Why every business needs a Network Access Control solution

Soliton®

Introduction

Since the early 2000s, businesses have used Network Access Control to monitor and regulate their networks, create an optimal working experience for employees and guests alike, and improve performance. However, as technology has advanced, the capabilities of NACs have grown with it. In addition, it has needed to cope with the proliferation of new connected devices and new ways of working. Today, a NAC is an essential tool for any business that runs a network.

IT managers today face a variety of challenges every day. They need to offer a safe, reliable network for company machines and devices that belong to employees and guests (including IoT). While doing this, they need to mitigate the risks of cybercrime. NACs help IT managers achieve this balance by offering complete visibility around who is on the network and what they're doing, regulating access levels, and monitoring interactions. A NAC can also improve a network's performance.

In this guide, we'll examine what NACs are and what they do. We'll also look at why your business needs one, including how they make life easier for your employees and create a seamless experience for your guests. Finally, we will also look at what sets NetAttest EPS apart from other NAC solutions on the market.

What is NAC?

A Network Access Control system is a tool that regulates an organisation's network.

NAC systems are there to ensure that only the right users with authenticated and reliable devices (whether they belong to the company or the individual themselves) can log on to the network. Once they are there, the NAC regulates the areas of the network users can access while monitoring and logging their activity.

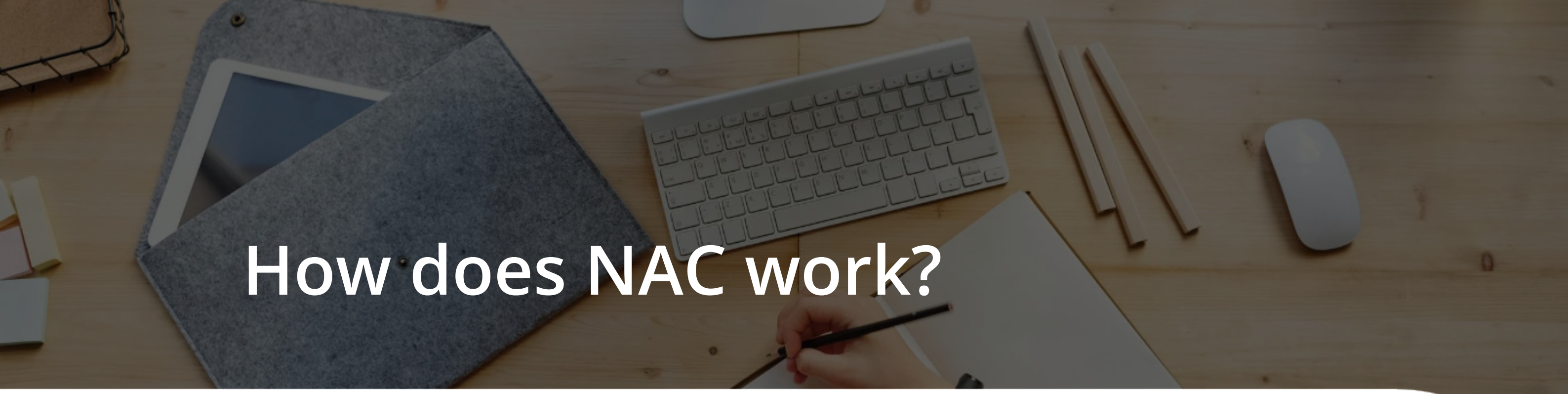
NACs follow the principle of the 3 A's:

Authentication - Who are you? Can you prove you are who you say you are?
Authorisation - What are you allowed to do on the network?
Accounting - What are you doing, and for how long?

Every organisation's network contains private data that, if the wrong people access it, could cause serious, life-changing issues. NAC solutions protect your network and your business from such disasters. This scenario has always been the case, but having a robust NAC has become even more critical in recent years.

The number of machines on a business' network has increased sharply in recent years. There are company-owned devices, plus personal ones owned by individual employees who can log on remotely, including mobile phones. In addition, there are connected devices, from smart speakers to automatic light switches, that need a slot on the network. Businesses also need to offer an opportunity for guests in their buildings to log on to the network.

This increase presents new risks; which NACs help IT Managers control. A NAC solution allows businesses to create a safe and productive working environment for employees, guests, and associated external stakeholders.



How does NAC work?

