Hurdling in the automotive industry - NAC put to the test

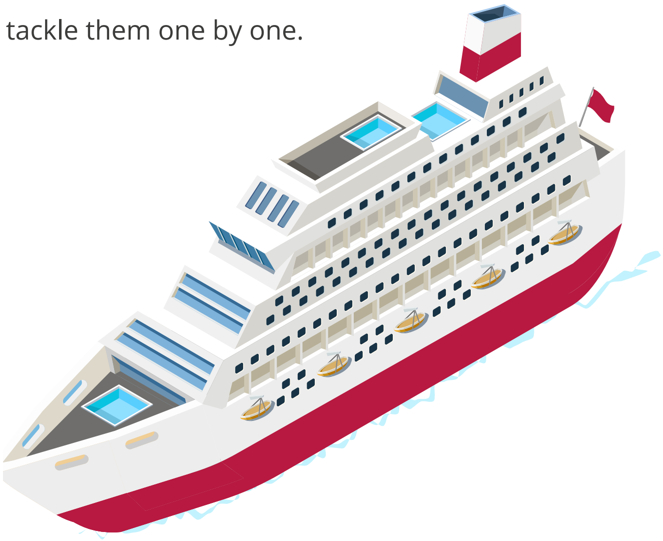
Imagine a technical firm in the automotive industry, building car components for prominent brands such as Volkswagen. Digital transformation is turning on the pressure, creating a shockwave through the entire production chain. As car brands try to protect their intellectual property and avoid reputational damage through data breaches, they increase pressure on their suppliers to make their computer networks watertight. The firm in question suddenly finds itself looking for solutions to problems they never knew needed solving, especially in the field of network security. Not an easy job, as they're dealing with employees, production machines, partners and guests that all need access. Could a NAC solution help them take all the hurdles? We'll tell you here.

The security wish list

Looking at the pressure coming from partners, the different sorts of access that were needed (employees, partners, guests, machines) and the complexity of today's security solutions, our firm had some work to do. Add to this that they had some wishes of their own too. For example, they wanted to secure their production machines without the need to install any software. Second, they wanted to use built-in VPN software rather than implementing new software, to make the implementation of the new security solution as simple as possible. Third, they needed a guest portal and a place where they could store details on guests and partners. Oh, and by the way: the solution had to be as low-maintenance as possible. All in all, our experts faced the challenge of implementing a low-impact high-security solution that would tick all of these boxes:

1. The ability to allow access to cleared devices to specific network segments
2. The ability to manage the way that users are allowed to enter the network (so using cable, Wi-Fi and/or VPN)
3. An integration with the existing user directory
4. Usage of the built-in client software that can be found on all Microsoft Windows and macOS computers
5. Integration of legacy production machines that don't have the required software components, without having to change their configuration
6. Easy but secured access for partners
7. A guest portal

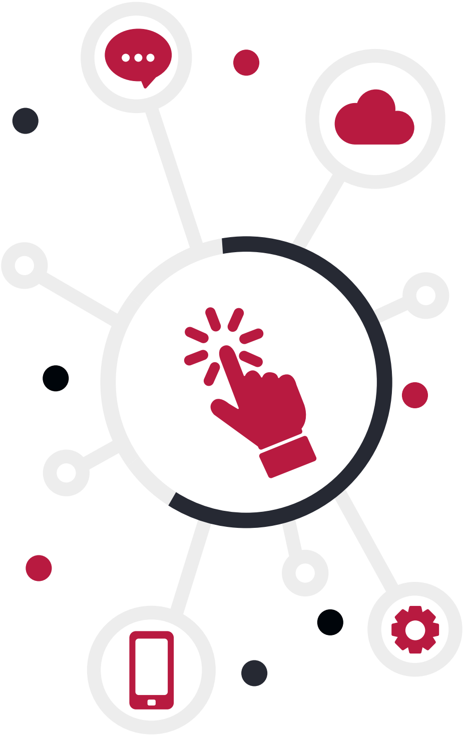
That's a lot of requirements, we reckon. Our experts decided to tackle them one by one. There we go:



HURDLE 1: Compartmenting

The first thing our experts did was create several different network compartments. This way, it became easier to control access for devices and users, which was already a major step forward. To achieve this goal, our experts implemented a Network Access Control solution (NetAttest EPS), which included a Certificate Authority (CA) to automate the creation of digital certificates and also a RADIUS server for the authentication of users and devices. Then, our experts integrated the NAC solution with the company's Active Directory, which contained information on employees and their access rights. This way, all the changes made in the directory would be immediately shared with the NAC solution, meaning access rights would always be up to date. Second, it saved the administrator a lot of trouble, as he'd only deal with the directory, which, in turn, would deal with the NAC solution.

