A technical exploration of why NAC is failing

White Paper

Catching the Unicorn

There are a variety of reasons NAC has failed in its quest to become a mainstream technology. This white paper reveals why NAC will not succeed as a niche market. It's an exploration of the technical intricacies of current network access control technologies, why they're failing and an explanation of how vendors, the industry and consumers can make it successful in the next eighteen months.

First Release
2009-09-18

Special Thanks

I'd like to extend a special thank you to several people who have contributed directly or indirectly to this piece. In no particular order: Alan Shimel for his inadvertent contribution to the title, Chris Tobkin for his insight, Dave Minella for his editing skills, Michael Santarcangelo for his extensive review and assistance in clarifying points, Mike Fratto for several tidbits of vendor details and data, Vik Phatak who helped with several iterations of clean up. In the anonymous list, another Chris, a Greg and another Dave; thank you all!

Catching the Unicorn

A technical exploration of why NAC is failing and how to redefine the technology for success

There are a variety of reasons NAC has failed in its quest to become a mainstream technology. This white paper reveals why NAC will not succeed as a niche market. It's an exploration of the technical intricacies of current network access control technologies, why they're failing and an explanation of how vendors, the industry and consumers can make it successful in the next eighteen months.

Jennifer Jabbusch
Carolina Advanced Digital, Inc.
http://cadinc.com
http://SecurityUncorked.com

Executive Summary

Network access control (NAC) solutions have been failing as a technology in the IT security market, a truth punctuated by numerous NAC vendors closing their doors and an abundance of failed implementations in the past two years. The failure of NAC is detrimental to manufacturers of the technology, integrators offering the solutions and most importantly, to the countless organizations with security challenges that NAC will solve.

This document provides a unique perspective into the NAC market and a comprehensive dive into the technical difficulties that are inhibiting NAC technologies from seeing widespread adoption. Beyond explaining the issues of NAC adoption, this effort reveals a detailed plan to remedy the current situation – with explicit calls to action for manufacturers, consumers and the industry as a whole.

Catching the Unicorn is vendor neutral and presents issues from several angles, making it relevant to all NAC vendors and those interested in NAC technologies.

Included in the first two sections are background information and a brief overview of the technology market as it relates to NAC. This information lays the foundation for understanding the larger underlying issues that need to be addressed for the market to be successful. In the third section *Mapping NAC Functions*, basic concepts of the feature component set of NAC are identified and explained. Part four *Reducing Cost and Complexity for Widespread Adoption* begins the exploration f primary technical complications of NAC and outlines ways to streamline each feature component as a means to simplify the solutions enough for widespread adoption. Throughout the paper, several key concepts of security, network security and access security around which NAC was developed are discussed. Part five concludes with specific recommendations for vendors and consumers alike on what must happen to turn NAC into a viable solution.

Key findings

- NAC will not succeed as a niche market.
- NAC will be a feature set, not a product.
- Much confusion of NAC stems from ambiguous terminology, a result of NAC's evolution from other products.
- The hindrances in adoption of NAC are due to technical challenges.
- There are four feature components of NAC: Authentication, Access Rights, Endpoint Integrity and Behavior Monitoring.
- There are frameworks and standards in place that will help NAC reach widespread adoption.

Key recommendations

- Vendors should focus on standards of interoperability in order to succeed.
- NAC solutions should be renamed, based on the feature components they offer.
- Consumers of NAC technology must demand standards and roadmaps from vendors.

Table of Contents

Executive Summary **5**

Table of Contents **6**

I. Background **8**

History of the Topic 8

Defining the Unicorn 8

II. Introduction to the NAC Market **10**

Market Analysis & Strategy 10

Technology Adoption Lifecycle 10

Where NAC is now 10

Holding NAC Back 11

NAC is Not a Niche 12

Standards to Cross the Chasm 12

Integration, Adoption and Perception 13

III. Mapping NAC Functions **14**

Tackling NAC Terminology 14

The four feature components of NAC 14

Access Management versus Threat Management 17

Mapping the Relationships 18

Using the mapping to reduce complexity 18

IV. Reducing Cost & Complexity for Widespread Adoption **19**

Moving to Tornado 19

Revisiting the Technology Adoption Lifecycle 19

Cleaning up each of the four components 19

1. Cleaning up Authentication 20

a. Leverage current network logins 20

b. Move to 802.1AR (Device ID) under 802.1X-REV instead of MAC-Auth 21

c. Drop Authentication completely by registering devices only and monitoring behavior 21