When a machine attempts to log on to a network regulated by Network Access Control, a sequence of events takes place:

- Identification - The NAC primarily identifies the device. The issued certificate is typically stored in the Computer store to enable the access before the user logs onto the Computer. If necessary, in a second step, it's also possible we are also evaluating the user and the group membership.
- Who is it?
- Is it a known user?
- What area are they trying to access?
- Where are they located?
- When was the access request made?
- How was the request made (cable, Wi-Fi, VPN)?
- Assigning a role - NAC defines which parts of the network they can access and the parts they can't
- Enforcement - NAC can deny access to areas where certain users are not allowed

The ability to restrict access to certain parts of the network for specific users is called segmentation. As well as preventing unauthorised access, it also helps prevent viruses and malware from spreading across the network if something goes wrong.

If a NAC system refuses access to a user or device for some reason, it puts them in a restricted area with little or no access to the network. This keeps the network free of unauthorised devices and reduces the risk of cybercrime.

A NAC makes a business' Wi-Fi network safer by automatically applying encryption keys for each session. As a result, attackers cannot use any shared or publicly known secrets to sniff network traffic.

Solutions like NetAttest EPS use digital certificates to make this process faster, simpler, and more secure. In the next section, we'll explain this in more detail.

How digital certificates give you the edge

A digital certificate is a credential that identifies a user (and often their device or devices) known to the network. With certificate-based authentication, a business can verify that all devices connected to its network are authorised.

In the past, networks would combine certificate-based authentication with user authentication such as a username and password. However, solutions like NetAttest EPS can deliver all the benefits to a business without users having to deal with unwieldy passwords. And on Windows it's possible to use the current Windows user with the certificate of the device. Passwords are time-consuming to set up and quickly forgotten, which causes more problems.

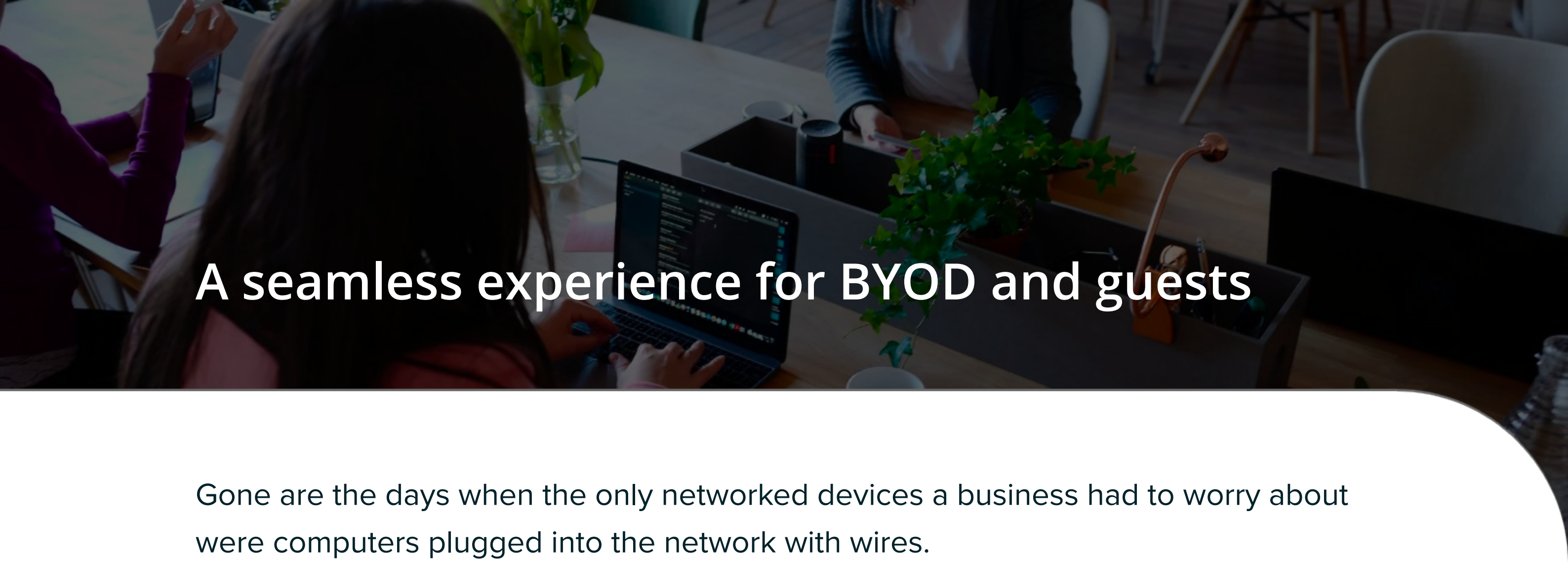
Digital certificates allow users to access the correct areas of the network the first time and every time, which reduces queries to IT support teams. For businesses, digital certificates are scalable - it's never been simpler to add devices to the network, essential when there are more devices than ever and more employers checking in from random office locations.

