# Network Access Control—Has It Evolved Enough for Enterprises?

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

**Trevor J. Dildy,** CCNA
Is a member of the classroom technology team at East Carolina University (USA). The team is responsible for researching the latest state-of-the-art hardware and software for ECU classrooms. He is a former member of the IT security team at Vidant Health, assisting with access administration requirements for the health system.

Information security is a field that continues to grow and mature. As technology advances, there will always be growth in new security techniques or solutions to help protect data from various attacks. Network access control (NAC) is the technique for network management and security that enforces policy, compliance and management of access control to a network. It also monitors and controls activity once devices and/or people are on the network.

Over the years, NAC has grown and many companies, such as Cisco, Trustwave and Bradford Networks, have developed solutions to help with its evolution. However, not all organizations believe that NAC has evolved to fit their needs. While NAC is an important part of information security and can help with data breaches, is it truly ready to be used in all enterprises or does it need to develop into a more usable technical solution before it is utilized everywhere?

## Reasons to Implement NAC

Enterprises have a lot of reasons to consider implementing NAC. When it comes to access controls, they need to have a wide range of options. But perhaps the pertinent question is whether or not enterprises are even ready to be utilizing NACs. NACs can be expensive to implement, but expense should not be an excuse to ignore the fact that threats are frequently trying to compromise enterprise systems.

One of the top reasons for implementing NAC, is bring your own device (BYOD) threats.[1] With more and more employees taking their own devices to work and using them for work purposes, NAC is becoming more in demand. There are many variations of mobile devices; some of the top operating systems are Apple iOS, Android and Windows. There are hundreds of combinations that deal with device type (e.g., smartphone, laptop and tablet) and model. Each of these smart devices now comes with a huge selection of applications (apps) that can be downloaded onto them.[2] There are many possible threats, especially since these personal devices do not typically have enterprise-level antivirus/antimalware or mobile device management (MDM) solutions installed.

Most NAC technical solutions are able to support the major operating systems on the market today. These solutions can automatically detect devices as they connect to the network and then make sure that they are not compromising the security that is in place. NAC is very useful when it comes to protecting the integrity of the network, but it can also help with allowing or denying access to the network. Active directory is the best implementation option for allowing and denying access to the network.

> **"NAC is very useful when it comes to protecting the integrity of the network, but it can also help with allowing or denying access to the network."**

Delivering role-based network access is another reason for moving to a NAC scenario.[3] As IT professionals know, having to deal with a large amount of network share permissions in a very large organization can be a difficult task. A NAC product solution makes it a little more bearable to manage all of the permissions that are needed for network storage folders as well as other active directory groups.

A third reason for implementing NAC in an organization, is reducing the risk from advanced persistent threats (APTs).[4] NAC does not provide any sort of solutions that will detect and stop APTs, but it can stop the attacking source from gaining access to the network.[5] This means that if a user account is causing an attack, the NAC can stop that account from causing any further harm if the NAC system detects any foul play.

When implemented correctly, NAC can help an organization feel in control of the network and the devices connected to it, especially with the huge numbers and types of devices that are being used.

## NAC Products

Cisco TrustSec, from worldwide IT industry leader Cisco, simplifies the provisioning of network access. Cisco TrustSec is embedded in the Cisco infrastructure that many organizations already use.[6] This solution comes with a firewall; the NAC portion comes as a separate component. This allows for easier security policy management and helps the organization manage network access.

The Cisco NAC solution helps by recognizing the users who are on the network, as well as their devices and roles. Another feature of the Cisco NAC solution is that it provides guest access and makes sure that the access provided is safe and secure. This is a valuable feature for anyone who is looking to implement a NAC system.

Another feature is that auditing and reporting are enabled. This allows for the tracking of who is on the network as well as making sure they do not try to gain unauthorized access to restricted parts of the network to which they should not have access. The features that Cisco's NAC system offers are very beneficial for most organizations that are willing to implement NAC systems.

There are other companies that have NAC products that can help organizations keep access limited to those who truly need it or base the access on the job that they need to perform each day. Trustwave Network Access Control, offered by global managed security services leader Trustwave, can be deployed seamlessly without an agent. Like most NAC products, it can be integrated into the active directory in order for it to be easier to determine who has what access.

According to Trustwave, its NAC solution has automated detection and restriction of noncompliant devices, as well as complete protection for all endpoints—managed and unmanaged. This is a very bold statement when it comes to NAC products.[7] Also, Trustwave claims that analysis of every packet from every device can be done. While it is possible to analyze many packets, it is hard to claim that there is a way to analyze every packet that comes through the NAC.

