

Network Access Control (NAC) Buyer's Guide

You expert guide to network access control (NAC)



In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

■ Introduction to network access control products in the enterprise

Rob Shapland, First Base Technologies LLP

Network access control can keep rogue or compromised devices off of corporate networks. Expert Rob Shapland explains how NAC can benefit enterprises.

The technologies and processes that make up NAC security have been around as a product in various guises for many years -- originally as part of intrusion prevention systems (IPS), or integrated into various other products such as wireless systems. However, in the past, NAC security wasn't delivered in the unified manner in which it can now be deployed.

In addition, organizations would traditionally leverage NAC technologies to detect and protect against rogue devices connected to the physical network, usually in the form of Windows desktops or laptops. However, as technology has progressed and the number and types of network-connected devices have proliferated, NAC products have been updated to account for wireless networks, mobile devices and the bring-your-own-device (BYOD) phenomena, and cloud-based services.

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

BYOD, in particular, has hugely impacted the face of the NAC market, with controlling personal devices -- primarily smartphones and tablets -- becoming one of the most important roles that NAC products play over the last few years. As a result, NAC vendors are increasingly partnering with mobile device management (MDM) providers in order to ensure that mobile devices are handled correctly.

Partnerships between MDM and NAC providers usually involve integrating mobile management modules to a NAC control system. There are a number of advantages when MDM providers integrate their products with NAC. MDM software is only aware of devices that are already enrolled in the system; and, by integrating with NAC, it can be aware of new devices connecting to the network as well.

Also, MDM does not typically control network access, only access to applications and enforcement of encryption. NAC integration can provide the same policy enforcement and access control to mobile devices as it does with desktops and laptops, and can enforce the installation of the MDM agent before network access is permitted. Integration also means there is only one system to manage, which leads to less conflict between MDM and NAC policies.

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

Why network access control?

Network access control products are useful because they allow organizations to control the myriad of different endpoints connected to corporate networks, thereby helping to protect them from rogue and compromised devices. They do this by enforcing pre-defined policies, which require connected endpoints to meet prerequisites, such as the type of device or the presence of up-to-date patching and antivirus software.

While NAC products can be used by organizations of all sizes, they are most relevant to those that have a large number of employees with many different devices (for example, smartphones, tablets and laptops). In addition, NAC aids IT in the enormous challenge of securing network access when a company has many satellite offices.

How network access control works

When deployed, NAC products immediately discover all devices connected to a network, categorizes them by type, and then react to them based on pre-configured compliance rules implemented by the organization's security team. By react, we mean NAC enables device access to a network based on a specific, per device basis with granular controls over what type and level of

In this e-guide

■ [Introduction to network access control products in the enterprise](#)

■ [Three reasons to deploy network access control products](#)

■ [Five questions to ask before you buy NAC products](#)

■ [Comparing the best network access control products](#)

access is allowed. These controls are delivered by policies that are defined in a central control system.

Policies that might be defined would be to disallow all Android smartphones and tablets, for example, or disallow all devices that run Microsoft Windows that do not have the latest service pack. Admins could even block devices based on a whitelist of MAC addresses, making it more difficult for rogue devices to connect to the network.

The importance of NAC integration

What is becoming increasingly important for organizations is that NAC products seamlessly integrate with existing security infrastructure, especially security information and event management (SIEM), IPS and next-generation firewalls (NGFW). NAC systems can use alerts generated by these integrated products to better react to changing network status. Such as blocking all new device connections if an intrusion attempt is flagged, or blocking a single device based on its behavior (e.g., the device is initiating port scans) and (if necessary) block a device based on the information received -- be it because a specific device is initiating attacks on the network, or because it has been compromised.

Some NAC products can also integrate with Active Directory in order to control network access based on group policy, ensuring the user only has the network access required to fulfill his job. For example, an organization wouldn't want a

In this e-guide

- Introduction to network access control products in the enterprise
- Three reasons to deploy network access control products
- Five questions to ask before you buy NAC products
- Comparing the best network access control products

call center agent to have access to the human resources database, or a contractor to have access to pension information.

