The Evolution of Network Access Control

09

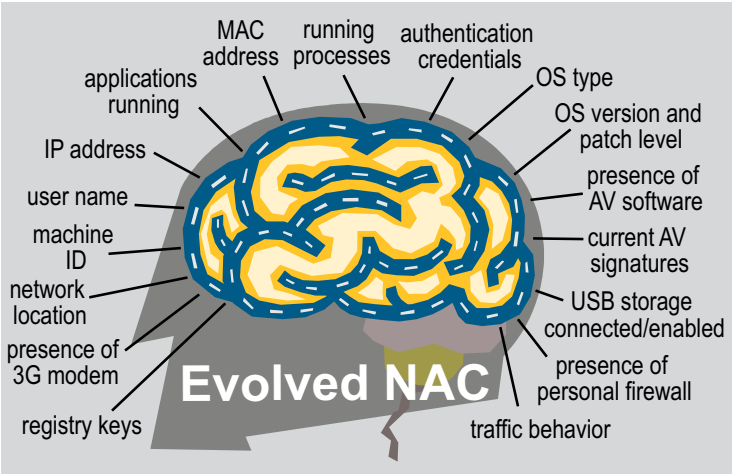
By JEFF WILSON, Principal Analyst, Security
Infonetics Research, Inc.
November 2009

Rich Knowledge Becomes Powerful Enforcement

What is network access control? The original concept of NAC, dating back to 2003, was to prevent the spread of malware by preventing infected computers from accessing the network. The original implementation of NAC was complex: you had to install new switching technologies (802.1x), fit endpoint computers with new supplicants and agents, and deploy servers dedicated to storing and managing access control policies. This original concept of NAC did not enjoy widespread adoption because the solution was judged to be more painful than the original problem, and many companies found it difficult to justify the investment.

The latest generation of NAC solutions is far more easily deployed than the first generation. Plus, today's leading-edge NAC solutions gather more data, provide more information, and fit more use cases. Advances in the intelligence of NAC solutions have transformed NAC from a simple tool for preventing the spread of malware to a rich source of knowledge and a powerful security policy enforcement engine.

NAC'S BIG BRAIN



Today's NAC solutions gather more data, provide more information, and fit more use cases

As a result, NAC has become an extremely useful tool for a wide range of security problems, including, but not limited to:

- Providing guest network access
- Controlling where employees and contractors can go on the network
- Enforcing security policy—antivirus, patch levels, applications, process, and registry files
- Generating endpoint compliance audit reports
- Remediating systems that are non-compliant
- Managing removable storage
- Providing visibility into who and what is on your network
- Preventing malicious activity

In the following pages we will review the forces that have driven NAC technology to its current state, and then we will explore each of the following domains to understand what information and control can be obtained from a state-of the-art NAC solution:

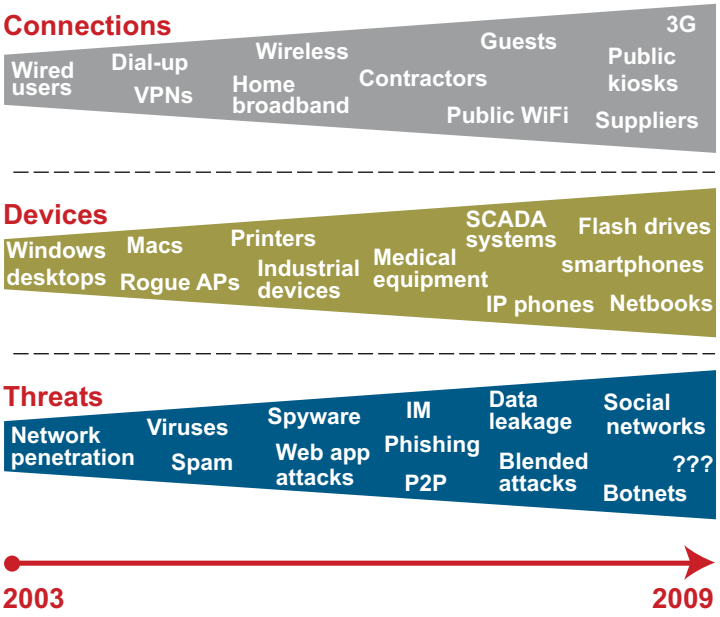
- Users
- Devices
- Software
- Peripherals