d. Increase universal interoperability of 802.1X 21

e. Create centralized management for 802.1X enforcement points 22

f. Increase support and features outlined in IEEE 802.1X 22

g. Use behavior analysis and monitoring only 22

2. Cleaning up Access Rights 23

a. Simplify network segmentation with 802.1X-REV Network Advertisements 23

b. Redesign VLAN use, provisioning and mapping 23
c. Make use of firewalls inside the network 24
d. Offer an on/off only solution 24
e. Secure with a safe instead of a moat 24
f. Use behavior analysis to track communication on the network 24
3. Cleaning up Endpoint Integrity 25
a. Scrap agent-based endpoint integrity for managed endpoints 25
b. Simplify and broaden endpoint integrity rules 25
c. Use built-in agents for endpoint integrity testing 25
d. Monitor behavior instead of implementing endpoint integrity checks 26
e. Use standards and frameworks for endpoint integrity enforcement 26
f. Use firewalls or application-aware devices to stop undesirable activity 26
4. Cleaning up Behavior Monitoring 27
a. Integrate frameworks for reporting (such as TNC IF-MAP) 27
b. Use switches and infrastructure tools already in place 27
c. Use firewalls/IDS devices internally to investigate signature-based attacks 28
d. Use centralized log management and visualization to track trends 28
V. Moving Forward 29
How the industry is cleaning up NAC 29
Bringing accountability to vendors 29
Inciting customers to demand more 29
Renaming NAC 30
VI. About the Author 31
About Carolina Advanced Digital, Inc. 31
Contact 31
Appendix A: Index 32
Appendix B: Terminology 33
Appendix C: Resources 35

I. Background

Professionally, I've been focusing on network access control technologies for a couple of years. After working with a variety of vendor solutions, I reached the conclusion that network access control technologies were too complicated to be successful. Their finicky nature, cost and complexity have doomed NAC solutions as we know them now. About a year ago, I gave up on the technology and refocused my efforts to other areas of infrastructure security.

There was one problem with my decision; customers still wanted NAC. I ended up with an assortment of customers in high risk environments that really *needed* the features that NAC solutions could provide. The only solution was to turn our attention back to NAC and find a way to make it work.

History of the Topic

For more than a year, I've been discussing this topic and many of the contents of this white paper with various members of the network security industry; colleagues, partners, vendors, integrators and consumers of the technology. Over the past several months, I've been able to pull together the thoughts into a complete collection. *Catching the Unicorn* is a technical exploration of why network access control (NAC) technologies are failing and how we can redefine the technology and terminology to make it successful.

Don't be put off by the name. In the next section, *Defining the Unicorn*, you'll understand that the title has an important hidden meaning, crucial to getting the point across.

Although I've had this document prepared since the beginning of 2009, the contents of this white paper have only been presented in its entirety once, to a small group attending the Security B-Sides Conference in Las Vegas during Black Hat USA 2009. I have reservations about discussing this topic, as it may alienate me from, or frustrate, several partners in my professional life who are actively pursuing their spot in the NAC market. Reservations aside, I decided to (as we say here in the South) git'r done and tell it like it is. And so, it's all here for you now, in black and white.

If you're not familiar with me, my blog, my company or my backdrop, please see the About the Author section at the end for more information about my background and experience with these technologies.

Defining the Unicorn

Security professionals today like to throw around "unicorns" and "rainbows" along with "clouds" and other snazzy words. The title of this white paper was actually inspired by a comment made by Alan Shimel of StillSecure while I was speaking at a panel on NAC during INTEROP Las Vegas earlier this year. "Boy, this guy just wants unicorns and rainbows all around," he said in response to an audience member who wondered "Why can't [all the vendors] just get along?" From that comment the title was created, but it has a much deeper meaning.

I'll present this to you as I did to the Security B-Sides Conference attendees. Let's play a little game of Spot the Unicorn. I presented the attendees with a series of unicorn images and asked them to identify which of the following images is a real unicorn. Let's see if you get it right.

Unicorn 1	Unicorn 2	Unicorn 3
		
Unicorn 4	**Unicorn 5**	**Unicorn 6**
		(Specimen 6 was too fast to capture on camera)

We have five unicorn images above. If you had to pick one (and just one) that most closely represented your idea of a unicorn, which would you choose; Unicorn 1, 2, 3, 4 or 5?

