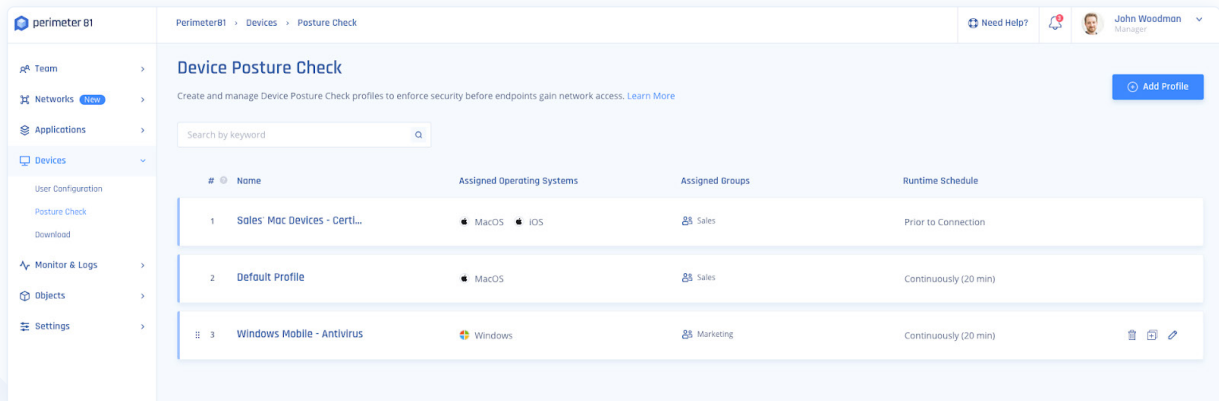perimeter 81

Device Posture Check

Endpoint vigilance for the Bring Your Own Device and remote work era

Modern organizations allow employees to access the corporate network from far beyond the traditional network perimeter, and frequently encourage employees to use their own devices.


While these steps increase operational agility, they can also significantly expand security risks. Any number of these devices regularly access sensitive data and resources, becoming targets for hacking and a key locus of vulnerability for the organization.

Perimeter 81 Device Posture Check (DPC) enhances your network security and ensures that employees can only connect with secure devices. It allows administrators to guarantee that only devices that comply with your security policies can connect to the network and gives IT the device inventory and reporting tools they need to ensure that the network stays secure.

Benefits & Features

- Enhance network security by establishing trust only in devices that comply with security policies

- Prevent malicious access and attacks by automatically denying access to insecure or compromised devices on login or at predetermined intervals

- Provide continued monitoring and support for company-wide compliance with DPC reporting capabilities

- Benefit from an up-to-date inventory dashboard of devices with network access, including access history and device details

Follow Us

perimeter 81

Endpoint Access Control with Device Posture Check:
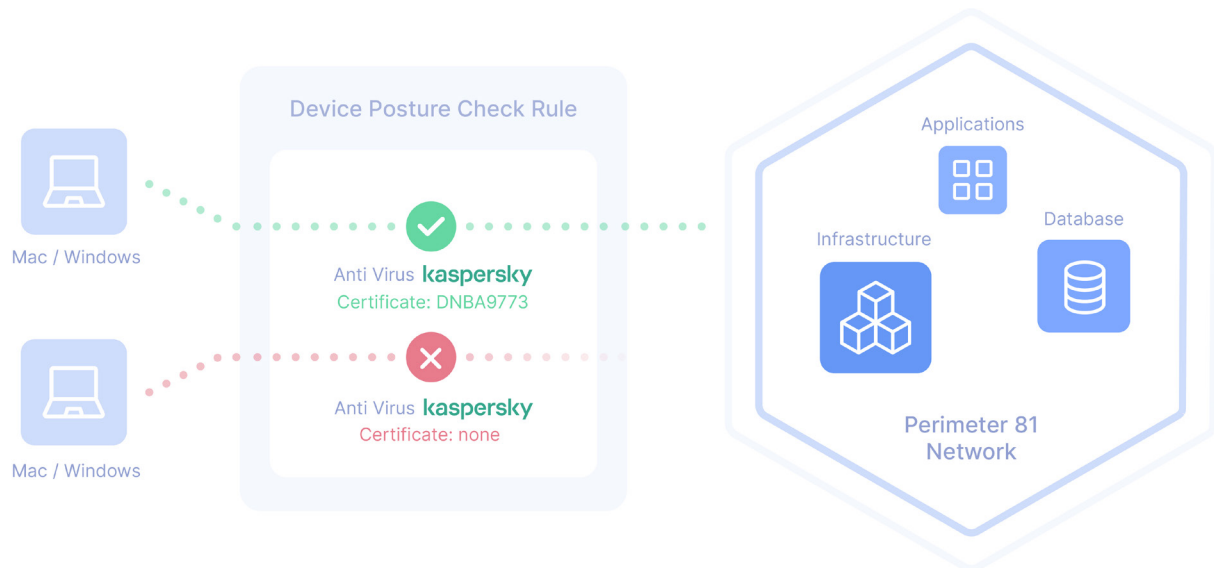
A gatekeeper for your devices

Define device trust with posture check profiles

Device security requirements can vary by role, device, OS and other factors to account for security gaps. Device Posture Check profiles are therefore user- and group-specific, making it easy to create relevant device posture rules for access. Specific rules can apply to any subset of your users, such as contractors, branch offices or departments.