There are a few options in implementing the Trustwave product as outlined in **figure 1**. Like the Cisco NAC solution, Trustwave offers integrated support for BYOD. BYOD integration from Trustwave will help with device identification, authentication, categorization and threat mitigation. Trustwave helps organizations make the BYOD solution decision by providing a side-by-side comparison of its different options. The solutions they offer are an enterprise NAC, a managed NAC and a plug-and-play NAC. Each of the solutions has its own benefits. The plug-and-play option is an add-on software module that goes with the Trustwave managed unified threat management

**Figure 1—Options in Implementing Trustwave**

| TS-25 | TS-150 | X2500 |
|---|---|---|
| • Protects up to 100 endpoints<br>• Up to 64 virtual local area networks (VLANs)<br>• Can be installed on a desktop computer<br>• Option to include the rack mount kit | • Protects up to 1,000 endpoints<br>• Up to 128 VLANs<br>• Needs to be installed on one rack unit (1RU) rack mount | • Protects up to 2,500 endpoints<br>• Up to 128 VLANs<br>• Needs to be installed on a 1RU rack unit |

**Source:** Trevor J. Dildy. Reprinted with permission.

## Enjoying this article?

- **Learn more about, discuss and collaborate on access control and network security in the Knowledge Center.**
  *www.isaca.org/knowledgecenter*

(UTM) service. The managed NAC is similar to the enterprise NAC, but it is at a reduced cost and will not incur any capital expense. The enterprise NAC provides all the features and costs more than the other two options.

Trustwave offers numerous benefits, but it also has some very big claims that should be explored further. Trustwave's NAC products seem to be very good at what they do, and they will protect an organization's network without having to worry about an agent.

ForeScout Technologies is a global provider of continuous monitoring and mitigation solutions. ForeScout's NAC solution is CounterACT. This solution allows the organization to have real-time visibility of the people, devices, operating systems and apps that are connected to the network. The CounterACT solution will not disrupt users' daily operations; it will actually make sure that operations are not disrupted while giving the user automated controls to help preserve the experience of the user.[8]

CounterACT is different from some of the solutions on the market now as it is basically a turnkey solution. Everything within the CounterACT solution is contained in a single physical or virtual machine. This means that the setup is fast and easy. CounterACT also works with a majority of the routers, switches and firewalls that are on the market today. Like Trustwave's NAC, CounterACT is agentless, which means it can identify, classify, authenticate and control network access for devices whether they are managed or unmanaged.

CounterACT is also nondisruptive; this means it can be deployed in a phased approach. This will allow users to continue working without having to worry about losing access to critical files. A useful feature of CounterACT is the ability to decide what happens with devices that match certain parameters. When dealing with those parameters, there are three levels of control options: alert and remediate, limit access, and move and disable.[9] When it comes to alert and remediate, the system alerts when it detects an incident and triggers other endpoint management systems to remediate the issue. Limit access deploys a virtual firewall around the selected device and takes action to either restrict access completely or put it on a preconfigured guest network. The strictest parameter, move and disable, moves the device to a quarantined VLAN and blocks access to the network from the device.[10] With ForeScout's solution being one of the quickest and easiest to set up, deploy and integrate, it can be considered one of the top solutions that could potentially be implemented on a network.

When it comes to selecting NAC products, enterprises should choose the solution that best fits their network's needs. In addition to considering all of the costs, it is best not to select a solution that is designed for a smaller network.

## Advantages and Disadvantages of Implementing NAC

There are some arguments for, as well as against, the implementation of NAC. There are some compelling arguments that show that NAC should be installed on many of the organizations' networks so that those networks can have the proper protection against looming threats. One of the benefits is that it will stop malicious actors from being able to plug into the organization's network infrastructure. With employees and users bringing their own devices into the workplace, it is easy for them to also bring the necessary cable(s) in order to connect to one of the empty Ethernet ports and try to gain access to the network. NAC will help to prevent this from happening because the device that they are trying to connect to the network is not listed on the approved list or has not been registered as a trusted device within the NAC.

Another plus for NACs are that there are audit logs that can determine if empty ports are turned on or off. This can help the organization determine if there are some ports that were left on that should be taken offline so no one mistakenly connects to them. NACs also allow for the detection of devices that are plugged into the network's infrastructure that should not be.

