

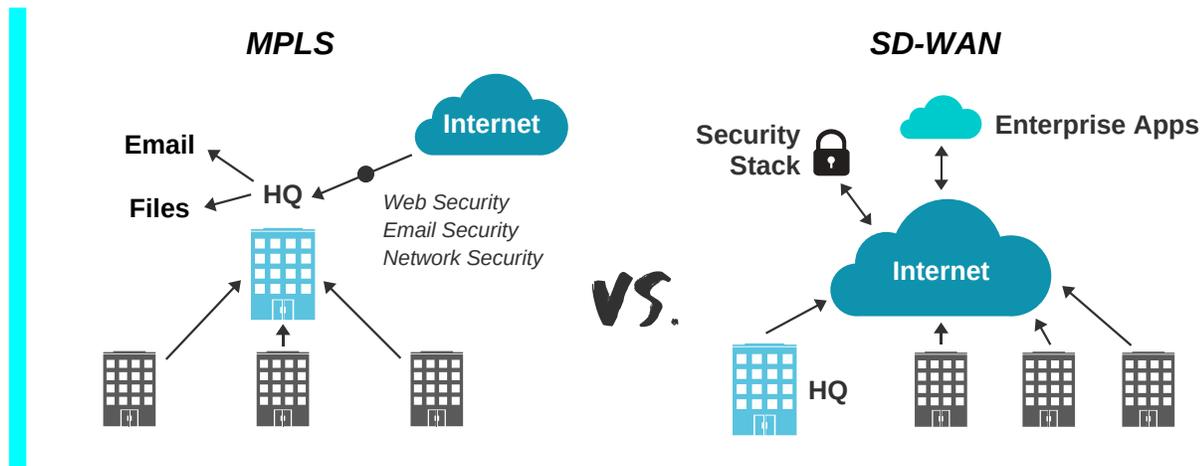


WHITE PAPER

How Organizations Can Control Corporate Network Access in an SD-WAN World

Why SD-WAN, Why Now?

The rise of Software-as-a-Service (SaaS) and cloud services is resulting in decentralized data traffic flows, in turn rendering the traditionally expensive Multiprotocol Label Switching (MPLS) inefficient for wide area network (WAN) transport.



The emergence of software-defined WAN (SD-WAN) in response to rising cloud adoption is significant because it promises to deliver reduced cost and enhanced performance and availability. This is a trend that is unlikely to go away. In fact, it's set to intensify. According to Gartner, SaaS and Infrastructure-as-a-Service (IaaS) will grow at 17% and 27%, respectively, through 2022. Both are key drivers of SD-WAN adoption in that time.¹

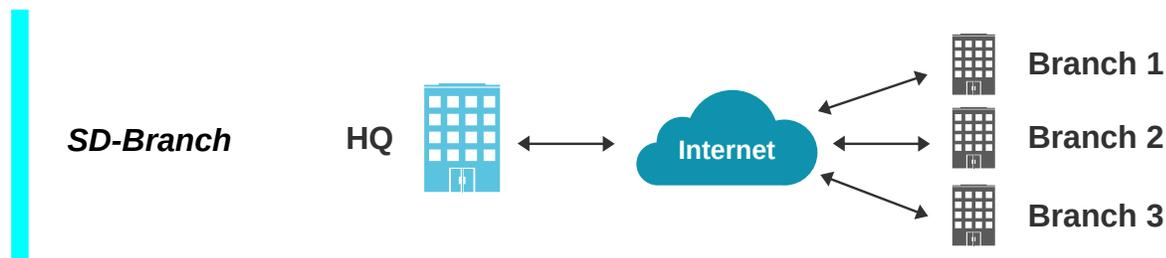
The Impact of SD-WAN on Network Security

Today, organizations can leverage SD-WAN technology to implement software-defined branch (SD-branch) as a way of extending IT environments to any of its branches outside of its headquarters that require high-quality network connectivity.

1. SD-WAN is Killing MPLS, So Prepare to Replace it Now, Gartner (2018)

For retailers, hospitality groups (hotels, restaurants, etc.), commercial banks and other large distributed organizations, SD-branch is particularly useful as it utilizes SD-WAN technology to simplify a branch's IT architecture – reducing the resources and budget needed to maintain operations.

Branches are typically more at risk of network threats than organizational headquarters due to the fact that they're inherently understaffed or underserved from an IT standpoint.