Agent and agentless network access control

The first task NAC must achieve is to inventory all the devices connected to the network. This can be done with agents (or an app for mobile devices) that are installed on each endpoint to gather this data, or it can be agentless. Whether inventory is performed with or without an agent (or a combination of the two) varies from NAC product to NAC product.

While NAC products can be used by organizations of all sizes, they are most relevant to those that have a large number of employees with many different devices.

Agents gain detailed information about devices by accessing their registries, running processes and file structure in order to enumerate the installed operating system (OS) and software versions, hardware makeup (processor, memory, storage, and the like) and detect any security concerns. There are certain limitations to agent-based NAC that organizations should be aware of, however.

First, NAC products need to be able handle devices that connect without an agent. Relying on an agent would only leave admins with two options: deny all

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

access or grant access to everything. Neither of which is a valid response, because denying all access would make it impossible to add new devices to a network, and allowing all access would defeat the purpose of the NAC system.

Additionally, individual agents do not work with all OSs and certainly can't be installed on devices such as printers, routers or voice over IP (VOIP) systems. That's a problem because an all-encompassing NAC system should be able to control access for all types of devices. There can also be problems if a device is required to connect to a different network, because it may not have the correct agent installed, though this can be alleviated if the agent is non-persistent and therefore only installs temporarily while connected to the network.

In agentless installs, information is gathered either through passive or active discovery. In simple terms, passive discovery monitors the network for traffic emanating from endpoints, and uses information that is present within the traffic to discover information about the endpoint (for example, the manufacturer and software versions). Active discovery allows for the gathering of much more detailed information, and achieves this by logging onto connected devices using Active Directory credentials (in the case of Windows devices), or by using port scanning and fingerprinting techniques for other devices.

Once a NAC product has inventoried all the devices connected to the network, it continues to monitor them for changes and malicious activity. Any activity from an endpoint that is deemed to be a security risk (such as a port or vulnerability scan) can therefore be detected and stopped.

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

The cost of and management of NAC

NAC products are sold either as virtual or physical appliances. Pricing depends on the number of endpoints that the system will need to handle, but typically ranges from around \$10,000 to \$25,000. On top of this, there are ongoing support costs of around \$2,500 a year, plus any additional costs in providing training to staff members responsible for managing the product.

The technology is managed centrally using an appliance provided by the NAC vendor. Some vendors provide training as part of the package to teach staff how to use the equipment, how to configure policies and how to manage the alerting systems. With this in mind, organizations that are looking to implement NAC systems should be aware that time (and potentially money) will need to be dedicated to training, and an internal admin will need to have part of his job role dedicated to managing the NAC product.

Conclusion

NAC is a powerful security product when implemented correctly, and can help an organization feel in control of the network and the devices connected to it, especially with the huge number and different types of devices that are now being used. It is not a silver bullet that protects against all network threats,



In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

however. NAC technology should be used in conjunction with other systems such as SIEM, NGFW and IPS.

In addition, implementation of NAC should be backed up with security testing to ensure that the specific NAC product chosen by the organization is a good fit with existing IT security. And it should not either over-zealously block resources or provide too much access. The next article in this series examines different use cases for NAC to help readers determine if the technology is the right fit for their organization and, if necessary, help them make the business case for it to executive management.



 Next article

In this e-guide

- Introduction to network access control products in the enterprise
- Three reasons to deploy network access control products
- Five questions to ask before you buy NAC products
- Comparing the best network access control products

■ Three reasons to deploy network access control products

Rob Shapland, First Base Technologies LLP

Expert Rob Shapland presents use case scenarios that have led to a rise in the adoption of network access control products among enterprises.

Network access control (NAC) is a system that allows organizations to restrict access to resources on their internal network. Primarily used by financial institutions, corporations with high security requirements and some universities, NAC has (so far) failed to become the mainstream security product some thought it would when the technology first entered the market at the end of 2003.