Before you keep reading, really look and think about it. I have my reasons, just hang with me here. Which unicorn is really a unicorn? Your hint is that there is one correct answer.

You're probably looking at Unicorns 1 and 5. You've ruled out Unicorn 3 because he has wings and is thus a Pegasus. You've probably ruled out Unicorn 2 because it looks like a malformed goat and you're probably trying to figure out if Unicorn 4 is a Unicorn or a dog-deer creature of the middle ages.

*A **unicorn** (from Latin unus 'one' and cornu 'horn') is a mythological creature. Though the modern popular image of the unicorn is sometimes that of a horse differing only in the horn on its forehead… the traditional unicorn also has a Billy-goat beard, a lion's tail, and cloven hooves—these distinguish it from a horse.*

Working with the above definition of a unicorn, our candidate Unicorn 2 is actually the correct answer. Yes, our strange Billy-goat-esque buddy up there is THE unicorn. One could argue with the definition, the history, the logic or the images, but that's what we're going with.

You're wondering how exactly unicorns are relevant in network security. Well, NAC is our unicorn of the day. It's a mostly misunderstood and misinterpreted technology that has no clear widely-accepted definition in the industry. My unicorn might be number 2, yours might be number 5 and because it's a mythological creature, there's no definitive source or a scientific and verifiable definition from which to work. I told you it would be relevant.

II. Introduction to the NAC Market

One of my theories in networking, and IT in general, is that we (as technologists) get too caught up in the gadgets, gizmos and check boxes of our world, often to the detriment of understanding the overall business goals. We find ourselves too involved in the minutia of daily tasks that we fail to see the big picture and forget WHY we're implementing all these technologies.

Market Analysis & Strategy

Even if this feels rudimentary or irrelevant to you, this section has purpose: it sets the foundation for how to successfully address this issue. Solving this dilemma requires grounding in the challenges of the technology from these different perspectives.

Technology Adoption Lifecycle

Technology vendors all establish their place in the technology adoption lifecycle. Depending on the business model, some direct attention to the earlier stages of the lifecycle and maintain solutions in the Innovators valley. These companies put more R&D into proprietary solutions and innovative technologies that meet a specific need, but may never see widespread adoption. Other vendors choose to target a larger market; those companies aim for the green areas of the curve, seeking widespread adoption with possibly more basic offerings.

Whatever the focus may be, not every vendor has goals of mainstream adoption for all technologies. Many solutions find their niche in the Innovators valley and succeed there, addressing specific needs for customers. NAC, however, has a feature set above and beyond what a single point solution can provide, and for this reason NAC will not succeed as a niche solution that lives in the innovation basin.

Most technologists implementing products will never see or think about this curve, but it dictates much of our lives in the world of IT. The technology adoption lifecycle concept and diagrams used here are from *Crossing the Chasm*, by Geoffrey A. Moore which uses a variation of the original technology adoption lifecycle created by Beal, Rogers and Bohlen.

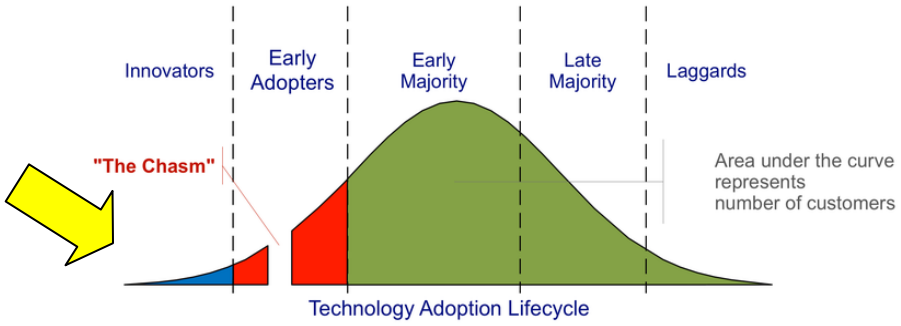


Figure 1 from "Crossing the Chasm"

Where NAC is now

NAC has been unable to progress past the "Innovators" and "Early Adopters" stages of the lifecycle curve. In fact, it hasn't even really approached the chasm. Perhaps this *is* the chasm that NAC has hit and hasn't been able to cross. Regardless of its exact position in the adoption curve, it's clear NAC technologies and vendors are trapped in the blue and red areas in the lowest valleys of the lifecycle.

