud is the only way truly to keep it safe.

This does not mean that traditional border/ perimeter security isn't still viable — we simply cannot assume that plain text data should ever exist within a cloud environment. Keeping that data protected with



data-centric security, such as tokenization and format-preserving encryption, is the fail-safe, or mitigating, mechanism in cloud security. Even if cloud resources are misconfigured or somehow the perimeters are breached, threat actors cannot leverage data they cannot read or understand.

Secure Access Service Edge (SASE)

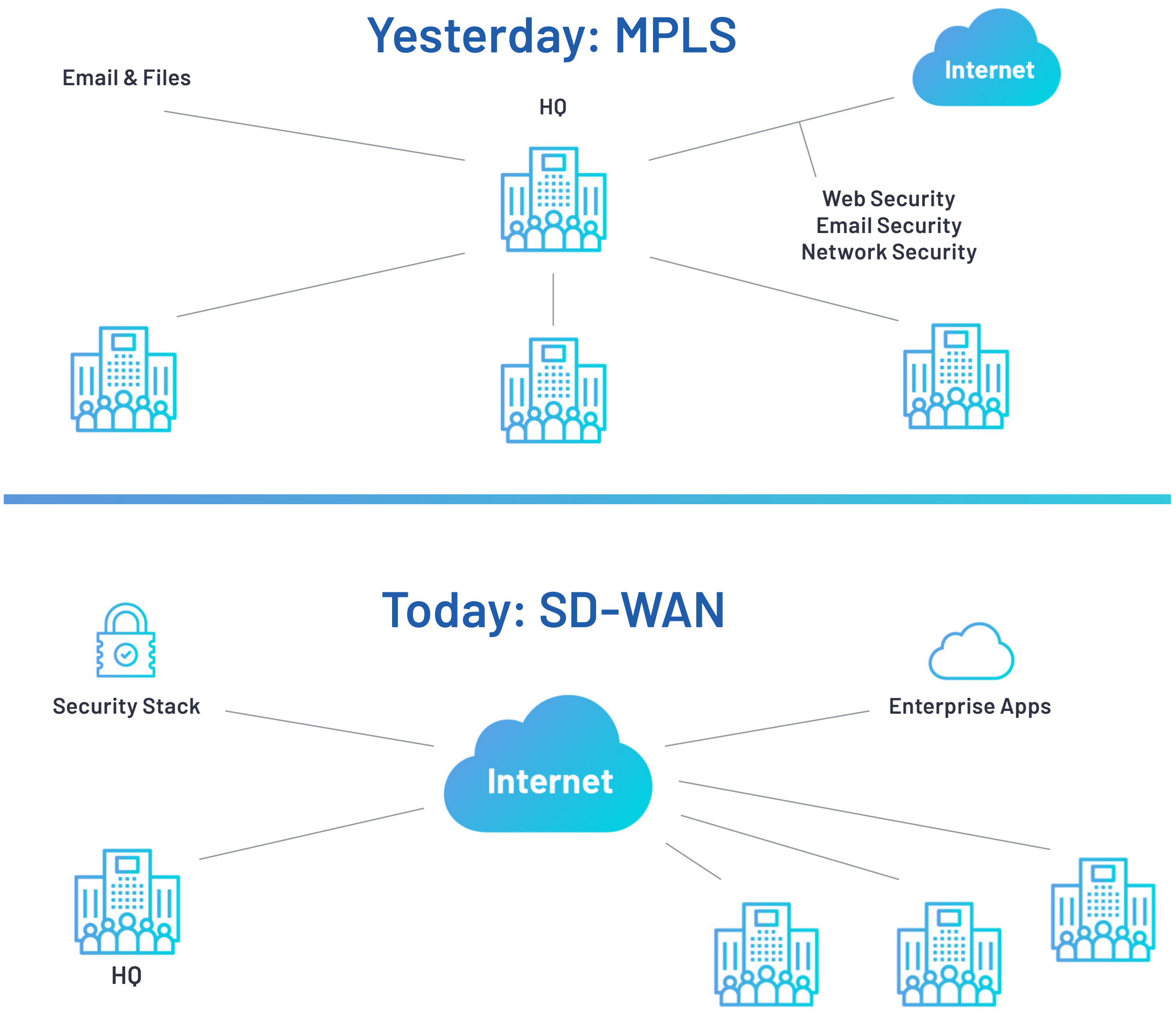
SASE, pronounced "sassy", stands for Secure Access Service Edge. It is a cloud-based network security model and category, proposed by Gartner in 2019, to support agile secure access to enterprise assets. This model includes the network security solutions in a global and cloud-native service that allows IT teams to easily connect and secure all of their organization's networks and users in an agile, cost-effective, and scalable way. This is especially useful in the currently globally dispersed digital enterprise.