Times are changing, however.

Thanks to the advent of bring your own device (BYOD) and the integration of NAC technology into mobile device management (MDM) products, NAC is enjoying a rise in popularity among enterprises in general. That's because a growing number of organizations are evaluating NAC as a useful IT security tool to better control device access to their networks.

//////

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

Large organizations are the primary group showing an increased demand for NAC. This is due to the unique demands enterprises have in regards to number of employees and granting access to contractors, visitors and third-party suppliers. As awareness of the risk of breaches associated with these groups grows, so too does the demand for NAC to help mitigate the risk. Most NAC vendors are also reporting an increase in demand in the small and medium-sized enterprise (SME) market. This has largely been driven by media reports of breaches and the potential reputational damage they engender.

However, NAC is an expensive investment, particularly for SMEs, so organizations must consider whether it will provide a tangible security benefit before deciding to purchase network access control products. It is especially important to assess the risk to the organization from BYOD, weak access permissions and advanced persistent threats (APT).

NAC scenario #1: BYOD threats

BYOD is the key reason NAC is increasingly becoming an in-demand technology. That's because securely handling mobile devices is a key concern for CISOs tasked with providing secure network access with minimal disruption to end users.

As the line between personal and professional time blurs, end users are demanding to use not just corporate-owned devices (smartphones, tablets,

//////

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

laptops, among others.), but personal ones for business as well. This greatly complicates endpoint and network security for organizations, which -- meanwhile -- need to support not just employees connecting devices to the network, but devices from third parties (e.g., visitors, partners and contractors) as well.

There are hundreds of combinations of device type, model and operating system versions out there today; and mobile devices can be configured in innumerable ways with a vast selection of installed apps. Personal devices, meanwhile, generally do not have enterprise-level MDM and antivirus products installed. Users quite commonly disable basic security settings, or install apps that appear to be genuine but may actually perform actions that compromise the security of the device.

All of this creates a unique challenge for organizations regarding how to allow these devices to connect and not compromise the security of the network; the more devices that connect, the greater the risk that the network can be compromised. Mobile devices, meanwhile, are increasingly being targeted by criminals, and apps containing malware have become a popular attack vector.

This is where NAC can play a vital role -- the top NAC products on the market today support Apple iOS, Android and Windows devices -- in automatically identifying devices as they connect to the network, and providing access that does not potentially compromise security. For example, when a personal mobile

//////

In this e-guide

■ [Introduction to network access control products in the enterprise](#)

■ [Three reasons to deploy network access control products](#)

■ [Five questions to ask before you buy NAC products](#)

■ [Comparing the best network access control products](#)

device connects, it can be granted access only to the Internet and not to any corporate resources.

NAC scenario #2: Delivering role-based network access

While NAC is generally thought of as a security technology that either allows or denies access to the network, one of the major advantages of it is the ability to deliver network access on a granular basis. This can be integrated with Active Directory controls to provide network access only to areas of the network that allow the particular owner of the device to perform their job role.

As most IT managers are aware, managing both Active Directory group membership and network share permissions in a large network is an often insurmountable task, and inevitably leads to excessive network permissions. Being able to manage this centrally through a NAC product can allow greater control and flexibility for delivering access to shared folders.

For example, on most internal network penetration tests I've been involved in, weak controls on network shares are a key vulnerability that NAC products would have gone a long way toward solving. They either directly provide access to personally identifiable information or provide access to data that allows further enumeration of network resources. In one test, a misconfigured IT share allowed access to passwords for a number of key databases that contained

//////

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

customer names, addresses, dates of birth and payment card details. NAC technology would have mitigated the risk posed to this data.

NAC scenario #3: Reduce the risk from APTs

Although NAC does not provide functions that directly detect and thwart APTs -- malicious software that establishes remote, persistent access to a network to extract data in a stealthy manner over a period of time to limit the risk of detection -- it can stop the source of the threat from connecting to the network. Some NAC systems even integrate with APT detection products (such as FireEye), and automatically isolate affected systems before attackers can further access the network.