> Our experts had to look for a way to integrate the VPN-solution, which was discouraged by the VPN vendor

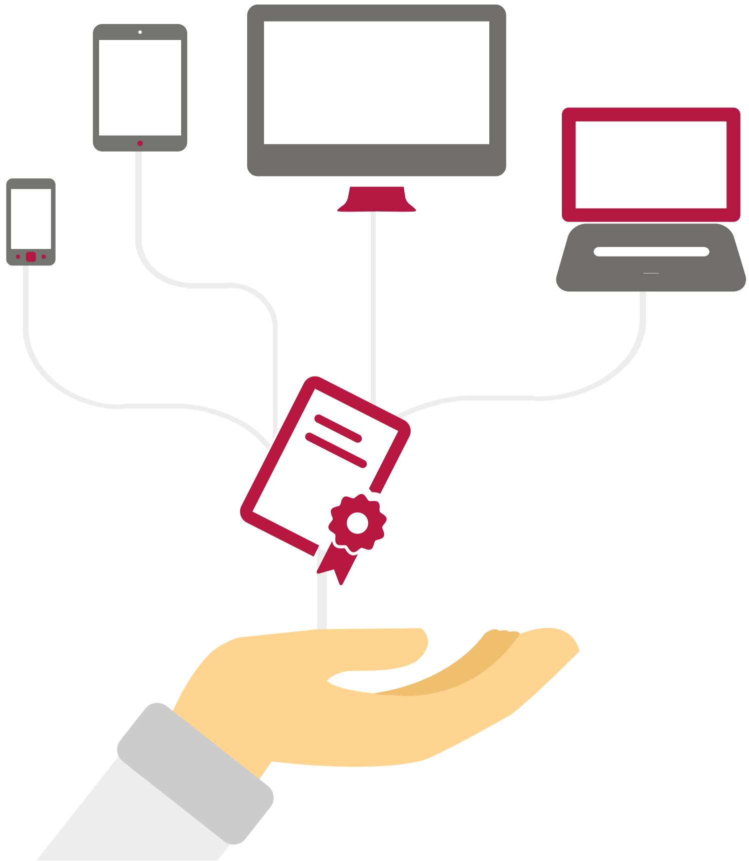


HURDLE 2: Safely connecting the VPN

Using Active Directory, the firm also wanted to be able to control the way users were allowed to enter the network, either using a cable, the Wi-Fi or a VPN. Moreover, this had to be possible by using only one single certificate. By using the integration that was created in the first step, this could all be managed in the Active Directory, so no problem there. The biggest challenge lied in the VPN, because the vendor of the VPN-solution discouraged the use of an external authentication solution and promoted their own. However, our experts found out that it was not that difficult to integrate the VPN solution with the NAC solution, which complied with the customer's wish to integrate both systems. So far for hurdle two.

HURDLE 3: Creating a Point of Contact for non-Windows devices

So far so good. Or more precisely: so far so good for Windows devices. Microsoft computers come with a built-in method that automatically distributes and installs certificates (Group Policy). MAC computers, however, don't have such a built-in method, nor do mobile phones and tablets. This means that you need to find an alternative way to install client certificates on these devices, which is time-costly and prone to error. If, for example, an employee installed his own certificate, but did it wrong, he'd risk being denied access. Or worse: being robbed of his certificate. Even the thought of this happening compromises the trustworthiness of a security solution. Alternatively, the administrators could put all non-Windows devices under some sort of device management, but as the company didn't want to install any additional software either, this wasn't an option. Our experts did come up with a solution, though. By using an easy-to-use application that runs on all devices, they enabled employees to install their certificate themselves, without the risks of this going wrong. And that was the end of hurdle 3.