According to Gartner's analysis, SASE can be characterized as an identity-driven, cloud-native, globally distributed technology that supports and impacts all enterprise edges and IT domains. For example, this would include a branch office in LA along with the main HQ in London, while traveling/mobile team members can connect on the go.

SASE addresses the numerous problems with traditional network security methods, many of which are rooted in the idea that network security architectures should be placed at the center of connectivity in the HQ or data center, where typically branch locations are more vulnerable to attack.

Zero-Trust Network Access (ZTNA)

ZTNA is an IT security solution that provides secure remote access to an organization's applications, data, and services based on clearly defined access control policies. ZTNA differs from virtual private networks (VPNs) in that they grant access only to specific services or applications, where VPNs grant access to an entire network. As an increasing number of users access resources from home or elsewhere, ZTNA solutions can help eliminate gaps in other secure remote access technologies and methods.



Use cases for ZTNA include:

- Authentication and Access — The primary use for ZTNA is to provide a highly granular access mechanism based on a user's identity. Where IP-based VPN access offers broad access to a network once authorized, ZTNA offers limited, granular access to specific applications and resources. ZTNA can provide more levels of security with location- or device-specific access control policies, which can keep unwanted or compromised devices from accessing the organization's resources.This access can be contrasted with some VPNs that offer employee-owned devices the same access privileges that on-premises admins are granted.
- Holistic control and visibility — Since ZTNA does not inspect user traffic after authentication, there could be an issue if a malicious employee uses their access for nefarious purposes, or if a user's credentials are lost or stolen. By incorporating ZTNA into a SASE solution, an organization can benefit from the security, scalability, and network capabilities needed for secure remote access, as well as post-connection monitoring to prevent data loss, malicious action, or compromised user credentials.

Extended Detection & Response (XDR)

XDR enables an enterprise to go beyond typical detective controls by providing a holistic and yet simpler view of threats across the entire technology landscape. XDR delivers real-time information needed to deliver threats to business operations for better, faster outcomes.

Extended Detection and Response (XDR) primary advantages are:

- Improved protection, detection, and response capabilities
- Improved productivity of operational security personnel
- Lower total cost of ownership for effective detection and response of security threats

Extended Detection and Response (XDR) holds the promise of consolidating multiple products into a cohesive, unified security incident detection and response platform. XDR is a logical evolution of endpoint detection and response (EDR) solutions into a primary incident response tool.

Software-Defined WAN (SD-WAN)

The adoption of Software-as-a-Service (SaaS) and cloud services has decentralized data traffic flows, making Multiprotocol Label Switching (MPLS) inefficient for wide area network (WAN) transport. This has given rise to SD-WAN for the implementation of software-defined branch (SD-branch), now allowing IT environments to be extended to branches outside of the headquarters that need high-quality network connectivity.

Traditionally, in order for most cyber security products to effectively operate, they needed a direct connection to headquarters and appliances deployed on-site at individual branches. This is a costly, time-consuming endeavor, and has historically limited the use of SD-WAN and SD-branch. Fortunately, SaaS is eliminating the need for on-site appliances and on-going maintenance. Now, all one needs is an internet connection to implement.

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.