portnox™ | SOLUTION BRIEF

Zero-Trust Remote Access Control

Zero-trust remote access control as a cloud service.

PROTECTING TODAY'S EXPANDING NETWORKS

Today, your network is expanding by the minute. Employees are using their devices - personal or work-issued - from home, hotels, airports, restaurants, or any place with an internet connection. This poses a unique security challenge, particularly as the critical resources your remote workforce needs access to consist of both cloud-based platforms AND internally-hosted business systems. The million dollar question keeping network security professionals awake at night is: how do we extend the same level of awareness and access control as is done on the LAN to this growing number of remote devices that might not connect directly to the LAN for weeks or months?

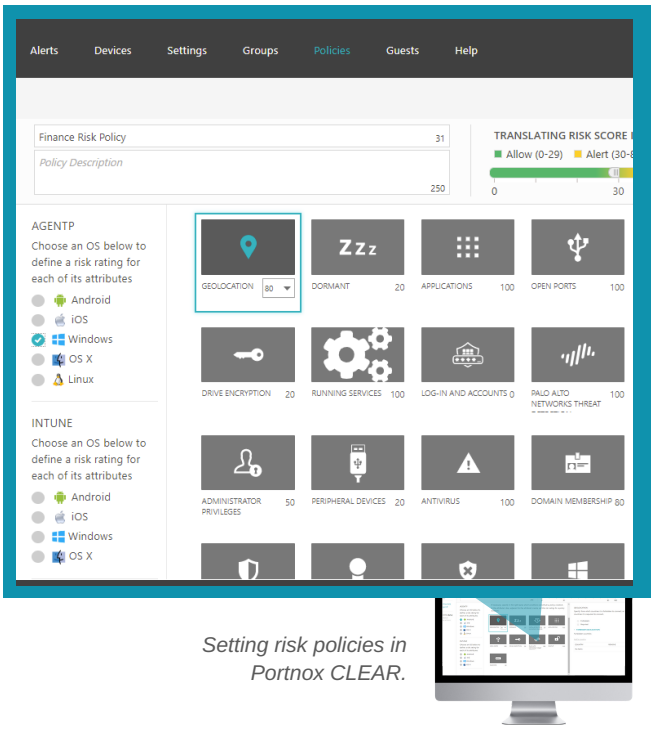
The Answer: Portnox CLEAR

Portnox CLEAR has been purpose-built to easily enhance your remote access security for VPN, VDI and enterprise cloud applications with full endpoint risk awareness and zero trust access controls. Put simply, CLEAR delivers zero-trust remote access control as a cloud service.

ENDPOINT RISK AWARENESS & ACCESS CONTROL

As a cloud-based solution, Portnox CLEAR is always aware of the current risk of remote devices, regardless of if they're "on" or "off" the network - giving you full, continuous visibility and risk awareness. Awareness is only a piece of the puzzle, however. Actionable awareness is where Portnox CLEAR separates itself. By leveraging the current risk posture of a device - which can be configured in line with your compliance policies, like having antivirus up-to-date or the latest patches in place - Portnox CLEAR can automatically allow or block remote access through your VPN, VDI or cloud applications via Okta.

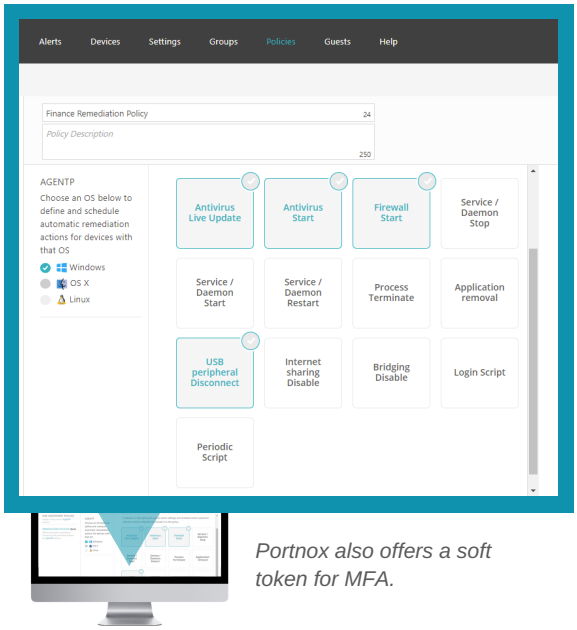
Portnox CLEAR also extends this awareness to geo-location. So, for instance, if you want to allow users from the U.S, but block access attempts from North Korea, you can do so. For VPN connecting devices, Portnox CLEAR can even dynamically direct trusted devices to their proper VLANs based on policy.