Using the famous example of the attacks against Target in 2013, the original infection occurred when a third-party vendor that sold heating and air conditioning connected to Target's IT network. Hackers targeted the third party, whose connection was in turn used to attack and exploit Target's network.

NAC would have made it possible to automatically restrict access to the Target network by the HVAC vendor, thereby restricting access that the APT had to corporate data and resources. This would make it much more difficult for the attack to have the same level of impact it had, saving Target a lot of money and both the retail behemoth and its customers a ton of hassle.

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

Key questions to ask before deploying NAC products

NAC is not suitable for all businesses. The larger an organization -- and therefore the more devices that will connect to the network -- the more useful network access control products will be. That's why it is important to not just understand the use cases for NAC technology outlined above, but to also ask a few important questions when deciding whether or not to deploy NAC products:

- Do I know how many devices are connected to my network? What they are and who owns them?

If you don't know the answers to all these questions, then an organization probably feels like it has little control over what is already connected to its network, and what will be connecting in the future. In this case, NAC is strongly worth considering, as it will provide visibility to existing infrastructure and any new devices connecting to the network.

- Who will be looking at the alerts generated by NAC?

The organization needs IT staff capable of interpreting these alerts and ensuring that network access is delivered securely but with minimum disruption to legitimate users. Bear in mind that this may be a full-time job dependent on how many endpoints are being managed by the NAC system. At the very least, the

In this e-guide

■ [Introduction to network access control products in the enterprise](#)

■ [Three reasons to deploy network access control products](#)

■ [Five questions to ask before you buy NAC products](#)

■ [Comparing the best network access control products](#)

IT team will need to be assigned specific time for monitoring alerts generated by the NAC system.

- Do I feel I have control over the data leaving my network?

Devices connecting to the network are obviously one of the key ways that data then leaves the network. If an organization is concerned about what data is being removed from the network -- and specifically what type of data -- NAC could help deliver network access to only the data required for the specific purpose a user is connecting. In this way, if a malicious user accesses the network, the NAC system would restrict their access, limiting the damage done by the compromise.

- Do I have current security systems that would need to integrate with NAC?

Consider what security systems are already present on the network. Are these being used effectively, or are they just white noise? If an organization chooses to implement NAC, it should ensure it integrates with, for example, its MDM or security information and event management (SIEM) products. This will save the additional overhead of managing different IT security systems on separate platforms.

- Does the business need the ability to scale up deployment?

NAC products are often sold on a per-endpoint basis. Organizations will therefore need to consider the cost of adding more endpoint licenses as its

In this e-guide

■ [Introduction to network access control products in the enterprise](#)

■ [Three reasons to deploy network access control products](#)

■ [Five questions to ask before you buy NAC products](#)

■ [Comparing the best network access control products](#)

infrastructure expands. For example, say an organization of 1,000 endpoints purchases a NAC product. However, because NAC licensing is delivered on a per-endpoint basis, if the organization expands greatly to 5,000 endpoints, the cost of the NAC product will increase dramatically as well.

Obstacles to NAC product deployment

Before deploying network access control products, consider the following obstacles:

1. Ensure there is sufficient time available to monitor alerts. Without monitoring and interpretation of alerts, the data provided by the system can be at best wasted and -- at worst -- disrupted (if network access is blocked for a user that requires it).
2. Look at the connections into the organization's network. Do users connect via SSL VPN, or over a product such as Citrix? Ensure the NAC system integrates with the systems already established on the network or it won't work to full effect.

Choosing to implement NAC can drastically improve an organization's network security posture by allowing for greater control over what devices are accessing the network, and what they are granted access to. By effectively sandboxing



In this e-guide

- Introduction to network access control products in the enterprise
- Three reasons to deploy network access control products
- Five questions to ask before you buy NAC products
- Comparing the best network access control products

untrusted parties (such as visitors or third parties) into protected areas of the network, the risk of an intentional or accidental breach can be reduced.