DRIVING FORCES BEHIND NAC'S EVOLUTION

NAC solutions didn't evolve in a vacuum; they evolved to meet huge changes in the IT landscape that have occurred since 2003. The changes, summarized in the diagram below, are the following:

- Explosive growth in the complexity of network connectivity—multiple technologies, multiple user types, multiple locations
- Increasing diversification and sophistication of endpoint devices
- Increasing (and mutating) threat environment

EVOLUTION DRIVERS



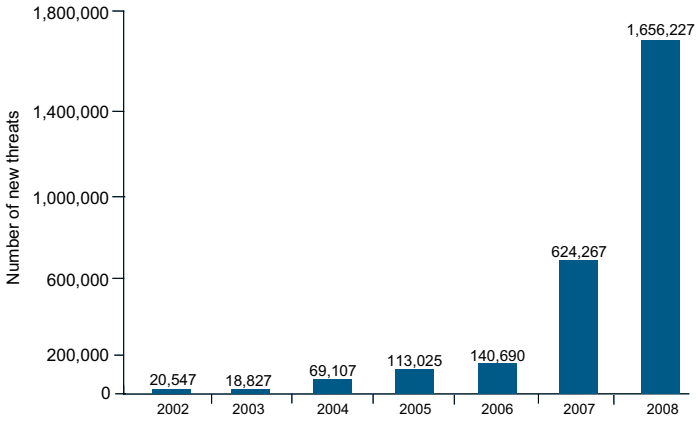
One example that combines the three drivers listed above is the now-common use of smartphones on corporate networks. In our March 2009 study User Plans for Smartphone Security, we interviewed 80 large companies (>1,000 employees) in North America about their plans to deploy security solutions for smartphones. Respondents are concerned about security on smartphones (particularly data loss and the use of removable storage), but only 52% plan to purchase client software specifically for the smartphones themselves; the rest rely on the smartphone OS to handle all security issues. The barriers to smartphone client security investment are telling: nearly 40% of respondents said there are simply too many device types and operating systems to control.

Networks must be open, and many networks include invisible, unmanaged, and unprotected devices like smartphones, which creates a significant demand for security solutions like NAC.

The chart below shows the number of malicious code threats detected in the wild from 2003 to 2008. The number of threats grew 60% from 2006 to 2007; by the end of 2008, 60% of all threats detected were first seen (and likely authored) in 2008. The rapid expansion of threats is a result of the transformation hacking has undergone since the turn of the millennium. Hacking is no longer a hobby, it's big business. Hacking enterprises have outfitted themselves with threat development toolkits and an army of code writers in the last two years. Given the accelerating pace of threat development, NAC solutions had to evolve to keep up. To deal with malicious code threats, NAC solutions had to expand the amount of data they mined about software running on a given device. Other threat vectors drove parallel evolutions.

The increasing threat environment as a driver for NAC's evolution is worth examining in more detail. The chart below shows the number of malicious code threats detected in the wild from 2003 to 2008.

NEW MALICIOUS CODE THREATS



Source: Symantec Corporation

Visionary NAC vendors have evolved NAC technology in response to the forces listed above. At the center of the evolution is the ability to gather a vast amount of knowledge about users, devices, networks, software, and peripherals, and store that data in powerful profiles. The data is useful, actionable, and auditable, and profiles organize the data so that security policies can be applied to individuals and groups. To truly understand what an evolved NAC solution can do, we need to look at each knowledge domain in detail.

KNOW YOUR NETWORK

Knowing what's connected to your network is difficult. As we've discussed already, the number and variety of devices connected to corporate networks has grown dramatically since the beginning of the NAC market, making it increasingly difficult for IT managers to maintain consistent security across all devices. If you were to ask CIOs how many devices are attached to their networks, they would have an answer, but it would likely be wrong. Inventory management tools and vulnerability scans help, but in many cases they provide periodic data and are therefore insensitive to real-time changes in the network.

