

## SECURITY

The sophisticated capabilities of network access control make it a flexible, effective security tool, writes Anish Chauhan

# A discerning approach to security

### KEY POINTS

- Network access control enables businesses to manage all levels of access holistically
- Some systems prevent users on unrecognised devices from connecting legitimately
- NAC checks the terminal and applies updates to make it safe before granting access

**A**lthough network access control (NAC) has been around in one form or another for two or three years, it is now gaining significant momentum as an emerging technology. Awareness is growing within businesses as they begin to understand NAC's capabilities and the benefits that it can provide, instead of opting for less holistic approaches to network security or relying on firewalls and anti-virus software to keep intruders at bay.

The term NAC describes a system that controls all levels of access to a network, from user authentication to refusing network access to unknown or unsafe users.

This approach brings substantial benefits, providing flexibility, security and efficiency, which can all contribute to a very real return on investment. It can significantly reduce security issues surrounding unauthorised access and viruses, which can cost businesses huge amounts of time and resources to correct.

The problem with existing approaches is that they can prevent users from connecting to a network on unrecognised devices, without offering an alternative. This is not only frustrating for the user in question, but it is also a root cause of inefficiency: employees cannot access their work, and yet again the IT department is called upon to resolve the issue. Consequently, IT managers go through this painstaking process every time an employee wants to access the company network via a new laptop or smartphone.

#### Finding the problem

NAC systems provide a more sophisticated solution by assessing the end point, and only allowing network access if it meets the criteria laid out. The real advantage is that instead of simply denying the user access, NAC will check and update the terminal in question to make it safe.

For example, if the local agent reports that the anti-virus software is



NAC can improve efficiency by allowing legitimate users to access a network remotely

out of date, the NAC management platform will then quarantine the terminal, only allowing it access to the internet to update the software. Once the terminal is judged to be secure, it is then granted access to the rest of the network.

As more and more employees are given company laptops and smartphones and the number of remote workers rises, so the need for NAC increases. Large, network-critical companies with a mobile workforce can benefit greatly by implementing an NAC system, which adds value by decreasing the amount of time IT departments spend firefighting network access issues.

General network security is also enhanced, and employees can connect their devices to the company network more easily, securely and without risk.

Companies that have previously been deterred by a perception of high set-up costs may be interested to learn that NAC is one of the cheaper methods of giving "unmanaged" de-

vices access to a network, in addition to being one of the most flexible. As ever with security issues, the decision to opt for NAC is a question of priorities.

#### Closer integration

As NAC becomes more established, it is likely to evolve over the next few years. There is already evidence of the technology being integrated with other software and hardware systems. Currently, the reporting agent has to be pre-installed on every terminal, but this is progressively moving to a position of improved integration of NAC with existing operating systems.

These developments will provide customers with even greater flexibility and value, but even now, network access control remains one of the most effective catch-all solutions for securing an organisation's network. ●

NAC is one of the cheaper methods of giving 'unmanaged' devices access to a network

Anish Chauhan is network consultant at Networks First

Security management is high priority  
<http://tinyurl.com/ygqv656>