Follow Us
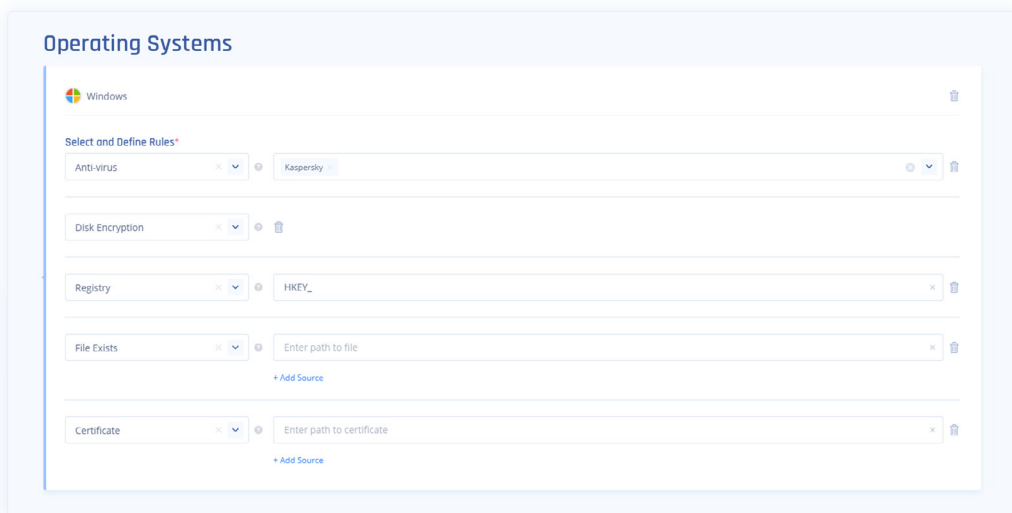
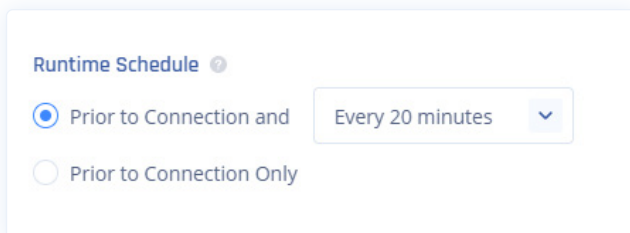## Optimized compliance parameters for every device posture

Device Posture Check rules include parameters that ensure access is only occurring from secured and recognized Windows, Mac and Linux devices, while iOS and Android mobile devices can be included or excluded from access based on the device posture rule.

- Antivirus: Check if the device has your organization's preferred antivirus software installed.
- Certification: Check whether a specific certification exists on the device.
- File Exists: Check if a file required for the proper security posture exists on the device.
- Disk Encryption: Check if the disk is encrypted.
- Windows Registry: Check whether a specific registry path or value exists in the device's Windows Registry.
- Process Running: Check if a specific process (or antivirus program not in the antivirus dropdown) is running on the device.

## Enforce device posture pre- and post-connection

Attackers can exploit a device before it accesses the network or even while it is already connected to critical resources. Accordingly, Perimeter 81 DPC makes it easy to check the security posture of your devices before connection and continuously on a custom schedule, for around-the-clock device security.

Follow Us

Get detailed device monitoring and reporting

Data on your connected devices and their activity is crucial for effective security policy. Device posture check reports can be examined in-depth in the Device Posture Check monitoring panel, where you'll find your device inventory, history of device and user logins, successful or failed posture checks, session information and other reports useful for optimizing the health of your network.

Reports can be filtered by time period and relevant aspects of the device. Drill-down views display the in-depth details of particular devices including user information and access history.
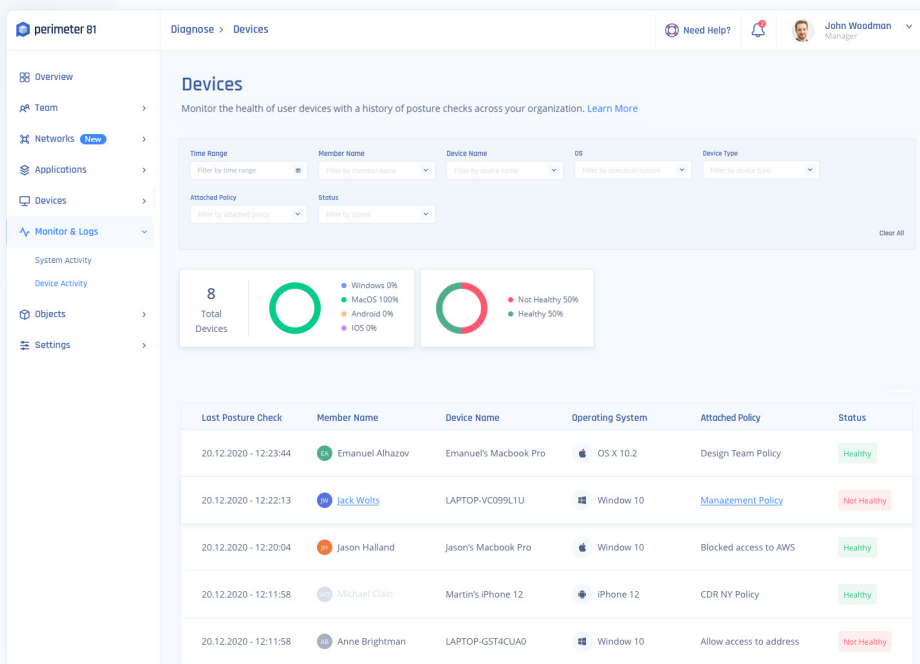
Contact Us

Perimeter LTD.

www.perimeter81.com

1-929-575-9307

Request a Demo

Follow Us