The Soliton KeyManager offers networks a more straightforward way to distribute digital certificates. By introducing a less complicated 3-step certificate administration process, IT managers can dramatically shorten the life of a digital certificate, which enhances security.

The application offers a user self-service to automatically request and install user and device certificates on any device, with only three steps. The Soliton KeyManager app presents the user a warning to renew their certificates, allowing users to click the appropriate link, which delivers four significant benefits to businesses:

- Reduces the time the IT team spend on certificate management
- Adds a new layer of security to the Simple Certificate Enrolment Protocol (SECP) via a unique secret per request
- Enables public and private key pairs to be generated

  Thanks to the way it's created, it never leaves the device during the issuing process



A seamless experience for BYOD and guests

Gone are the days when the only networked devices a business had to worry about were computers plugged into the network with wires.

Today, businesses need to offer reliable Wi-Fi services on their premises. Employees will want to (and be expected to) log in at home using their own devices, as well as company machines. We call these Bring Your Own Devices or BYOD. This is even more relevant during and in the aftermath of the COVID-19 pandemic.

Some guests arrive at a business' premises expecting to access Wi-Fi quickly and easily or plug wired devices into the network to give presentations or facilitate transactions.

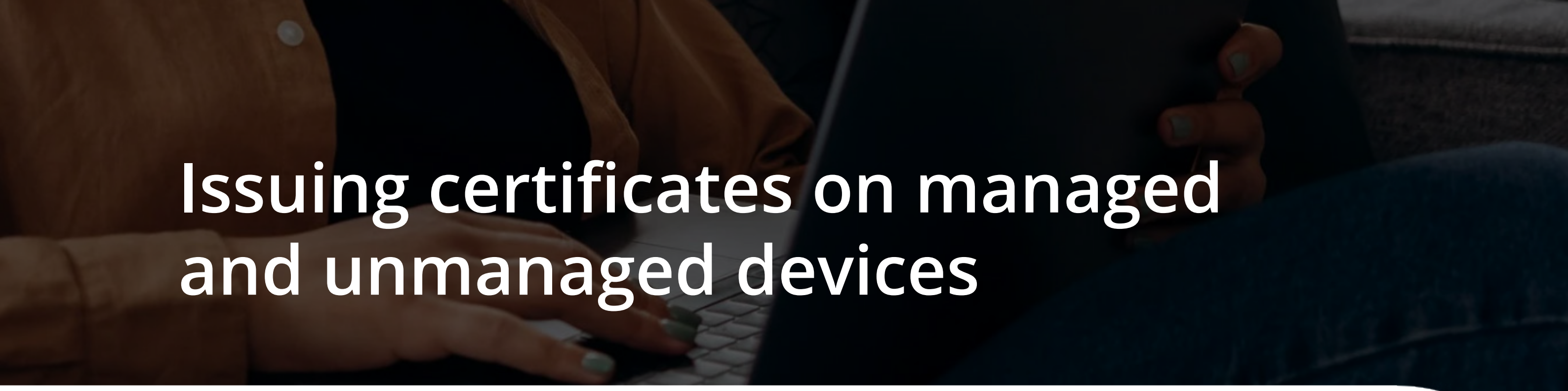
How can IT managers balance these expectations with the need to safeguard security?

A business' NAC is the key to balancing a seamless service with robust security. As well as authenticating, authorising and accounting, your NAC must be able to:

- Protect authentication flow as it travels between devices
- Only allow approved users and devices to access the network
- Limit access to specific areas and services of the network
- Give your IT team visibility over precisely who is on the web, with which specific devices, including guests

NetAttest EPS comes with a built-in RADIUS server. The RADIUS server allows control over who can connect with a company's network. It supports various methods to authenticate users and prevents private information from leaking out to suspicious outsiders. You can also use it to assign individual users to special network permissions.

And what's more, it's simple to use, with support for all common security standards. Your employees will appreciate its ease of use, while your guests will be delighted with the seamless network access you provide when they visit you.



Issuing certificates on managed and unmanaged devices

The great thing about using digital certificates for authentication (as opposed to usernames and passwords) is that you can issue them to devices that your company does not manage without troubling your IT team.

The NetAttest EPS-*ap* is included as standard with the NetAttest EPS solution that helps distribute certificates to unmanaged external systems, such as personal devices or the devices of partners and contractors. In addition, the Soliton KeyManager app removes the need for specific mobile device management to deploy these certificates, making it easy and secure for users to install digital certificates on their systems.

Many companies find providing network access to external devices a security problem. So they're using a MAC-based NAC solution that is easy for hackers to spoof and evade restrictions. By getting hold of machines under false pretences, spying on broadcast traffic, or using brute force, cyber-criminals can get authorised MAC addresses, which leads to unwanted access to your network.

