portnox™

Zero-Trust Cloud NAC Enables Secure Remote Access

Mar 10,2020

The Rise of Remote Work & Remote Network Threats

Gone are the days of teams working shoulder to shoulder at desks or cubicles day in and day out. Don't misunderstand – on-site work obviously still happens, but remote work is increasingly becoming the norm. Today, 50% of employees globally are working outside of their main office headquarters for half of the work week.

This growing trend doesn't take into account unforeseen forces either. The outbreak of COVID-19, or the coronavirus, for example, is putting pressure on companies to allow (or even demand) their employees work from home. Microsoft, which employs tens of thousands of people in the Seattle, Washington area has requested that all employees who can do their jobs from home should do so for the month of March due to the virus.

Organizations undergoing such a dramatic, overnight shift to a majority remote workforce are – as you would imagine – finding their networks increasingly vulnerable to external threats as company devices remain "off network" for extended periods of time. It's a network administrator's worst nightmare.

Coronavirus aside, organizations with significant remote worker populations, and those with existing bring your own device (BYOD) policies are increasingly at risk of a network breach. It's a shared sentiment among IT professionals – in fact, 90% agree — that remote workers are not secure.

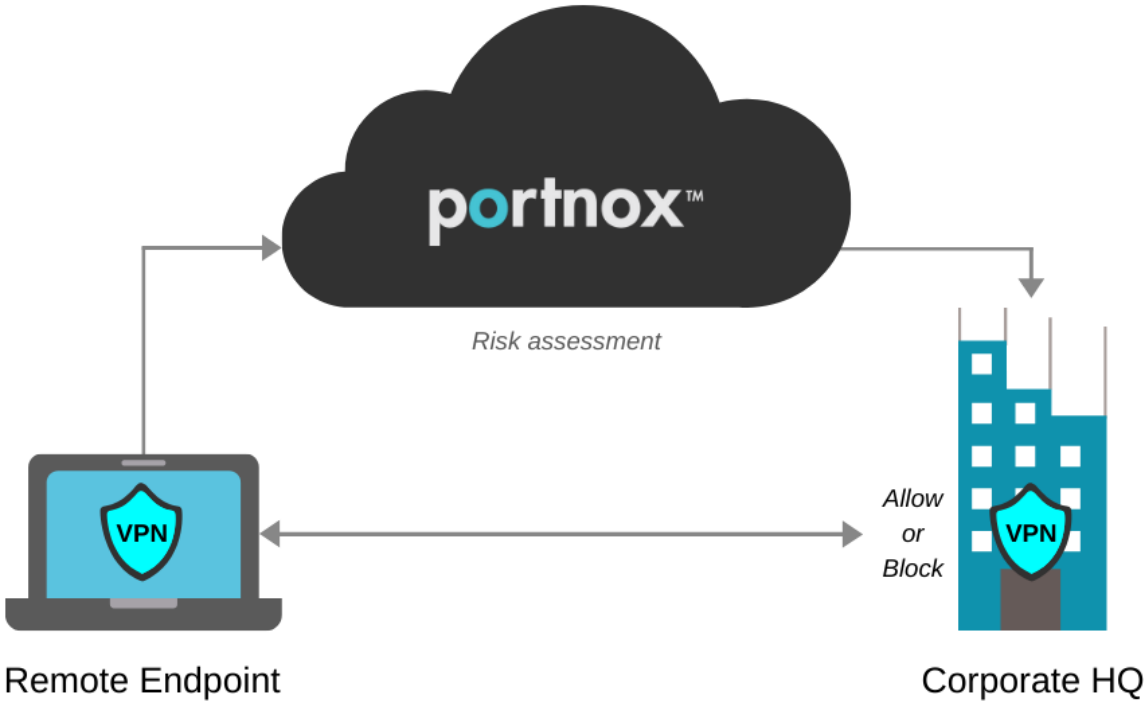
VPN is Just the Start

Historically, companies have relied on VPNs to provision remote employees with a secure encrypted connection for remote access to the corporate network. The VPN, however, does not STOP an endpoint from accessing the network. It's only a means of delivering remote access connectivity for employees off-campus.

While a VPN will ensure all traffic is encrypted and even lets you bake in two-factor authentication (2FA) to better manage who is connecting, it tells you nothing about the risk posture of their devices. When you rely solely on a VPN, you have no way of knowing if a device is compliant. Even more importantly, if a device is not compliant (which you wouldn't know), you would have no way of preventing it from connecting through VPN.

In fact, some of the world's biggest vendors do not support a remote check of the endpoint during VPN connection. This includes Meraki, Sophos, Watchguard, Checkpoint and others. This means if, for example, your endpoint runs MAC OSX, you may not be able to run endpoint posture assessment from your VPN provider.

Thus, what's needed to remedy these blind spots is a zero-trust NAC solution layered on top of your VPN.