NAC integrates well with other solutions. NACs are not meant to be stand-alone solutions; they are supposed to work in conjunction with firewalls and other security solutions to help improve the overall security measures of the organization. NACs are

needed to help an organization be more secure in relation to who has access and who should not have access. This also helps to minimize the number of breaches to the network.

It can be difficult to find the appropriate NAC product that best fits into the enterprise's network infrastructure. NACs have come a long way from where they used to be, but this does not mean that all enterprises are ready to implement them into their network. Like most software solutions, there are some benefits to NACs and some drawbacks. It is important to consider the downsides when deciding on a NAC solution.

It has been said that endpoint security checks work only when you need them least.[11] What this means is that NACs tend to work well when they are used to monitor laptops and desktops, but not so well when they are needed to monitor other devices/users coming into the enterprise. Another drawback is that, in general, NACs are always preparing to fight the last war, not preparing for the next one. NACs focus on the threats from the previous week. While this is beneficial, it is not what needs to be happening when it comes to advanced security threats. NACs need to be able to focus on the threats of tomorrow in addition to the threats of last week.

The return on investment (ROI) on NACs is a big unknown. While it might be crucial to have a NAC connected to the network, it might not yield the expected ROI. Putting a NAC in place is not cheap; it is very expensive and might prove to not be worth it for some organizations.

Another failure: Too much information can sometimes overload a NAC.[12] With a NAC, an organization can set its own policies for each user. This could result in a lot of policies, which would eventually yield a great deal of information that is not needed at the time or cause the NAC to generate false alerts.

Another NAC failure is that the network can control only what is seen.[13] With some of the NAC solutions allowing users access to officially permitted servers, this causes a huge hole in the NAC configuration. When anyone can have access to permitted servers, the server may become what is called a "jumping point" that will allow users to cruise the network and access other network objects or shares.[14] It is easy to get into the network when the MAC address is faked to the host. When it is faked, it will let the user or attacker into the network. Significant threats can come from the inside or outside because there is little to no physical security. Without proper physical security, it is easy for anyone to gain access to the NAC and harm its functionality. If there is no failover scenario, it is very likely that the organization will cause a denial-of-service (DoS) situation for itself—the same type of threat that the organization is trying to avoid.

> **"NACs need to be able to focus on the threats of tomorrow in addition to the threats of last week."**

NACs are also hard to manage with large numbers of switch ports because it is difficult to make sure that the switch ports are configured correctly all of the time. This can be harmful to the network. It is very important to make sure that, even where there are many ports, they are all configured correctly.

## Conclusion

All of the necessary research needs to be completed to determine what exactly the network requires to be as secure as possible. After the research on the proper product has been conducted, the pros and cons can be weighed and the decision made whether the cost of the NAC is acceptable to the organization. Cisco, Trustwave and ForeScout have NAC solutions that can be beneficial to any network; however, full realization of the benefits depends on fitting the solution to the network infrastructure currently in place. NACs will help to limit the access devices have and users are given. Access is determined based on users' job roles, which helps ensure that their access to network storage aligns with what they need to complete their job—not what they believe they need. NAC is not required, but it can save the organization damage to reputation, legal fees and additional work required after experiencing a breach.

## Endnotes


1 Shapland, R.; "Three Reasons to Deploy Network Access Control Products," *TechTarget*, 7 April 2015, *http://searchsecurity.techtarget.com/feature/Three-reasons-to-deploy-network-access-control-products*

2 *Ibid.*

3 *Ibid*.

4 *Ibid*.

5 Boscolo, C.; "How to Implement Network Access Control," *ComputerWeekly.com*, November 2008, *www.computerweekly.com/opinion/How-to-implement-network-access-control.*

6 Network Admission Control, Cisco, *www.cisco.com/c/en/us/solutions/enterprise-networks/network-admission-control/index.html*

7 Trustwave Network Access Control, *www.trustwave.com/Products/Network-Security-and-Access-Control/Network-Access-Control/*

8 Network Access Control (NAC), ForeScout, *www.forescout.com/solutions/network-access-control/*

9 Snyder, J.; *NAC Deployment: A Five Step Methodology, Opus One*, February 2007, *www.opus1.com/nac/vendorwhitepapers/opusone_nacdeployment.pdf*

10 *Ibid*.

11 Snyder, J.; "The Pros and Cons of NAC," *NetworkWorld*, 12 June 2006, *www.networkworld.com/article/2304152/lan-wan/the-pros-and-cons-of-nac.html*

12 *Ibid*.

13 *Ibid*.

14 *Ibid*.