Smartphones, as discussed above, are among the new types of devices confounding many IT organizations, but the problem goes far beyond smartphones. There are laptops at Starbucks, iPods on a user's home WiFi network, kiosks at the airport, network-connected manufacturing devices, point-of-sale terminals, medical devices, ATMs, IP phones, and rogue network elements (such as user-connected wireless routers).

First generation NAC solutions provide an incomplete picture of what's connected to the network. For example, Microsoft can help you figure out how many Windows systems are connected, but Microsoft tools are blind to printers, switches, routers, Macs, Linux, and many smartphones. NAC solutions that are based on 802.1x and switches can tell you about devices that have 802.1x agents installed on them, but they are blind to devices that don't have agents. Client-based solutions can gather a lot of data about the device the client is installed on but have no visibility into other devices.

Not only do you need to "see" everything on your network, but for true security, you need to "know" a lot about the devices. Evolved NAC solutions identify devices by:

- IP address
- Hostname
- MAC address
- Machine ID
- Traffic fingerprinting

This broad range of device identification methods allows evolved NAC solutions, especially out-of-band solutions that aren't tied to either 802.1x or a specific vendor's security client, to do the best job of seeing everything on the network. We talked to a security manager from a large hospital who recently installed an out-of-band evolved NAC solution. This hospital is subject to standard IT security issues as well as HIPAA regulations. The security manager we spoke with said that prior to installing NAC she was fairly certain there were about 8,000 devices connected to the network. She installed a modern out-of-band NAC appliance—one that did not rely on client software or 802.1X to perform inspection—and she quickly discovered that the hospital actually had 12,000 devices on the network. Even worse, many of the devices she didn't know about previously were devices with no security solution in place, most notably smartphones.

Her out-of-band NAC solution was able to discover all the devices (computers, printers, medical devices, smartphones, tablet PCs, etc.) in real time and keep track of changes, something that periodic scans for inventory and vulnerability purposes can't do. She was able to completely inventory her organization's network, then create profiles for a wide variety of device types that could be leveraged for management, control, and compliance. Device information is the foundation of profiles that evolved NAC solutions keep and leverage for the wide range of use cases they support.

KNOW YOUR APPLICATIONS AND OPERATING SYSTEMS

Security managers must know what applications are running on their networks. For some companies it's a matter of regulatory compliance, such as ensuring that peer-to-peer and instant messaging applications are not running. For others, it's a matter of basic security. Knowing what software is running on your devices is the key to:

- **Plugging vulnerabilities**: An OS that isn't patched may expose you to a serious vulnerability
- **Hardening defenses**: Making sure that antivirus software is running and up-to-date is key to making it a useful line of defense
- **Eliminating threats**: Identifying malicious software operating on a device is the first step containing malware

Many organizations have already deployed patch management and vulnerability assessment solutions to help keep endpoints secure. These systems work well for static environments and managed endpoints. But as we described above, the modern IT environment is characterized by rapid change, more ubiquitous connectivity, and an explosion in the number of unmanaged endpoints. In these environments, the standard patch management and vulnerability management solutions miss the mark.

There are thousands of stories about unauthorized applications in use on corporate networks around the world. In the absence of a state-of-the-art NAC solution, it would be very difficult for any organization to understand what their employees are installing themselves, or what hackers have managed to install through malware. On September 24, 2009, researchers at Damballa released the results of a three-month study of more than 600 botnets. Their research found that seven to nine percent of enterprise computers were bot-infected.

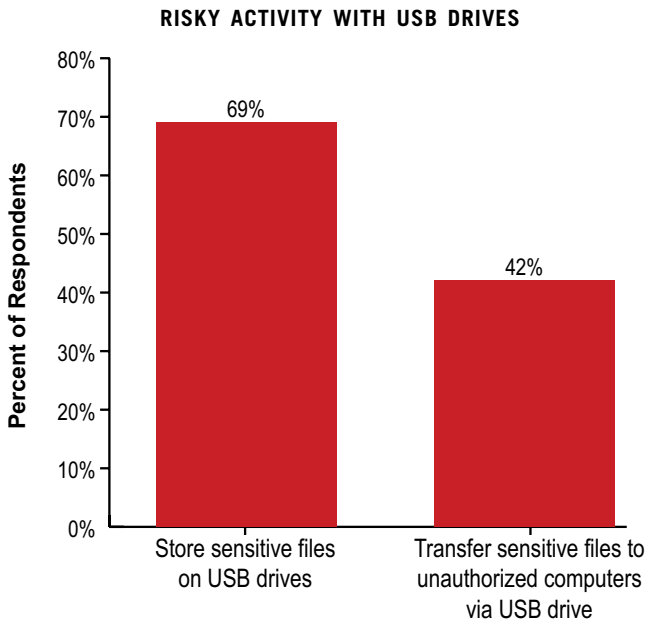
No enterprises willingly allow bot infections, but they happen nonetheless. An evolved NAC solution with a full inventory of connected devices and deep knowledge of the software running on those devices is an effective way to deal with bots and many other software-related threats. An evolved NAC solution can:

- Indentify which operating systems are on the network
- Inspect device registries
- Gather extensive information about applications running on the device
- Monitor patch levels of specific applications
- Check for AV updates
- Indentify active services
- Keep track of registry values

Software data is added to the profiles that started with device information, and these profiles become an even more powerful tool for device management, control, and compliance.

KNOW YOUR PERIPHERALS

Unmanaged or unknown peripherals can represent a significant threat to security. Take the case of USB flash drives, where stories of data loss are now well-etched into our memories. A recent study of 967 users at US companies by the Ponemon Institute found that many users engaged in potentially dangerous activities with USB drives, as shown in the chart below.



Source: Ponemon Institute

Another example of the threat posed by USB drives was seen in the way Conficker spread. The authors of the worm very cleverly altered the AutoPlay window that popped up when a USB device carrying Conficker was inserted. Some IT shops automatically disable the AutoPlay feature for USB devices. However, the Conficker authors got around this by re-arranging the AutoPlay options so that when the user clicked "open device to view files" they actually launched the executable and infected themselves with the worm. A nice bit of social engineering for sure.

But the problem extends beyond USB flash drives. Smartphones typically have microSD card slots, so they represent another opportunity for data egress. Webcams can present all kinds of problems. Printers are often much more than printers, especially when they are running their own operating system, which can be as vulnerable to hacking as a PC.

Many laptops now have 3G modems built in, or are outfitted with external 3G modems that present another type of peripheral threat. 3G modems represent another network connection that must be managed, and an evolved NAC solution knows that a user with a 3G modem is usually connected to the network twice. If access control rights must be removed from a user because they are fired or suspected of malicious activity, an evolved NAC solution that is aware of connected peripherals can remove standard network access rights (wired or wireless LAN) and simultaneously disable USB devices, killing the 3G wireless connection as well.

Current state-of-the-art NAC solutions can detect all of the peripheral devices mentioned above and allow management from a security perspective. Evolved NAC solutions detect USB mass storage devices, classify them, and can block them from connecting depending on your policy. Data about peripherals is added to the rapidly growing device profile that already contains a wealth of device (hardware) and software information, as discussed above.

KNOW YOUR USERS AND THEIR BEHAVIOR

All the information that NAC solutions gather about devices, software, and peripherals needs to be associated with the user using them. For a NAC solution, knowing the user means matching their authentication credentials with profile and policy information stored about them. What makes a NAC solution evolved, from a user point of view, is its ability to:

- Define and enforce roles for individual users or groups of users
- Help users modify their behavior relative to security

Many companies **define roles for their users** in very simple terms: "employee" and "guest" are very common. From an IT security and access control perspective, the employees category should be further subdivided (for example, engineers, finance accountants, salespeople, and research, or even multiple types of researchers working on separate projects). Evolved NAC solutions enforce group policies that have the capability to treat accountants different from researchers or even treat two researchers differently. For example, policies can be built to specify which types of devices each researcher is allowed to use, when and where they're allowed to connect, which applications they should or should not be running, and whether they're allowed to use removable storage devices or Web cams.

Companies looking to offer network guest access require similar flexibility and granularity when defining and enforcing access rules, because there are many types of guests. Is the guest a customer looking to use the Internet while on-site? A contractor working on-site for six months and accessing company data? Or an auditor who is on-site for a short time but needs deep access? The credentials granted and policies applied to these guests will be very different, and evolved NAC solutions are flexible enough, and have access to enough knowledge about the users and the devices they use, to handle these cases and more.