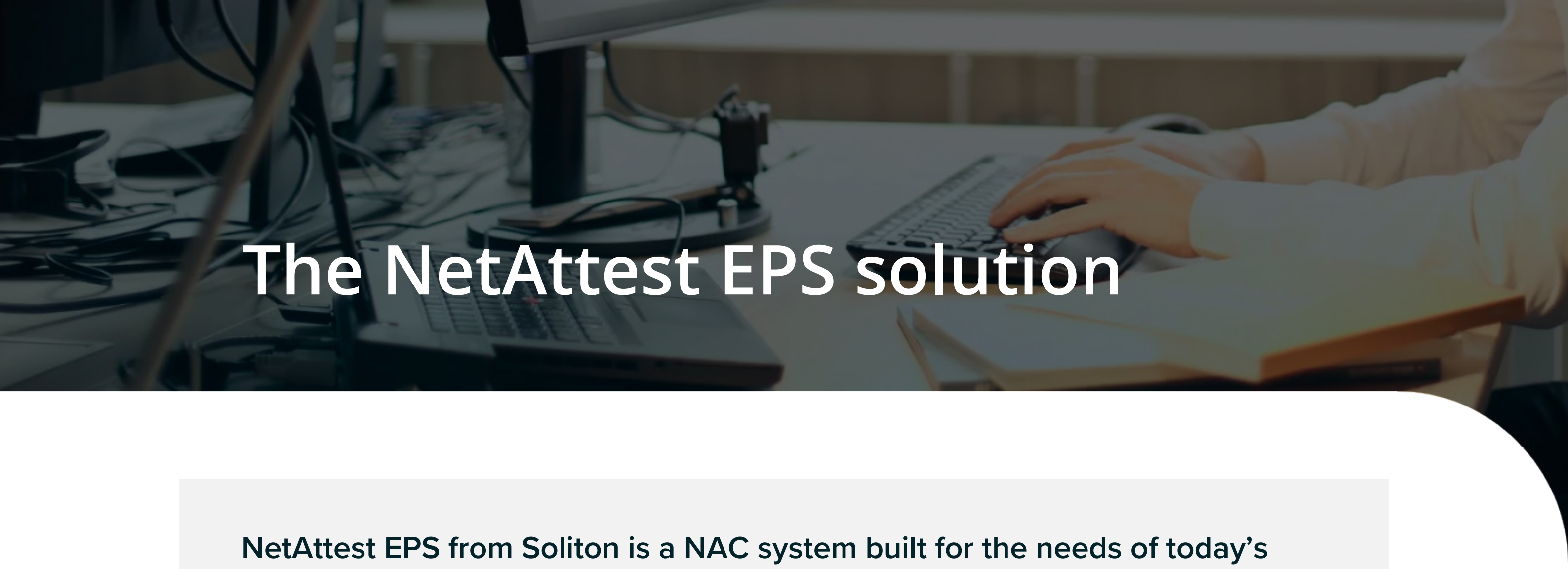
It's impossible to entirely avoid dealing with machines that only come with MAC addresses (especially in areas such as healthcare and automotive) as an identity. At Soliton, we've worked hard to balance these requirements with your security needs.

Using a dedicated database for MAC addresses, NetAttest EPS simplifies the process of issuing access for these devices:

- It gives you all the tools you need to add new devices to your network quickly
- A secure MAC address database with storage for up to 200,000 addresses
- A dedicated interface for registering new MAC addresses

One thing that makes NetAttest the ideal NAC solution is that it never uses agents. It does not require anyone to install software on their devices, making safe BYOD genuinely possible. Plus, it improves security as the use of agents increases the attack surface.

Does your NAC solution give you this level of protection and convenience?



The NetAttest EPS solution

NetAttest EPS from Soliton is a NAC system built for the needs of today's businesses.