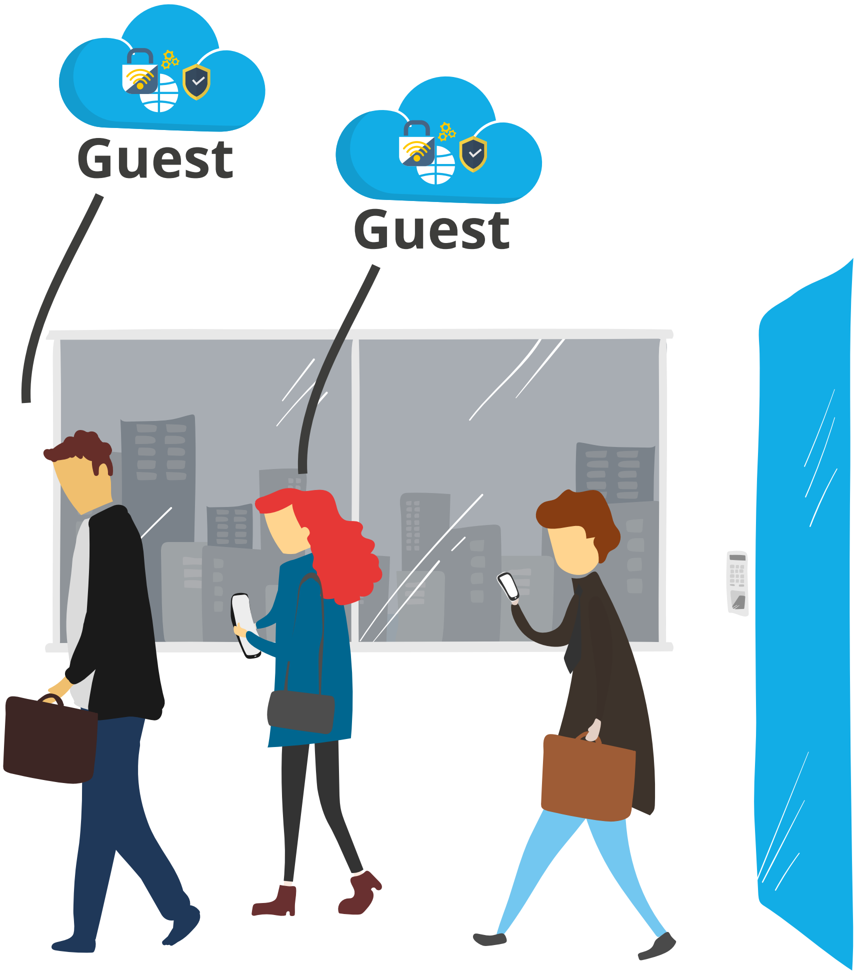
HURDLE 4: Connecting production machines to the network

Another challenge revolved around some of the older systems, such as the production machines in the production hall. They seem innocent at first sight, but as they too are connected to the network, our firm needed to find a way to integrate them as well. As they were all legacy systems, production machines didn't have the supplicant software that allowed them to use certificates. But of course, these machines can be recognised by their MAC-address. Therefore, our experts decided to use the integrated MAC-address database of the NAC-solution to automatically connect the production machines to separate compartments in the network. This way, the NAC solution functions as a single point of authentication, also for those devices that cannot use certificates.

> "Our experts built a guest portal so the administrator could allow access to guests within seconds, taking away the fuzz when welcoming new people"

HURDLE 5: Giving room to partners and guests

The last hurdle revolved around two important groups of people interacting with the firm: partners and guests. Understandably, the company didn't want to add them to their Active Directory, as this tool was meant to exclusively store details on employees. For partners, our experts used the internal user directory of the NAC solution itself, so partner details could be safely stored outside the Active Directory. Then, they created a separate network compartment for partners to work in. As for guests: they were directed to a guest portal where they could request access to specific network resources. Based on the request, an employee would allow them the access rights to specific resources for a limited time. The MAC-address database and the guest portal in combination with the integration of Active Directory meant that the administrators only had to deal with one system instead of three for authentication, authorisation and accounting.



Final judgement?

All hurdles taken! The firm was very happy, especially because they secretly thought their wishes were too good to be true. Our experts managed to comply with every single requirement, and even found a way to safely connect all devices to the network, including the ones that don't have certificates, and either through cable, Wi-Fi or VPN. Moreover, the NAC solution that was installed is low-maintenance, as everything had been automated. This means that our customer's administrator can manage everything in their own directory and doesn't need to access the NAC solution at all. For users, certificate renewal is easy: they get a notification and if they still have the rights for it, they get their new certificate without any hassle. Administrators work with a portal to welcome new guests, and connecting new devices is peanuts. All the administrator has to do, is notify the NAC solution that things have changed, and it will take of the rest.