If NAC were a *niche*, the technology could succeed in the Innovators and Early Adopters sections of the curve; but NAC is not a niche. This will be explained in the next section.

This raises two key questions: What's holding NAC back, and how are these obstacles overcome to achieve widespread adoption of the technology?

Holding NAC Back

NAC has failed to successfully jump the chasm and gain widespread adoption, not for lack of trying or marketing, but due solely to two technical reasons.

First, the technology is too difficult to integrate in heterogeneous environments. In fact, NAC is difficult to integrate even in a completely homogenous environment of a single switch vendor and standardized operating systems. The running joke among engineers is that NAC installs require three experts, two special moon alignments and a Latin chant. Far from plug and play, the technology changes faster than consumers can evaluate and implement. Since NAC is not a niche, enterprises resort to a variety of less complicated ways to meet their needs.

Secondly, the larger industry fosters a melting pot of NAC terminology that has no meaning. One term means one thing to Vendor A and another to Vendor B while a second term may not actually have a meaning at all; perhaps Vendor C's marketing department made up that *feature*. How can consumers responsibly evaluate, compare and discuss technology that has no formalized definition? What do decisions makers do when they are confused and feel unable to select a solution? Nothing. They do nothing – which is a pivotal part of why NAC is failing.

SIDEBAR | A brief background on the birth of NAC

The confusion in features and terms stems largely from the fact that NAC solutions have grown as an offshoot from different vendors' set of competencies. Switch and wireless vendors incorporated NAC-like functions to their hardware. Remote access and SSL-VPN vendors tweaked host evaluation rules, turning them inward facing to scan LAN devices. Software vendors with heavy agents on endpoints leveraged that integration for self-enforced NAC.

Cisco led the way of NAC with their Network Admission Control technologies. Over the following years, they were followed closely by other security vendors wanting to stake their claim in the NAC market. **Juniper** grew their NAC solution (the Infranet Controller) from their SSL-VPN platform. Obviously **Symantec**, **McAfee** and other software vendors tweaked their endpoint security software agents to provide NAC-like security. **HP ProCurve** and **Enterasys** took advantage of their switch platforms in conjunction with various centralized management software to provide NAC functions. **ForeScout** used technology from their ActiveScout product for controlling worms and malicious traffic on the network. **StillSecure** is one of the few vendors with a purpose-built NAC platform already capitalizing on a variety of partners and technologies to support their solution. **Bradford** has another widely-adopted NAC-like solution they've recently relabeled Adaptive Network Security. There have been a few other purpose-built solutions that have already risen and fallen in just a few short years. Mentioning these niche companies is fruitless, since I expect their times are all short lived, and they'll likely be out of business by the time you read this paper. The failed companies have generally banked on NAC as a niche product, many of them in the form of in line appliances. In the next sections, I'll explain why all these models are failing and why they will continue to if the model doesn't change.

NAC is Not a Niche

NAC is not a niche. NAC, regardless of the feature set and definition, is a solution that involves a diverse set of components in the network. Regardless of the implementation, NAC involves several disparate systems in the network. At a minimum NAC includes: the devices that want access, the devices through which those are connecting, and the devices making the decision to allow or deny that access. In the most basis configuration those devices would be a laptop, a switch and a server.

The fact that the solution consists of many integrated components means that a single purpose-built piece of hardware (or software) will never be the answer. **NAC will not be a product; it will be a set of features.**

The set of features an organization is seeking will determine the components involved and the underlying management product(s) selected. A single NAC product will not, in any environment, scale or grow to a level acceptable for widespread adoption. At the moment, the solutions are too difficult to implement and there are other alternatives that give organizations many of the features NAC can offer without the hassle involved with implementing NAC.

I predict that every niche vendor with a NAC product on the market will dissolve or rename that product in 18 to 24 months. Why? NAC is not a niche and NAC will not be a single product; any company with a business model that doesn't take that into consideration will fold or be forced to refocus. Switch vendors are great at making layer 2 and layer 3 devices. Software vendors are great at making agents. Switch vendors don't need to be designing and pushing software agents to endpoints, and software vendors shouldn't be mucking around in the hardware enforcement space. Failures in the NAC market are discussed more in upcoming sections.