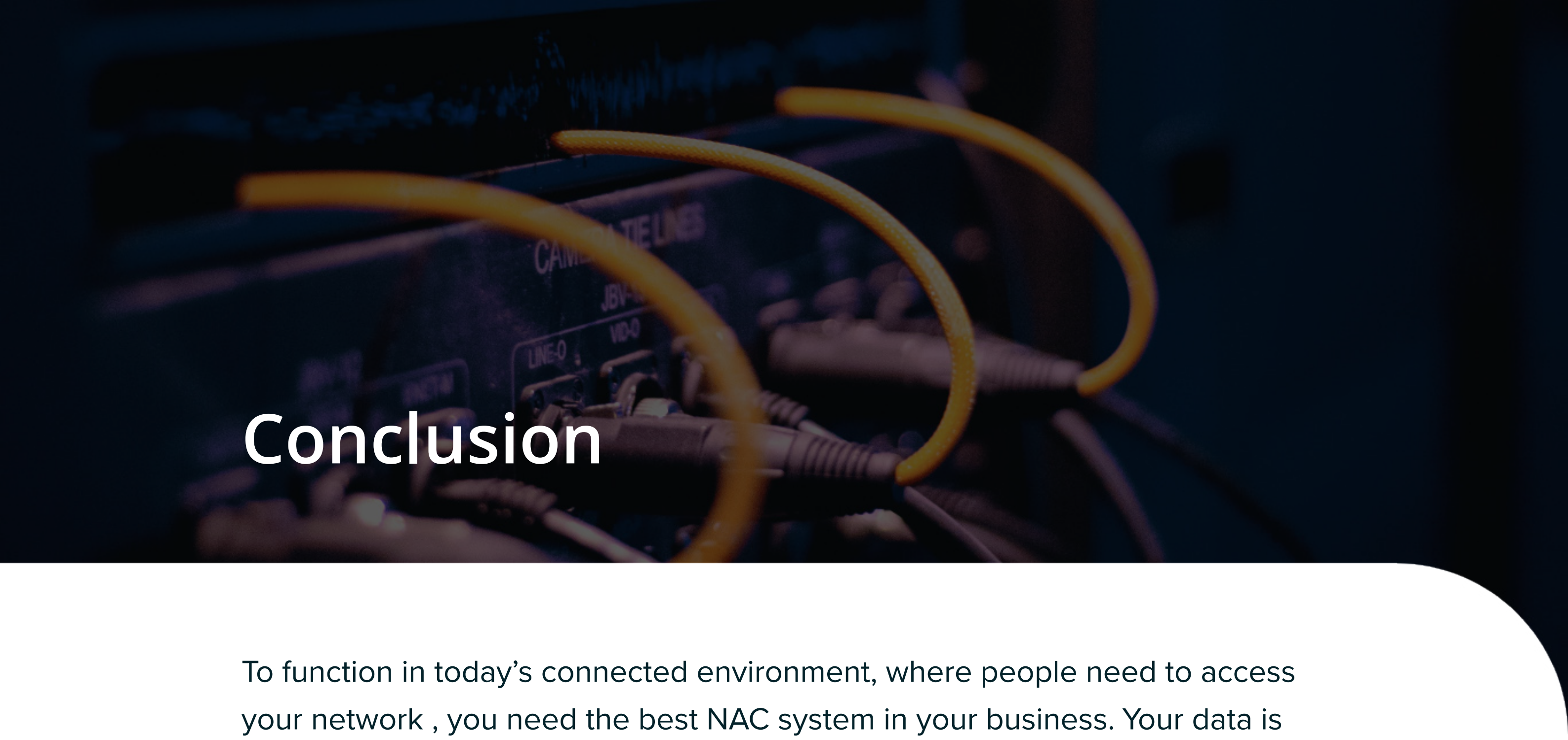
NetAttest EPS is a 100% rock solid, dedicated NAC solution. It gives IT managers everything they need to secure their network, regulate the access and improve performance.

Here's what sets NetAttest EPS apart from the herd:

- Stand-alone all-in-one solution - Includes everything you need in a NAC solution,
- including the Certificate Authority for creating certificates and a RADIUS server for enforcing access policies
- Suitable for businesses of all sizes - available for virtual or hardware appliances
- Flexible deployment with high availability
- Cost-effective - low implementation cost and low operating costs
- Soliton KeyManager application helps users securely download and install certificates on their devices, even if those devices are private and unmanaged
- Soliton KeyManager app allows users to avoid common mistakes which could negatively impact IT security

Of course, there are also a few things NetAttest EPS doesn't do:

- There's no vendor lock-in
- We don't use agents at the endpoint - avoiding complex life cycle management due to software updates and agents with security holes
- No posture checking



Conclusion

To function in today’s connected environment, where people need to access your network , you need the best NAC system in your business. Your data is too precious to trust to anything else.

However, a NAC is more than a security solution. It helps you create a productive working environment for your team and create an impressive, seamless experience for your guests.

NetAttest EPS is the industry-leading NAC solution for your business - pioneering technology for today’s world.

See NetAttest EPS in action today.

Get in touch

If you’re concerned about remote access, cybercrime, or VPN user frustration, simply get in touch to find out more about G/On.

🌐 solitonsystems.com

✉ emea@solitonsystems.com

☎ +31 20 896 5841