NACVIEW

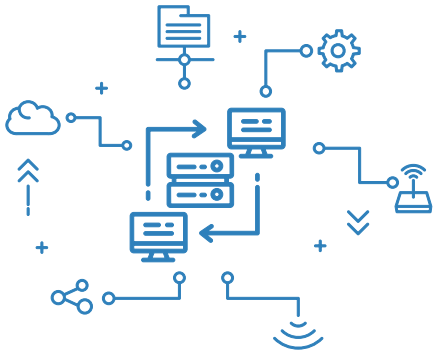
www.nacview.com

NACVIEW a must-have for the modern manager

DO YOU KNOW WHAT AND HOW MANY DEVICES ARE IN YOUR NETWORK?

Work phones, devices of company visitors, devices of remote workers, IoT devices, computers not in the compliance with the present regulations, and having an outdated operating system or anti-virus system disabled. All these unprotected devices, connected to the corporate network, may pose a threat. Just one infected device is enough for the problem to be spread out to the entire computer network. This will make all your data unprotected. Further it could be easily accessed by unwanted users, confidential information could be stolen or corporate data encrypted, and even finances and reputation may be inevitably and sadly lost.

The NACVIEW NAC system provides protection against unauthorized access to unknown networks or potentially dangerous devices. The system enables full visibility of all objects connected to the network and manages granting access to the specified subnets. This makes the entire corporate network more secure, better coordinated and, obviously, more efficient.



In times of omnipresent access to the Internet for all kinds of devices, individual organizations cannot afford lack of control over what and when connects to the central company network. During the most famous attacks - such as WannaCry or NotPeyta - corporations with central network access management could have drastically reduced the risk by isolating outdated devices from the rest of the network. **NACVIEW will make your corporate network better protected and free from any unidentified devices.**

WHY IS IT WORTH IT:

IMPROVED CYBERSECURITY.

Corporate assets are vulnerable to malware, ransomware and DDoS attacks. Hackers are constantly looking for access to sensitive data that they can sell on the Dark Web. **NACVIEW solutions can mitigate these risks by excluding outdated or suspicious devices and restricting what users can do on the network.**

VPN SECURED ACCESS.

Working from home has become a common trend. It results in all IT departments obliged to allow their employees to access enterprise network resources from the outside using VPN. The problem with this solution is the inability to fully verify them. Are we sure it is our employee connected to the network, or is it a person who took over the device or stole the VPN password? That is why it is our priority to secure remote access with a second authentication factor. **NACVIEW can be integrated with almost any VPN system and enables two-factor VPN authentication using a dedicated phone application or SMS one-time passwords.**

THE BETTER USE OF OTHER EXISTING SECURITY SYSTEMS.

The Network Access Control type system is a central fuse, so logs from other systems, such as Antivirus, Firewall, etc. can be easily redirected to it. This solution allows an automatic removal of potentially dangerous devices from the internal network.

WHAT ELSE YOU GET:

INCREASED PRODUCTIVITY AND WORK ERGONOMICS.

Thanks to the precise NACVIEW policy, employees, regardless of where and how they connect to the network, will always get full access to subnets dedicated to them, including access to the necessary resources and network services. What is important, the implementation of the NAC system is associated with network segmentation and network traffic regulation. Due to this, we will increase the bandwidth of the link for each user.

CONTROL OVER BYOD EMPLOYEES' PERSONAL DEVICES.

Nowadays the differences between private and business devices are becoming more and more blurred. Moreover, some companies even allow employees to use personal devices for company purposes to increase the efficiency of their work and reduce overhead costs. BYOD does not have to mean sacrificing security. The implemented network access control can allow access only to updated and secured devices or redirect devices to a separate VLAN or guest network.

CONTROLLED GUEST ACCESS.

Secure and automated access to the guest network is a sign of a modern and reliable company. With the use of the automated Captive Portal guests can self-register their account to gain access to the network. The Captive Portal can have an individual appearance by displaying a logo, graphic background and publishing marketing and information content on it. Thanks to this you will present your brand, and inform about current offers or you can promote selected services and products. All this will make guests feel welcome and the company will know who is using its network.

COST REDUCTION.

The system allows you to quickly and efficiently browse data and search for problems in the network. As a result administrators can quickly diagnose problems and immediately implement countermeasures to improve its performance. In addition, automation mechanisms allow you to plan many aspects in advance so that the system can apply them on the administrators' behalf. These will include, among others, pre-planned system commands, automatic switching off and on of Wi-Fi networks on non-working days so that they do not consume energy or transferring information about ports that have not been used for a long time. They will allow the maximum use of the currently owned equipment.

COMPLIANCE WITH THE SECURITY RULES.

NAC is also a valuable tool to ensure compliance with relevant cybersecurity regulations. Network security policies can be integrated into GDPR or HIPAA compliance plans, providing evidence that networks meet required third-party standards.

THE LOWER RUNNING COSTS.

NACVIEW is a system independent of network equipment manufacturers. Therefore, when buying new switches or replacing old ones, the company will not be dependent on one manufacturer in terms of price. It is possible to check numerous vendors of network equipment, so that each time you can choose the most advantageous in terms of security, functionality and performance and, equally as well, the most economical option.