Success in the NAC market will come to vendors who focus on their core competencies and work for greater integration with other vendor's products for a full-featured solution.

Standards to Cross the Chasm

Standards; you may love the word, you may hate it, but the truth is standards run the world of technology. Standards are what let us operate and interoperate both locally and remotely and at layer 1 and layer 7. Without standards, we're doomed.

Standards continue to emerge and grow in every aspect of technology. Over the years, wireless NICs moved from 3rd party external devices with external drivers to something built in to most operating systems. Organizations such as the Wi-Fi Alliance came together as a framework for developing wireless in a time when there was not yet a standard. We must have standards and NAC is no exception.

SIDEBAR | Standards and frameworks to watch

Currently, the frameworks from organizations such as Trusted Computing Group's Trusted Network Connect are the strongest and most widely adopted by vendors. The exception is Cisco, which has made a commitment to adopt the IETF NEA standards when they are put into place. On the wire side, the IEEE 802.1X standards for port security will dictate layer 2 port securities in most NAC installs.

Integration, Adoption and Perception

The current public perception of the NAC market is pretty dismal. Although vendors of the technology spin surveys and data to make it appear more appealing and more widely adopted, the truth is NAC is too hard, too expensive and too unmanageable to maintain in its current state.

Organizations interested in adding NAC to the network are apprehensive about the technology as they watch vendor after vendor close its doors. In early NAC acquisitions between 2004 and 2007, **Cisco** bought **Perfigo**, **Check Point** bought **Zone Labs**, **Symantec** bought **Sygate**, and **Sophos** bought **Endforce**. Most recently, managed security provider **Trustwave** bought out startup **Mirage Networks** to incorporate NAC in MSP offerings. These buyouts left a handful of niche NAC vendors that have been steadily falling by the wayside. The most recent victim, **Consentry Networks**, closed its doors just weeks ago, in August of 2009. Consentry's failure was preceded by several others; **Lockdown Networks** closed shop in March 2008, **Caymas Networks** in March 2007. **Vernier Networks** was renamed to Autonomic Networks in September of 2007 and dropped NAC all together. **Nortel's** NAC offering is tied up in a bankruptcy proceeding; it's future is unknown.

Most of these failed NAC vendors relied on proprietary solutions, in line devices and drop-in appliances designed for easy implementation. The trouble with their approach is that they treated NAC as a niche market and tried solving the problem with niche products.

Customers have two options; they can invest in these expensive appliance-based solutions, or face the impossible task of integrating NAC frameworks in their heterogeneous networks. Neither option is appetizing, but the prospect on an enterprise investing huge sums in a technology and a company that may not be around in ten months is extremely unpleasant and it’s another reason niche solutions *won’t* succeed and those built on standards and frameworks *will* succeed.

The industry will move forward as soon as vendors and consumers of NAC technologies accept that NAC is not a niche. **Vendors** playing in the NAC space must embrace standards and refocus R&D efforts on integration instead of product development alone. **Consumers** of the technology must adopt the concepts of standards-based integration and demand it from their vendors. Without this shift in consumer behavior, vendors have no motivation to change their ways.

III. Mapping NAC Functions

This section will clarify terminology by defining four feature components of NAC, used for describing and comparing various NAC solutions, and explore how these pieces fit together and overlap. That data will be used to map out the relationship of the four components and give a more clear understanding of which are interrelated, which are interdependent and which are completely independent.

Tackling NAC Terminology

One of the leading challenges in discussing NAC is tackling the terminology. Instead of referring to vendor terms or the random acronyms and naming convention used in the NAC frameworks, I propose using plan English verbiage from my *Universal NAC Feature Model*[1], which describes the four feature components of network access control systems. This can be used to map concepts to their vendor- or framework-specific counterparts.

SIDEBAR | Popular NAC Terms

There are a few terms in NAC that are used correspondingly from vendor to vendor and framework to framework. Worth mentioning is Layer 2 versus Layer 3 NAC. Layer 2 versus Layer 3 NAC: Layer 2 NAC will refer to a network access solution using IEEE 802.1X (a layer 2 standard) for port security in infrastructure devices. Using Layer 2 NAC gives organizations protection at the port level and offers a way to secure access on physically unsecured edge ports. For more information on 802.1X, visit www.SecurityUncorked.com and use keyword 802.1X. Layer 3 NAC refers to solutions that bypass layer 2 security, issue an IP address to the device under NAC control and then control its access using layer 3 standards, such as ACLs in switches or firewalls. Layer 2 is the more secure of the solutions but is often much more difficult to implement.

