



Are Your Users Smarter Than A Fifth Grader? (Article published on enterprisenetworksandservers.com, March 31, 2008)

By Gord Boyce, President, ForeScout Technologies

The question has been thrown around asking how smart are we as adults compared to what our children are learning in school. While this has made for some humorous television, I believe the concept also holds true for IT security professional. But instead of having to worry about being outsmarted by an elementary school student, you are required to always be on the offensive against threats, in the form of trusted users, which create security risks to your network.

Do you know who is on your network? Do you know what they are doing? Do you know what they are accessing? Network Access Control (NAC) has enjoyed significant attention from the CIO and IT security professionals for the past several years, but many are still asking "what's the value of adding this new layer of network security?" The question is valid, but the world of network security is rapidly changing and some of the old notions of how to protect the network need to be challenged. The threat landscape has evolved with a marked shift from kids trying to gain notoriety by launching the next great network worm or virus to highly skilled, highly organized groups trained to exploit users for financial gain. Their goal is not to take down the network, but rather to extract any data that could lead to a possible financial payday. And the main target is not bypassing your hardened security perimeter, but rather to gain access to the network through valid users: Your users.

This seems ominous. I know what you're thinking: "my own users?" Yes, your users. They are the target, but they may never know it, and they also may not know that their online behavior could have a significant cost to the company.

So the question, "Are Your Users Smarter Than A 5th Grader?" must be answered. How smart are your users? More specifically, how much security smarts do they have? Do they know how to avoid online threats or are they susceptible to tricks and tactics that could allow your network to be compromised?

The unfortunate reality is that your users typically are not going to go out of their way to ensure that the network or even their device is secure. Most users will not proactively download the latest security patch or update their antivirus software. So you, the Administrator, have put systems in place to push patches and automatically make sure your users' security software is up to date. But even with this, there are still users who are not in compliance with the established network security policies.

So it becomes the job of the seasoned network security practitioner to figure out a way to ensure that trusted users do not become the threat; to ensure their systems are protected to limit the chance of their device being exploited and used as a backdoor into the system. If users are not going to go out of their way to help you do your job, then you need to employ technology to address this "insider threat".

Teaching Users to Be Secure

I'm not sure if teaching users to behave can ever be truly accomplished. Inevitably, you will have users who do things that do not exhibit a high level of intelligence. They will give away their secure login and password to phishing schemes, they will let their kids download files onto their corporate laptops, and they will click on email attachments promising to show pictures of the latest Hollywood starlet's fall from grace. You can only do so much to curb these types of behavior, but there is hope. There are ways to use NAC to help shape the way users behave. Just like a teacher dealing with 10-year-olds, you need to be able to switch between June Cleaver and Nurse Diesel (if you're not familiar with Nurse Diesel of Mel Brooks' High Anxiety fame, you have my admiration...and jealousy), between hand-holding and hand-slapping.

The goal of network security is to protect the network from threats while not getting in the way of business. Often, when network security measures are increased, there is a direct impact on user productivity. Non-compliant users are blocked from doing their job due to some level of policy infraction. Often this is due to their systems being identified as vulnerable to attack, but not actually posing an immediate threat. This not only impacts the user, but ultimately business.

(CONTINUED)



ForeScout Technologies, Inc.
10001 N. De Anza Blvd. Suite 220
Cupertino, CA 95014, USA

T: 1.866.377.8771
F: 1.408.213.2283
Online at: www.forescout.com

NETWORK ACCESS. CONTROLLED.™

Using NAC to Shape User Behavior

NAC can be a lot of things, but at its most basic level, it is policy-based technology that governs who has access to what and for how long. NAC is built to ensure that when users attempt to access the network, they are compliant with specific network security policies and remain in compliance while connected. NAC exists to ensure that users do not become a threat to the network.

So how can you use NAC to shape a user's behavior? It starts at the policy level. You must first know what it is you need to enforce. Armed with the knowledge, you need to find a tool that provides you with the flexibility to be either June Cleaver or Nurse Diesel. Let me give you an example of both.

The June Cleaver approach to NAC:

A user who has been away from the network for several weeks returns to the office. After making the obligatory rounds to say hello, the user settles behind the desk and plugs in the laptop. This device has seen a lot of miles in the last two weeks and has been exposed to several hotel and coffee shop networks. During this same period, there was a major patch update and several antivirus updates. All of these were missed. Upon logging into the network, the NAC system identifies the device as belonging to a trusted user and begins to interrogate the system. It correctly identifies the policy violations present on the device. The NAC device initiates a browser redirect and displays a message on the user's screen letting them know that the device is not in compliance with corporate network security policies, that remediation is underway, and that the user can proceed with work while this process occurs. Transparent to the user, the NAC system has kicked off the patch management system to bring the device back into compliance. The NAC system monitors the device until it is in full compliance.