Consider whether the main benefits of NAC -- such as greater control over BYOD, more granular access to network shares and better protection against APTs -- is worth the investment. Take into account that implementing NAC not only requires upfront expenditure, it also entails ongoing investment in the form of additional licenses, training, monitoring of the NAC system and responding to alerts.

And, don't forget, NAC also needs to work harmoniously with existing IT security systems. A number of network access control products integrate directly with existing MDM or SIEM systems, which have central management consoles, and reduce costs associated with administration and training.

The next article in this series will outline the criteria organizations should consider when looking to procure a NAC product.



➤ Next article

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

■ Five questions to ask before you buy NAC products

Rob Shapland, First Base Technologies LLP

Expert Rob Shapland examines the important criteria for evaluating network access control (NAC) products for enterprise use -- before you buy.

As network borders become increasingly difficult to define, and as pressure mounts on organizations to allow many different devices to connect to the corporate network, network access control (NAC) is seeing a significant resurgence in deployment. Once seldom used by organizations, endpoint protection is now a key part of IT security, and network access control products have a significant part to play in that. From a hacker's perspective, well-implemented and managed NAC products can mean the difference between a full network compromise and total attack failure.

Today, NAC is often positioned as a security solution to the BYOD era, but it is also increasingly becoming a very useful tool in network management -- acting as a gatekeeper to the network. It has moved away from being a system that blocks all access unless a device is recognized, and is now more permissive, allowing for fine-grained control over what access is permitted based on policies

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

defined by an organization. By supporting wired, wireless and remote connections, NAC can play a valuable role in securing all of these types of connections.

Once an organization has determined that NAC will be useful to its security profile, it's time to consider the different purchasing criteria for choosing the right NAC product for its environment. NAC vendors provide a dizzying array of information, and it can be difficult to differentiate between their products. When you're ready to buy NAC products and begin researching your options -- and especially when speaking to vendors to determine the best choice for your organization -- consider the questions and features outlined in this article.

NAC device coverage: Agent or agentless?

NAC products should support all devices that may connect to an organization's network. This includes many different configurations of PCs, Macintoshes, Linux devices, smartphones and tablets. This is especially true in a BYOD environment. NAC agents are small pieces of software installed on a device that provide detailed information about the device -- such as hardware configuration, installed software, running services, antivirus versions and connected peripherals. Some can even monitor keystrokes and Internet history, though that presents privacy concerns. NAC agents can either run scans as a one-off (dissolvable) or periodically via a persistently installed agent.

//////

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

If the NAC product uses agents, it's important that they support the widest variety of devices possible, and can use agentless NAC if required. In many cases, devices will require the NAC product to support agentless implementation, to detect BYOD devices and devices that can't support NAC agents, such as printers and closed circuit television equipment. Agentless NAC allows a device to be scanned by the network access controller and be given the correct designation based on the class of device. This is achieved by aggressive port scans and operating system version detection.

Agentless NAC is a key component in a BYOD environment, and most organizations should look at this as "must-have" when buying NAC products. Of course, gathering information via an agent will provide more information on the device, but it's not viable on a network that needs to support many different devices.

Does the NAC product integrate with existing software and authentication?

This is a key consideration before you buy a NAC product, as it is important to ensure it supports the type of authentication that best integrates with an organization's network. The best NAC products should offer a variety of choices -- 802.1x (through the use of a RADIUS server), Active Directory, LDAP or Oracle. NAC will also need to integrate with the way an organization uses the

In this e-guide

■ [Introduction to network access control products in the enterprise](#)

■ [Three reasons to deploy network access control products](#)

■ [Five questions to ask before you buy NAC products](#)

■ [Comparing the best network access control products](#)

network. If staff use a specific VPN product to connect remotely, for example, it is important to ensure the NAC system integrates with it.

