



## **Best Practices for Implementing NAC:**

Why Remediation is the Key to Maximizing NAC Capabilities

Even as financially-motivated and stealthy attackers probe their networks, many enterprises still depend on old-school IT security methods. They rely on traditional perimeter and host defenses that are easily evaded by these new-school professional hackers. These criminals know how to prey on perimeter weaknesses and as a result, they are having a field day with corporate resources.

According to Gartner, more than 75 percent of enterprises will be infected with undetected, targeted malware by the end of 2007. These are not fly-by-night organizations. These are businesses of all types, including those that are supposed to be the best in their class. And yet their security teams are still falling short.

A telling example comes by way of a Washington Post story in April 2007. According to security reporter Brian Krebs, the paper found evidence of multiple spam attacks coming from servers held by Fortune 500 companies such as Home Depot, ExxonMobile and Electronic Arts. Systems from these organizations were not only compromised, but were also being used as part of massive bot networks to further fuel the criminal hacker economy.

Today's threat landscape is filled with internal threats, adaptive malware and self-propagating attacks, making an entire network open to these kinds of compromises if even a single endpoint is infected.

It might be tempting for IT professionals to throw up their hands in defeat, but all hope is not lost. By implementing network access control (NAC) solutions into robust security infrastructures, enterprises can regain control of their networks to protect against those single points of failure. If deployed the right way, NAC can help organizations analyze security posture, inspect for policy compliance, fix security issues and provide greater visibility into endpoint compliance states.

But that is a big "if." Deployed in a vacuum, most NAC solutions are purely preventative—they simply deny network access to non-compliant or infected machines. Without some way to automate the remediation, these NAC solutions can actually cause more problems than they solve.

Because of this, organizations that plan on utilizing a NAC solution in the near future must consider not only how they will block at-risk systems from accessing the network, but also how they will remediate those risks and put systems back on the network.

"NAC is not this thing that you are going to just plop in and have it do it all," says Charles Kolodgy of IDC. "It needs to have an environment where people can really leverage their investment. That is what is important."

Kolodgy believes that eventually the perception around NAC will evolve to the point where it is known less as a single-point technology and more as the framework for a mature security program.

"NAC is in many ways an infrastructure," he explains. "In order to flesh out that infrastructure, security pros will need to also have other elements to complement the access control component that most people today consider to be NAC."

This includes traditional perimeter defenses, effective identity management and authentication tools and perhaps even network behavioral analysis and content filtering solutions.

Acting as the central nervous system to this entire infrastructure is a vulnerability scanning and remediation toolset that can proactively manage the risk profile of the organization's network devices and endpoints. Working together with the access control component, this remediation toolset can allow administrators to set the security baseline that their organizations are comfortable with and seamlessly enforce it.

In concert, these elements of the ideal "NAC infrastructure" should allow organizations to enable the right users to access only the information they need without risk of misconfigurations, infections or data leakage.

## Still new technology

It is clear that NAC solutions are poised to play a big role in the future of many IT security programs. According to a recent report by Infonetics Research, the NAC appliance market nearly quadrupled between 2005 and 2006 and it will likely double this year.

Unfortunately, the NAC market is also still in its infancy. This can pose some difficult problems for those looking to deploy immediately.

"NAC doesn't have any best practices right now," Kolodgy says. "Part of the issue is that NAC is an emerging technology. And things haven't been set as to what it includes and how to really interact with it."

With such explosive growth and a lack of standards within the different vendors' technologies, the NAC market is in a Wild West state of chaos. Vendors are shooting it out for the millions of dollars earmarked for NAC in the coming years. Meanwhile, analysts are still scrambling to sort out the information about the technologies in order to best advise the customers.

This state of disarray has left plenty of room for numerous debates about NAC as a technology. For example, one of the biggest NAC arguments raging at the moment has to do with where the solution should be placed in the architecture. Some solutions are placed in-line with network streams and others are designed to sit out-of-band.

IT administrators that get caught up in those kinds of debates as they determine which NAC technology to use may be missing the point, however. Though the means may differ, the ends are the same. The goal is to identify machines and users at risk and quarantine, essentially putting users "in jail" (usually through a protected VLAN) until the risks have been remediated.

"Most of the industry debate on NAC has focused on the different jailing methodologies or technologies," says Matt Mosher of PatchLink Corporation. "But that is just one part of a NAC solution, how do you put my users in jail. The real questions should be how do you keep my use out of jail, and what level of policy inspection and remediation can you provide? These last two points will determine the success of your NAC implementation and answer two

question How will my users be impacted by NAC and can the solution inspect and remediate all elements of security policy?"

## Avoiding the Black Hole

This problem of remediation is the key pain point faced by early adopters who have deployed NAC without some sort of vulnerability remediation solution at hand.

"With NAC, you're often put in the situation where due to a vulnerability problem you put somebody in to a quarantine VLAN and you create what I call the black hole problem," says George Owoc, director of business administration for EADS Astrium North America. "You've quarantined somebody, now what are you going to do? They're stuck."

In order to avoid this black hole problem, administrators need an easy and seamless way to fix the problems identified and allow the user back onto the network with as little inconvenience as possible.

Which is why those such as Owoc treat the NAC enforcement solution not as a single miracle cure, but instead as a critical element to an overall network access control architecture. Using NAC in concert with vulnerability remediation technology allows administrators to ensure that user access is controlled, all of the critical inspection points are working to enforce policy compliance, and that exposed or infected systems are not only denied access, but are also fixed so that it can get back on the network.