Defining and enforcing access roles in this granular and flexible way mitigates the threats that exist as a result of the proliferation of devices and connectivity discussed earlier.

When it comes to helping organizations **manage and modify user behavior** relative to security, there are no point solutions available. Acceptable user behavior is part of the written policy at most organizations, and some of today's NAC products can help remind end users of the policy once they have violated it. One NAC product we are aware of provides several options in this regard, from sending a notice to the user's manager, to requiring that the user click to confirm that he is aware that he has just violated a policy and that he has read the policy.

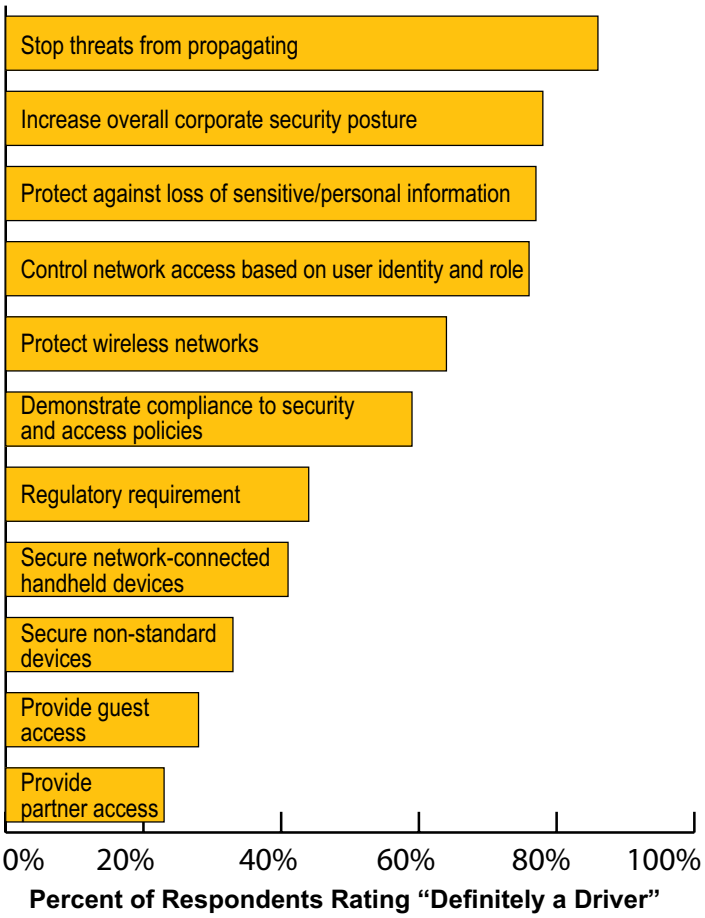
Evolved NAC solutions can use the wealth of information Evolved NAC solutions can use the wealth of information they gather to help modify user behavior. One small film company we spoke with was having an ongoing problem with a small group of users abusing P2P applications (and clogging up their valuable pipes). Their new NAC solution allowed them to solve the problem quickly without ever having to touch a single user's computer or change network configurations. The NAC solution let them see which users were causing the problem (it was a very small group), and upon launching the forbidden P2P application, the users were served up a Web page that directed them to their company policy about P2P apps, reminded them that ignoring company policy was grounds for firing, and forced them to click to acknowledge that they received the warning. The security administrator told us this technique achieved far better results than prior attempts to educate users through seminars and employee manuals. On-the-spot behavior modification, enforced by NAC, allowed them to educate the uneducated and warn the malicious.

SUMMARY

IT security managers are looking for new ways to monitor and control their IT environment. Traditional network security solutions—such as firewalls and intrusion prevention systems—provide no protection from insider attack. Similarly, traditional system security solutions—host-based agents for antivirus, patch management, and data loss prevention—don't address the threat from unmanaged systems that are increasingly finding their way onto enterprise networks. And unfortunately, the threat landscape has gone from bad to worse, as we have witnessed an explosion of new malware that has proven its ability to sneak onto enterprise networks through holes in the security fabric.