It is a significant overhead to support many different security systems that do not integrate with one another. A key differentiator between the different NAC products is not only what type of products they integrate with, but also how many systems within each category. Consider the following products that an organization may want to integrate with, and be sure the NAC product chosen supports the products already in place:

1. Security information and event management (SIEM): Integrating with SIEM can give context to alerts by providing detailed information regarding the device on the IP address that is the subject of the alert.
2. Vulnerability assessment
3. Advanced threat detection
4. Mobile device management
5. Next-generation firewalls

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

Does the NAC product aid in regulatory compliance?

NAC can help achieve compliance with many different regulations, such as Payment Card Industry Data Security Standard, HIPAA, International Organization for Standardization 27002 (ISO 27002) and National Institute of Standards and Technology. Each of these regulations stipulates certain controls that should be implemented regarding network access, especially around BYOD and rogue devices connecting to the network.

NAC can help with compliance with many of these regulations by continually monitoring network connections and performing actions based on the policies set by an organization. These policies can, in many cases, be configured to match those of the mentioned compliance regulations. So, when buying NAC products, be sure to have compliance in mind and select a vendor that can aid in this process -- be it through specific knowledge in its support team, or through predefined policies that can be tweaked to provide the compliance required for your individual business.

In this e-guide

■ [Introduction to network access control products in the enterprise](#)

■ [Three reasons to deploy network access control products](#)

■ [Five questions to ask before you buy NAC products](#)

■ [Comparing the best network access control products](#)

What is the true cost of buying a NAC product?

When you are ready to buy NAC products, this can be the most significant consideration, depending on the budget available for the procurement. Most NAC products are charged per endpoint (device) that is connected to the network. On a large network, this can quickly become a significant cost. There are often hidden costs with NAC products that must be considered when assessing purchase criteria.

Consider the following costs before you buy NAC:

1. Add-on modules. Does the basic price give organizations all the information and control they need? NAC products often have hidden costs, in that the basic package does not provide all functionality required. The additional cost of add-on modules can run into tens of thousands of dollars on a large network. Be sure to look at what the basic NAC package includes, and investigate how the organization will be using NAC. Is there extra functionality that will be required for the NAC product to provide all the benefits required?
2. Upfront costs. Are there any installation charges or initial training that will be required? Be sure to factor these into the calculation, on top of the price per endpoint (of course).

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

3. Support costs. What level of support does the organization require? Does it need one-off or regular training, and does it require 24x7 technical support? This can add significantly to the cost when buying NAC products (more on support in the next section).

4. Staff time. While not a direct cost of buying NAC products, consider how much monitoring a NAC system requires. Time will need to be set aside not only to learn the NAC system, but to manage it on an ongoing basis and respond to alerts. Even the best NAC systems will require staff to be trained so if problems occur, there will be people available to address the issues.

NAC product support: What's included?

Support from the NAC manufacturer is an important consideration, from the perspective of the success of the rollout and from assessing the cost. Some of the questions that should be asked are:

1. What does the basic support package (if any) include?
2. What is the cost of extended support?
3. Is support available at all times?
4. Does the vendor have significant presence in the organization 's region? For example, some NAC providers are primarily U.S.-based, and if an

//////

In this e-guide

■ [Introduction to network access control products in the enterprise](#)

■ [Three reasons to deploy network access control products](#)

■ [Five questions to ask before you buy NAC products](#)

■ [Comparing the best network access control products](#)

organization is based in EMEA, it may not provide the same level of support.

5. Is onsite training available and included in the license?

Support costs can significantly drive up the cost of deployment and should be assessed early in the procurement process.

What to know before you buy NAC

When it comes to purchasing criteria for network access control products, it is important that not only is a NAC system capable of detecting all devices that connect to an organization 's network, but that it integrates as seamlessly as possible. The cost of attempting to shoehorn existing processes and systems into a NAC product that does not offer integration can quickly skyrocket, even if the initial cost is on the cheaper side.

NAC should also work for the business, not against it. In the days when NAC products only supported 802.1x authentication and blocked everything by default, it was seen as an annoyance that stopped legitimate network authentication requests. But, nowadays, a good NAC system provides seamless connections for employees, third parties and contractors alike -- to the correct area of the network they are allowed to visit. It should also aid in regulatory compliance, an issue all organizations need to deal with now.



