A level of visibility that will transform your network security

The explosion in the number and type of devices connecting to your network, with emerging trends like Bring Your Own Device (BYOD), Internet of Things (IoT), Operational Technology (OT) and virtualised appliances, significantly expands your attack surface – but are invisible to most security products. In contrast, BT Managed Network Access Control (NAC) Security provides 100% device visibility across all IP endpoints as a foundation of your network security.

Continuous discovery, classify and assess devices to gain complete situational awareness and manage risk:

- discover all managed and unmanaged devices in real time as they connect to your network
- see devices connecting and categorise them to identify function, type, operating system, version, vendor and many other features
- assess their security posture to determine risk profile by determining patch status, security status and whether or not the device is authorised
- controlled deployment through accredited experts and project management delivering your solution
- peace of mind through reactive and proactive monitoring of the service
- continuous improvement and tuning of the service to maintain its effectiveness as attack vectors change.

Traditional network security solutions tend to focus on external attacks, but devices such as firewalls may have limited impact on threats arising from within the network. BT Managed NAC Security can be deployed to protect the network against insider threats such as:

**Rogue devices:** Well-meaning employees can extend the network with inexpensive wiring hubs and wireless access points. These can cause the network to become unstable, and become a source of infection and data loss. Our Managed NAC Security service will detect all devices connecting and be able to identify what and where they are.

**Malware and Botnets:** Studies show that even well-managed enterprises have infected computers because of zero-day attacks or out-of-date antivirus. Once your PCs are compromised, they can be used in "pivot attacks" whereby outsiders can scan your network and steal your data. We’ll help you identify and categorise endpoints and assess and report on their security status.

**Compliance:** Endpoints can be misconfigured, virtual machines can appear on your network with improper settings or inappropriate software, and security controls can be de-activated. Non-compliant systems are security risks. Our service can scan all devices connecting and identify instances of non-compliance.
A comprehensive solution to see and categorise all devices connecting to your network in real time

Our Managed NAC Security offers:
- the provision of NAC solutions from world leading vendors
- accredited expertise to design and deploy Managed NAC on your network in a controlled manner
- in-life management and monitoring of the solution
- continuous improvement and tuning so that it continues to meet your needs.

Why choose BT?
With operations in over 180 countries supporting some of the world’s largest companies, from financial institutions to pharmaceuticals, we have a unique perspective on cybercrime. We know that a cyber-attack can happen anytime.

We’ve built a team of 3,000 experts across global centres. They are constantly watching, learning, predicting and responding to threats to protect us and our customers. So you can rely on us to protect you.

Reduce risk, through a Managed NAC solution professionally managed and monitored by BT.

What could Managed NAC Security do for you?
Visit bt.com/security

Managed NAC Security