Network access control

https://www.techtarget.com/searchnetworking/definition/network-access-control

Network Access Control (NAC) is a method to bolster security, visibility and access control of a proprietary network. Networks can restrict the availability of network resources by enforcing security policies. Endpoint security protection such as antiviruses, firewalls, and vulnerability assessments can be provided along with security enforcement policies and systems authentication methods.Network Access Control (NAC) is a technology used by enterprises to ensure that only authorized users can connect to corporate networks. NAC helps prevent attacks, viruses and worms from entering the network.There are two types of NAPs, including the following: pre-admission: evaluates user access attempts and only allows access to authorized devices and users post-admission: Network Access Control (NAC) is an important part of securing your network. It helps you identify unauthorized users and devices attempting to connect to your network. You can use it to deny access to these individuals or limit them to specific areas. users trying to access a different part of the system. Also restricts lateral movement to limit damage from cyber attacks.

NAC tools are proactive and prevent unauthorized access to your network. They protect your network perimeter including the physical infrastructures, devices, software, apps and cloud-based assets from unauthorized access. You can bring your own device into the office but you need to be sure that the device you're bringing into the office is safe for work. NAC tools allow you to control what employees do when they connect to the internet.IoT devices are commonly used by businesses and governments. However, these devices are often overlooked when it comes to securing them. Security measures need to be put into place to protect these devices. IoT devices are usually left unattended and vulnerable to attacks. In addition, there are many different types of IoT devices. These devices should be separated into groups based on what type of device they are. This helps identify the vulnerabilities within each group. Once identified, the vulnerabilities can be fixed or remediated.