To combat this, the SD-branch approach is to have security functions present in the IT devices at the branch so that data transmitted from the branch to another node in the WAN is as secure as other parts of the network from square one, instead of waiting until the data reaches security tools outside the branch. It's like locking a house's front door instead of just the bedroom doors.²

Network Access in an SD-WAN World

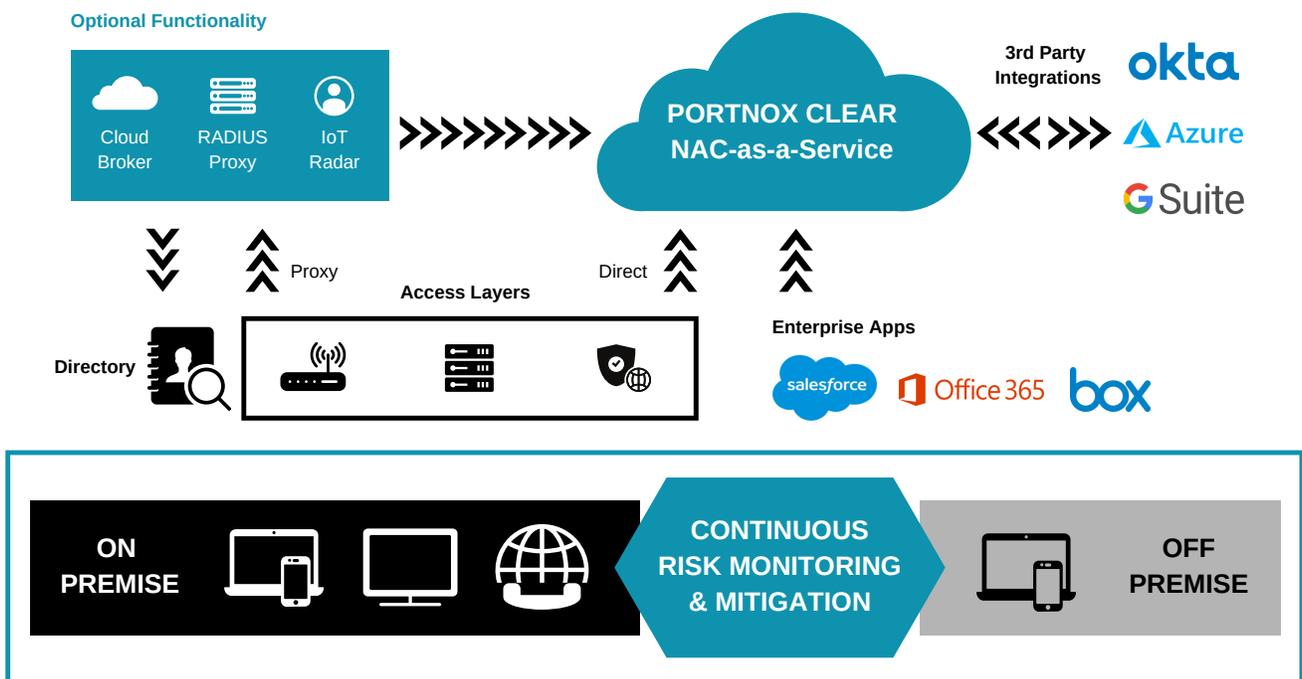
The rise of BYOD, mobile workforces and IoT has driven an exponential increase in the number and types of devices that can connect to today's corporate networks. Securing and protecting these devices - particularly agentless IoT devices - is a core principal and best practice in cyber security.

Today, device segmentation (especially for IoT) has evolved to become the only effective option for network defense, as it enable organizations to protect themselves against lateral movements and to detect network breaches faster.

2. What is SD-Branch?, SDXCentral (2019)

Executing this requires a network access control solution be deployed – one that can not only control the port security, but also segment the network by the type of device or its user. Traditionally, network access control has necessitated a connection to the organizational headquarters, with an appliance deployed at each branch. This has historically limited the use of SD-WAN / SD-branch technologies. Side-stepping these limitations has required innovation in network access control.

The logical next step in the evolution of network security is for organizations to be able to leverage a NAC solution that’s delivered as a cloud service. This eliminates the need for cost on-site appliances and on-going maintenance. Now, all that’s needed to control network access at branches and the headquarters alike, is an internet connection. With Portnox CLEAR, organizations gain unprecedented network visibility and continuous risk monitoring of endpoints across all access layers - no matter device type or branch location. All from the cloud with no on-premise components.





ABOUT PORTNOX

Portnox provides simple to deploy, operate and maintain network security, visibility and access control solutions. Portnox software can be deployed on-premises, as a SaaS/cloud-delivered service, or in hybrid mode. It is agentless and is vendor agnostic, allowing organizations to maximize their existing network and cybersecurity investments. Hundreds of enterprises around the world rely on Portnox for network visibility, cybersecurity policy enforcement and regulatory compliance. The company has been recognized for its innovations by Info Security Products Guide, Cyber Security Excellence Awards, IoT Innovator Awards, Computing Security Awards, Best of Interop ITX, Cyber Defense Magazine and more. Portnox has offices in the U.S., Europe and Asia.