In this e-guide

- Introduction to network access control products in the enterprise
- Three reasons to deploy network access control products
- Five questions to ask before you buy NAC products
- Comparing the best network access control products

Assessing NAC products comes down to the small number of key questions highlighted in this article. They are designed to help organizations determine which type of NAC product is right them, and if so, which vendor provides the product that most closely matches those criteria. The next article in this series will compare and contrast the top NAC vendors on the market against the criteria laid out in this article to further help readers narrow down their options when buying NAC.



Next article

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

■ Comparing the best network access control products

Rob Shapland, First Base Technologies LLP

Expert Rob Shapland takes a look at the best network access control products on the market today and examines the features and capabilities that distinguish the top vendors in this space.

The need for organizations to have greater control over their network perimeter, especially in the age of BYOD, means network access control is demonstrating a distinct upturn in its fortunes compared to when it was first introduced to the market. Today, network access control fills an important security role of automating the type of access a new device requires, providing granular control over what resources can be accessed. This role was previously filled by IT security staff, but without automation, that can be time-consuming and can lead to mistakes.

When an organization is looking for the best network access control product for its needs, there are several factors to consider. Not all products fit all types of organizations, however, with some more targeted at larger firms -- with the associated cost -- while others are more targeted toward smaller businesses that do not need to support a large number of new devices of varying types.

//////
In this e-guide

■ [Introduction to network access control products in the enterprise](#)

■ [Three reasons to deploy network access control products](#)

■ [Five questions to ask before you buy NAC products](#)

■ [Comparing the best network access control products](#)

This article reviews the best network access control products available today. For the purposes of this article, we considered the following leading vendors: ForeScout Technologies, Bradford Networks, Cisco, Aruba Networks, Trustwave, Extreme Networks and Pulse Secure.

Device support

The key criterion to consider when it comes to device support is agent-based versus agentless network access control (NAC). NAC agents supply detailed information on connected devices, allowing policies to be accurately applied. This can include restricting devices that do not have up-to-date antivirus or that have prohibited applications installed. However, agents rely on these devices being enrolled in the NAC system. NAC agents can be further divided into persistent and dissolvable -- persistent agents are installed on the target device, whereas dissolvable agents provide one-time authentication of the device, and are then deleted.

Agentless NAC products give greater flexibility in terms of identifying any type of device that is connected to the network and applying the suitable policies. This can either be implemented through Active Directory -- through which the agentless NAC code assesses the device when a user joins the domain -- or by integrating it with other security products, such as intrusion prevention systems or network behavior analysis. The ideal product combines agents and agentless

//////

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

systems, defaulting to the agent report when available, and using the agentless solution as a fallback. This provides the greatest combination of accuracy and flexibility, a key requirement in a large network that needs to handle many different device types, such as BYOD.

Cisco is one of the top two players in the NAC market, mostly due to its market share in the network infrastructure space. In many cases, organizations find it simpler to roll out NAC products from the same manufacturer rather than go through their procurement process with another provider. Cisco's Clean Access product is capable of identifying devices using agentless methods, but is best deployed on a network already heavily invested in other Cisco products. If your network infrastructure uses different manufacturers, there are other NAC systems that may be better suited or less expensive.

The other top player in the NAC market is ForeScout CounterACT, a highly flexible product that offers good agentless detection of new devices joining the network. This allows it to identify a large number of device types and apply policies based on these. In terms of device detection and support, ForeScout provides an excellent solution.

Bradford Networks products are flexible in terms of device support, and allow for both persistent and dissolvable agents, as well as agentless NAC implemented at the Active Directory level, or in combination with security devices.

In this e-guide

■ [Introduction to network access control products in the enterprise](#)

■ [Three reasons to deploy network access control products](#)

■ [Five questions to ask before you buy NAC products](#)

■ [Comparing the best network access control products](#)

Slightly less flexible in this area are Aruba and Trustwave. Aruba is a key player in the wireless market, and its NAC product is therefore very good for BYOD, but can also be used for wired networks. The Aruba NAC product provides a number of different options for provisioning of services once devices connect, though it doesn't support true agentless implementation. Trustwave offer agentless and dissolvable agent products.