Zero-Trust NAC in the Cloud

A cloud-delivered zero-trust NAC, like Portnox CLEAR, extends awareness, endpoint risk profiling and access controls across all company access layers, including the VPN. Portnox CLEAR offers policy-based dynamic access controls that automatically place trusted VPN connecting devices into the proper VLAN, ensuring only trusted and compliant devices are able to connect through it.

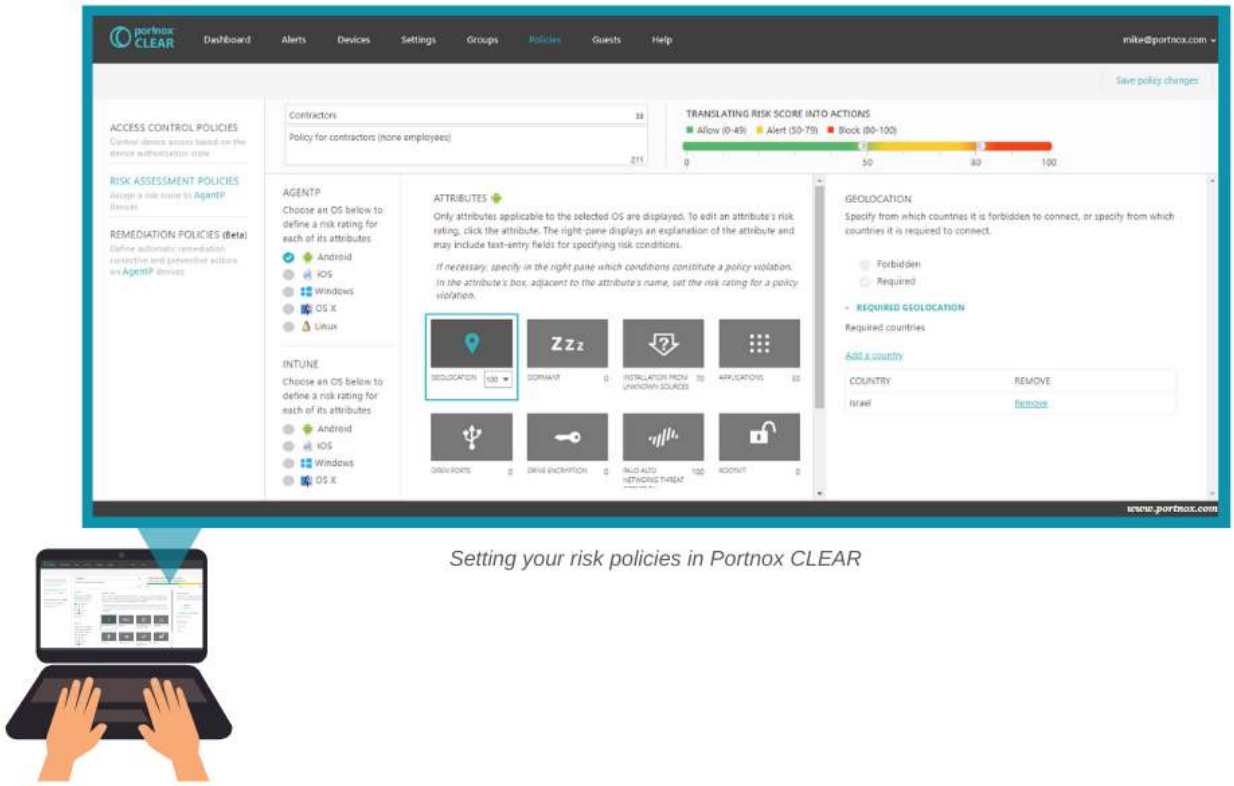
At the end of the day, it's really the cloud-delivered component of this that's key. Today's typical company network is expansive, and that means so too is its threat surface. There are whole variety of attack tactics out there – spear phishing, advanced persistent threats, identify theft, etc. The VPN,

even paired with most legacy NAC solutions, simply can't cover all of the remote access blind spots out there that are vulnerable to such attacks.

When working with a cloud-delivered zero-trust NAC, however, you eliminate the need for extensive endpoint scanning – it already knows the status of an endpoint, no matter its location. And while this doesn't reduce the size of an attack surface, it does ensure that the necessary measures are in place to protect both endpoints and your network.

Adding 2FA on Top

Through two-factor authentication (2FA) for VPN, Portnox CLEAR even goes a step further. While traditional 2FA solutions don't take devices into account, Portnox CLEAR offers device authentication through the use of its agent, *AgentP.*



Setting your risk policies in Portnox CLEAR

With *AgentP*, Portnox can deliver unique 2FA for VPN that looks at a user's credentials AND an enrolled device, ensuring that security is offered on two levels: authentication of the user themselves, and authentication of the device. So, if user credentials are compromised, they're effectively useless if the device being used is not enrolled.

For more info or a trial contact Full Control Networks:
t: 01677 428700 e: info@fullcontrolnetworks.co.uk