Modern NAC products are uniquely capable of dealing with the chaos of the modern IT infrastructure. NAC can protect networks against insider attack, and provide visibility and control over unmanaged systems. These capabilities are causing many IT managers to look to NAC solutions for a wide variety of use cases. In our June 2009 study of 160 medium and large organizations in North America, *User Plans for Network Access Control*, respondents stated loud and clear that there are many important drivers for NAC investment, as shown in the chart below.

DRIVERS FOR INVESTING IN NAC SOLUTIONS



Source: Infonetics Research, *User Plans for Network Access Control*, 2009

Very few respondents to our NAC user study had a single use case in mind. In fact, many of the drivers listed above encompass multiple use cases. While early NAC solutions could not solve all of these problems, many of today's highly evolved NAC solutions can.

For all of these reasons, we believe that enterprises will deploy network access control technologies at an accelerating rate. The concept of a network that can defend itself has been attractive for many enterprises, and evolved NAC solutions are the brains that can enable this. Modern NAC products provide a rich source of knowledge about the devices, users, peripherals, and applications on your network, and they include a powerful security policy enforcement engine that can deal with both managed and unmanaged devices. ■

INFONETICS RESEARCH

LEAD ANALYST/AUTHOR

Jeff Wilson, Principal Analyst, Network Security (Bio)

jeff@infonetics.com, +1 408.583.3337, twitter.com/securityjeff

With more than 14 years in the data networking and telecom industry and one of the most accurate forecast track records in the business, Jeff Wilson is a certifiable network security market guru. He has expertise in a wide variety of network security appliance, software, and services markets, including IPSec and SSL VPNs, firewalls, IDS/IPS, NAC, and content security (anti-x, mail security, Web security, data leak prevention). As principal analyst for security at Infonetics Research (www.infonetics.com), he covers the complex interactions between products, traditional managed services, and SaaS, and authors numerous network security market share and forecast reports, a series of end-user studies, and Continuous Research Service (CRS) research notes and surveys.

A major thought-leader in the network security space, Jeff is frequently quoted in trade and business publications, including *Business Week, Forbes, InformationWeek, Investor's Business Daily, InternetWeek, Light Reading, Network World,* and *The Wall Street Journal*, and writes columns for a variety of publications. He also speaks at industry events, moderates webinars, and is a highly sought consultant to startups, service providers, manufacturers, and the investment community, identifying market opportunities and offering advice on positioning, product development, business plans, and M&A activity. He is active in the financial community, educating VCs and investment bankers about new markets and technologies and performing due diligence for funding.

With Infonetics since its early garage days, Jeff helped build Infonetics' meticulous research methodologies and is a key driving force behind Infonetics' service development, with emphasis on exploring new and emerging markets.

Jeff graduated from the University of California, Berkeley in 1995 with a Bachelor of Arts in English.

SALES

Larry Howard, Vice President

larry@infonetics.com, tel: +1 408.583.3335 fax: +1 408.583.0031

Scott Coyne, Sr. Account Director - Eastern N. America, Europe, Middle East

scott@infonetics.com, tel: +1 408.583.3395 fax: +1 408.583.0031

ABOUT INFONETICS RESEARCH

Infonetics Research is an international market research and consulting firm serving the communications industry since 1990. A leader in defining and tracking emerging and established technologies in all world regions, Infonetics helps clients plan, strategize, and compete more effectively.

SERVICES

- Market Share, Market Size, and Forecasts
- Enterprise/SMB and Service Provider Survey Research
- Continuous Research Services
- Service Provider Capex and Subscriber Analysis and Forecasts
- Consulting, Retainers, and Quick Consults
- Webinar, Conference, and Event Speaking
- Custom Brand and Demand-Side Market Research
- Custom Market Size and Forecasts
- Technology and White Papers
- Competitive Analysis and Due Diligence

COVERAGE AREAS

- Mobile and Wireless
- FMC and Femtocell
- Mobile Backhaul and Microwave
- Service Provider VoIP and IMS
- Broadband
- IPTV and Video
- Next Gen OSS and Policy
- Services and Subscribers
- Service Provider Capex and Subscribers
- Carrier Routing, Switching and Ethernet
- Optical
- Data Center and Storage Networking
- Security
- Enterprise Networking
- Enterprise VoIP and Unified Communication
- Telecom and Datacom Equipment Totals