Integration

Ensuring that a chosen NAC system integrates with existing systems is one of the most important factors in choosing a suitable product. Many organizations have already invested heavily in products such as MDM, SIEM, vulnerability assessment, endpoint security and next-generation firewalls. NAC products will be less effective if they cannot integrate with these other security solutions. Before investigating in NAC systems, make a list of all the existing systems on your network that it would need to integrate with, and filter your search appropriately.

In terms of integration, the current winner appears to be ForeScout's CounterACT, with excellent partnerships with key players that sell various synergistic security products. It integrates with all the key vulnerability management tools, and provides support for most SIEM products that use

//////

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

standard messaging formats. There are also integrations with MDM and advanced threat detection products.

Another clear winner in this area is Bradford Networks' Network Sentry. The company has made it one of its policies to provide integration with as many products as possible -- its list of supported integrations is extensive, and include the major manufacturers. However, the downside is that many of these integration features add additional costs, which makes it one of the more expensive options. The other providers all have various different integrations, but none quite as extensive as the aforementioned two.

Regulatory compliance

NAC vendors are increasingly positioning themselves as great solutions for regulatory compliance with standards such as PCI DSS, ISO 27002 and NIST. Correctly implemented, NAC can help achieve compliance with these standards, but some vendors have better positioned themselves to do so more easily. The best in this area are Bradford Networks, Extreme Networks and ForeScout, all of which offer advice on how its products can be used for compliance.

ForeScout is particularly strong in this area through its Compliance Platform. This offers specific policies and reporting for compliance, including PCI DSS, SOX and HIPAA.

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

Support

Once your organization has chosen a NAC product, the next step is implementing and supporting it. For NAC to be effective, it needs to be managed by dedicated staff, or at least be made part of a staff member's responsibilities. It's important to consider what support is offered by the individual provider, and if that support is offered in your geographical location.

Support varies across the board in terms of costs and levels. In all cases, detailed technical support is an added extra that can considerably increase the cost of implementation. NAC products also have an end-of-life policy where the vendor stops supporting them, so the cost and frequency of upgrading the system will need to be considered.

Bradford Networks, for example, offers different levels of support with different costs. However, this support is primarily U.S.-centric, and therefore customers in other locations do not have access to the same level of support. Before investing in its product it would be prudent to assess its partners' ability to provide support. ForeScout also offers two levels of support, both of which come at a premium.

In this e-guide

- [Introduction to network access control products in the enterprise](#)
- [Three reasons to deploy network access control products](#)
- [Five questions to ask before you buy NAC products](#)
- [Comparing the best network access control products](#)

Evaluating the best network access control products

ForeScout is a good NAC product for large organizations with a similarly large budget, as it supports the most variety of devices and compliance modules. However, the integrations offered through its ControlFabric architecture -- such as SIEM integration -- often come as additional extras, and the product can cost significantly more than anticipated. Bradford Networks also offers a very versatile product, with excellent integrations and compliance support, but is limited in its ability to operate outside of the U.S. Cisco's product is primarily aimed at organizations that have invested in its hardware. The same is true of Pulse Secure's Policy Manager.

The next part of this series of articles will look at each product in turn, analyzing their strengths and weaknesses in more detail.

About the author

Rob Shapland is a senior penetration tester at First Base Technologies where he specialises in Web application security. He has used his skills to test the websites of companies ranging from large corporations to small businesses, using a wide variety of Web technologies. He is a firm believer that all penetration testing should have manual techniques at their core, using



In this e-guide

- Introduction to network access control products in the enterprise
- Three reasons to deploy network access control products
- Five questions to ask before you buy NAC products
- Comparing the best network access control products

automated tools to support these skills. He is also involved in network testing and social engineering.