Setting risk policies in Portnox CLEAR.

ENSURING REMOTE DEVICE COMPLIANCE

Continuous, anywhere awareness of device risk paired with the ability to dynamically control access based on policy is a critical part of the zero-trust remote network access control model. Portnox CLEAR goes one step further with automated corrective and preventative actions (CAPA). With CAPA, Portnox CLEAR is able to take real-time actions on remote endpoints to ensure they remain compliant with your risk policy.



Portnox also offers a soft token for MFA.

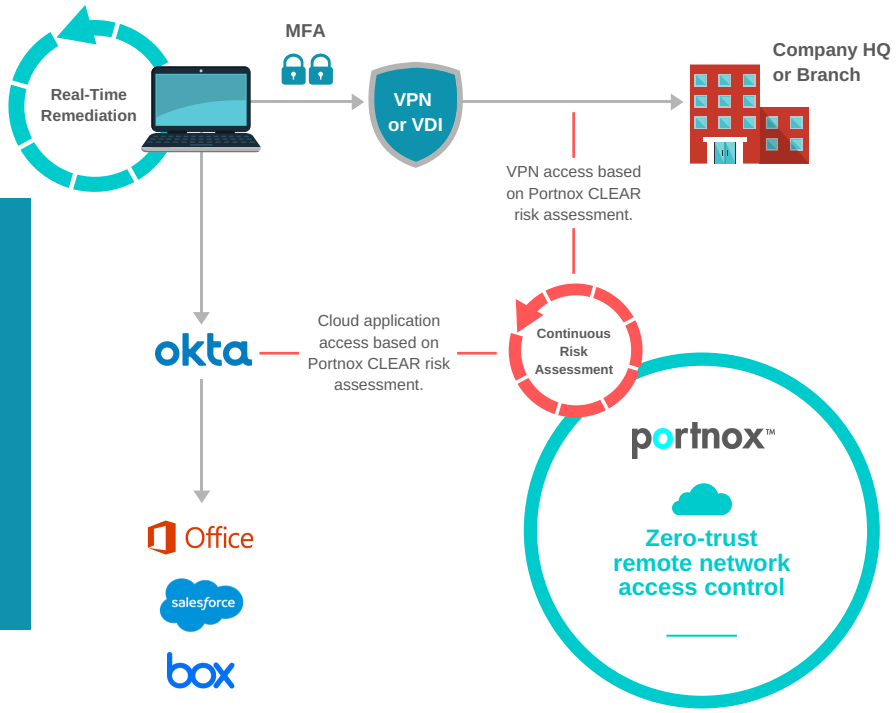
This includes ensuring the firewall is always on, AV is running and updated, or even restricting the use of a USB drive for someone on the team working remotely. These are merely some examples of the proactive remediation actions that Portnox CLEAR can take to maintain that devices used by off-site employees remained trusted and healthy at all times.

MULTI-FACTOR AUTHENTICATION (MFA)

While traditional MFA solutions don't take devices into account, Portnox CLEAR offers device authentication through the use of its agent, *AgentP*. With *AgentP*, Portnox CLEAR delivers unique MFA for VPN access 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 in not enrolled.

ZERO-TRUST ACCESS CONTROL TO ENTERPRISE CLOUD APPS

Beyond VPN access to on-premise applications and resources, your remote employees may also need access to cloud-hosted enterprise applications such as Office365, Salesforce, Box, etc. Through integrations like Okta, the market leader in single sign-on to enterprise cloud applications, Portnox CLEAR can extend the same endpoint risk-driven zero-trust access controls to your cloud applications. All it requires is for you to configure your Okta deployment to validate with Portnox CLEAR via Okta's secondary authentication option. Once configured, Portnox CLEAR will then be able to allow or deny the access requests based on the real-time risk scores of each device.



HOW IT ALL WORKS

Portnox CLEAR works with your existing remote access infrastructure. Simply create your Portnox Clear instance and define your remote access group policy within the platform (i.e. remote users/devices, risk/compliance policy, remediation policy and access control policy). Configure your VPN, VDI or Okta to connect to your Portnox CLEAR instance...and voila, you're done!

REQUEST A DEMO >