Doing so can not only prevent inefficiencies and slowdowns for the users, but it can also prevent the types of political gaffes that have made many in IT wary of NAC quarantining for some time now.

"The person who is going to get stuck in quarantine isn't going to be somebody unimportant. He's going to be somebody politically important," Owoc says. "It's going to be the CEO who just went on a trip overseas and he's picked up some virus over there on his computer and he's in quarantine and he's screaming bloody murder. It's not good for the career."

## Leveraging assets

While most NAC vendors position themselves as providing the overall solution to both quarantine and remediation capabilities, few actually offer the full framework for access control without working with partners that offer automated vulnerability remediation.

"No one company is going to deliver the whole package," Kolodgy says. "It has to be done throughout the security environment. The need for NAC is great, but the key here is using your existing security infrastructure, which includes patching, vulnerability remediation and authentication."

Even the rare few vendors that do offer some sort of remediation technology often do so with the caveat that users must make considerable network and security infrastructure changes in order to deploy. This simply is not a possibility for most organizations.

"You definitely don't want to rip and replace," Kolodgy says, emphasizing that many organizations should find ways to integrate current technology investments into future plans.

This means not only leveraging existing security tools, but also working with the network as it is already designed. Re-architecting the network simply for NAC will rarely pay dividends.

If the components for a fully-functioning NAC infrastructure are not already in place, it also may mean an additional investment to truly get a return on investment on the single point access control solution that NAC vendors currently sell. Especially important is finding a vulnerability assessment and remediation tool that can integrate with current NAC offerings to act as the “brains” behind the operation.

Integrated vulnerability scanning and remediation will give better control over the granularity of policies and provide more flexibility to determine what risks be remediated before users are allowed on the network.

## Five Phases to NAC

In order to make the right decision when choosing a NAC product on which to hang the rest of this access control framework, it is critical to ask how potential vendors approach vulnerability remediation. Rather than getting caught up in minutiae such as in-line or out-of-band placement, buyers should take a closer look at how well the product plays with vulnerability remediation tools and how easy it is for blocked users to get back onto the network.

Creating a network access control architecture that leverages vulnerability remediation tools can make all the difference in a NAC deployment. Ideally, successful NAC architectures should be able to control access through a five-phased program that encompasses the full NAC lifecycle.

### **BASELINE**

First, start by defining an acceptable security baseline. Set policies that ensure that endpoints attempting to connect to the network will meet baseline standards. This can include policies for up-to-date patches, software configuration and antivirus signatures.

SCAN. Next, endpoints will need to be analyzed against those established policies before the user authenticates. They'll be checked for both compliance and for potential malware infection. This scanning phase should be the most frequent action of the five, providing constant updates to the risk profiles of all elements of the network, including endpoints, routers, switches and the like.

### **QUARANTINE**

Systems that are not compliant or that are infected should be blocked from gaining access to network resources.

### **REMEDiate**

Systems should only briefly need to be “put in jail.” The infrastructure needs to be able to automatically update and scrub quarantined systems according to baseline policies.

### **AUTHORIZE ACCESS**

Once the endpoint meets the baseline, it should be admitted to view network resources based on the access level of the user. Ideally, users should also

confirm their identities with some form of strong authentication before final access is granted.

Together, these five phases should be nearly transparent to the user. The goal is to provide a balance of security and convenience. Without that, administrators might just have to field that dreaded call from a less-than-thrilled executive.

## Case Study

A lean and mean operation, Astrium specializes in designing components for NASA space shuttles. Based in Houston, the 23-person organization is a wholly-owned subsidiary of the European Aeronautic Defence and Space Company (EADS).

Though his organization is small, George Owoc faces many unique network security problems. As a contractor with NASA, Astrium must comply with stringent national security mandates that restrict foreign access to information regarding space shuttle technology. Because the company frequently hosts visiting executives and contractors from Europe, it must have a way to allow them to access network resources while restricting access to the sensitive information they are not allowed to see. In addition to these users, Astrium also works closely with on-site contractors and interns. Similarly, these users need to be segmented.

Owoc chose to use Lockdown Networks Enforcer appliance to help accomplish a high level of access control. He uses Lockdown's NAC solution in concert with PatchLink Update to ensure that infected or non-compliant systems are quickly remediated with minimal interruption and no action needed on his part.

"People sometimes say, 'You're such a small company, why do you need this stuff?'" Owoc says. "I say it's because I'm a small company that I need it. I don't have a team of people whose sole job is to worry about evaluating the latest reports from SANS. If I can look at that stuff once a month, I'm lucky."

Owoc says that he particularly likes the way that Lockdown integrates with PatchLink by deferring to PatchLink to determine whether or not a system has been remediated to an acceptable level before access is granted.

"You add that granularity of control by using PatchLink baselines. That means you don't have to be absolutely perfect, because a lot of times there are vulnerabilities that are not high risk or acceptable in certain environments," he says. "My objective is not to be as perfect as possible in implementation, but to have a user-friendly implementation. One that creates minimal impact on my users, minimum work for me, but still accomplishes the job."



PatchLink Corporation  
15880 N. Greenway-Hayden Loop, Suite 100  
Scottsdale, AZ 85260  
480.970.1025

[www.patchlink.com](http://www.patchlink.com)