User's response: "Golly Mrs. Cleaver, I had no idea that these were issues. Thanks for helping me fix it."

The Nurse Diesel approach to NAC:

An inside user is attempting to gain unauthorized access to resources where sensitive information is stored. Unbeknownst to the user, when they logged into the network, the NAC system associated their identity (Active Directory Group) and device. A policy was in place for this user's organizational group. This policy directed the NAC device to establish a virtual network segment in which the user was only allowed to have access to role specific resources. When the user attempted to access the unauthorized resource, the NAC system took a more "disciplinary" approach. In this case, the user received a browser redirect to a screen addressing them personally and stating that "access has been denied and due to this unauthorized attempt to access sensitive resources an email notification has been sent to HR and their immediate supervisor informing them of the security violation." Behind the scenes, the NAC system has automatically blocked the access attempt, logged the security event and alerted the appropriate parties.

User's response: "Ouch! I never knew a virtual spanking could hurt so much. Do I still have a job?"

Ideally, a NAC solution would offer you both options and a whole lot of variations in between. Enforcement is the key to gaining true business value out of a NAC solution. You must be able to enforce policies in a way that promotes business productivity while giving you a full range of options to accurately pair the enforcement response with the exact level of policy violation. This specifically means blending the two approaches above. You need to be able "June Cleaver" users when appropriate, or, if things get out of control, you need to be able to crank up the "Nurse Diesel" response. Ultimately, these responses and all of the variations in between are critical to ensuring that users do not pose a threat to the network.

What to look for in a NAC Solution?

Shaping the way users behave is a big job and requires some specific functionality from a NAC tool in order to get the job done. When evaluating a NAC solution, you should look for the following criteria:

Clientless Device Detection – Knowing what is on your network is essential to creating and enforcing appropriate policies. The NAC tool should be able to discover all devices on or entering your network without any prior knowledge of the device. This detection ensures that you have full visibility into your network and provides you with the ability to do real-time compliance checks ensuring that all devices in the network are compliant with your network security policies.

Granular Policy Creation – Look for a NAC solution that gives you the ability to customize the policies to your specific environment. Instead of asking, "does the product enforce X policies", ask "will the tool allow me to create policies to solve X business challenge." This puts the focus where it should be – on business challenges you want to solve.

Full Range of Enforcement Options – Being able to enforce the policies created is where the company experiences the business value of NAC, but it is also the aspect that creates the most fear. That is why it is essential to look for a tool that provides you with numerous enforcement options to allow you to match the level of enforcement to the exact degree of policy violation. You should also find a tool that provides you with the ability to build-in policy exceptions ensuring that your boss and the CEO never get "NAC'd" off the network.

Ease of Deployment/Ease of use – NAC should not take man years off your life when using man hours to roll out the technology. If the NAC solution requires you to do significant re-architecting of your network, asks you to roll out software to all devices, or will only work within a vendor specific infrastructure – keep looking.

Integration with Existing Systems – NAC should not be just another security tool, but should enable the orchestration of policy response. The NAC system should integrate with existing systems (remediation, patch management, trouble ticketing, vulnerability scanning, etc.), automating their use in response to network security policies. This extracts additional value out of existing systems protecting your current investments.

Real-time Threat Prevention – Ensuring that a device is in compliance with network security policies and that the user is only allowed to have access to appropriate resources is critical for NAC, but what happens if all of this is covered and the user's device becomes infected. This is why it is absolutely essential that NAC include the ability to detect and mitigate self-propagating threats instantly.

Reporting – It is essential to know what has happened in order to shape policy and account for security events. You need to be able to extract this information in order to understand exactly what is going on within your infrastructure. Not to mention the numerous regulatory compliance initiatives (PCI, SOX, HIPAA, etc) requiring reporting on security events and remediation actions.

Above All, Experience

Now that I have spent some time highlighting what you should look for in a NAC offering, I would like to offer one more word of advice. Find a NAC solution that has been deployed in a significant way. Ask the vendor for reference customers from other organizations of similar size and network complexity. This will quickly sort out which companies have hands-on knowledge in successfully rolling out network access control policies and turning on enforcement.

So we go back to the question of how smart are your users. With the right NAC solution in place, you can say with confidence that they are in the process of growing up and that you are helping shape their online behavior. And when they get out of line, you have already put the mechanisms in place to ensure the safety of the network. With NAC in place and policies in enforcement mode, you can have assurance that your network access is controlled.