The four feature components of NAC

At first consideration, many colleagues don't agree with my breakdown of the four feature components. However, after explaining the theory behind each one, they usually are in agreement by the end of the conversation. If you ask most professionals and vendors, they'll each tell you NAC has two or three (not four) components.

Some components are interdependent, while others remain independent. I've arranged them in the most logical order I can, with the understanding that they are not necessarily in a specific order of chronology or dependency.

The four feature components of NAC are: **Authentication**, **Access Rights**, **Endpoint Integrity** and **Behavior Monitoring.**

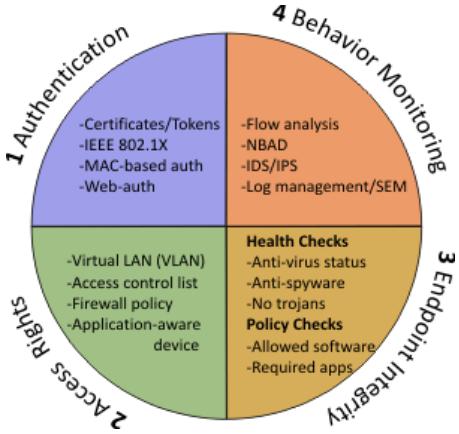


Figure 2 Four feature components

[1] The Universal NAC Feature Model is a proprietary documented model by Carolina Advanced Digital, Inc. and is not presented here in its entirety. In addition to describing feature sets, the model describes methods of authentication, enforcement, implementation and reporting.

1. Authentication

Who or what are you?

The first of the four components, authentication is much broader than it may initially appear. Authentication frequently refers to user authentication, where a person submits credentials (such as username and password) to be verified. Authentication in NAC could also mean device authentication using certificates, or even more generally, it could mean device *identification*, by way of MAC address.

Certain processes of authentication are actually only identification by virtue of the fact that nothing is in place to validate or verify that the device is who or what it says it is. A MAC address can be easily spoofed, and systems using MAC addresses for access are really only identifying the system, not authenticating it. For our purposes here though, identification will be described as a type of authentication.

2. Access Rights

Where are you allowed to go?

Access rights dictate what resources a user or device on the network can access. Again, the term is broad since access rights can be dependent on a variety of variables and enforced by an assortment of methods.

Frequently, organizations apply access rights via role-based VLANs (virtual LANs), user-based resource access or location- and time-based rules that dictate who can access what resources when. Access rights may be dependent on such things as:

- User type or role (user group membership)
- Access location (geographic)
- Access method (direct via LAN, remote access/VPN or wireless)
- Device posture (whether the device is healthy and compliant)
- Date and time (standard business hours use or after-hours access)
- Combinations of any of the above

Access rights may be enforced by VLANs, access control lists, firewall policies, layer 7 application-aware devices, self-enforcing software agents and other means.

> **SIDEBAR | Access Rights in Today's Products**
>
> Due to the speedy and virulent growth of products meant to address access rights management, several vendors have ended up with cobbled solutions built of disparate components that trample on one another. You may find several vendors with product overlap that leads to conflicting access rights rules. For example, the vendor may have a solution that enforces at the switch level and another that makes another judgment and enforcement at the application level. Even if the products are from the same vendor, if they were not designed to talk and confer with one another for decision making, you can end up with contradictory decisions and unpredictable results.

3. Endpoint Integrity

What is the current condition of the device?

To most consumers of the technology, endpoint integrity *is* NAC. The correlation is odd, since the vast majority of organizations looking at NAC are *not* looking at it to satisfy endpoint integrity needs.

Endpoint integrity is an evaluation of the endpoint, or device connecting to the network, on several criteria. These endpoint evaluations fall under two primary categories: health-based endpoint integrity checks and policy-based endpoint integrity checks.

Health-based endpoint integrity checks evaluate the device for potential security risks directly related to its health posture. These tests would include checking for up-to-date anti-virus definitions, the presence of anti-spyware, any matches on known virus signatures and so on. If the endpoint appears to be infected with malicious code or is a likely candidate to become infected, it should not pass an organization's health checks.

Policy-based endpoint integrity checks, on the other hand, evaluate an endpoint's posture against allowed configurations in the corporate policy. These policies may address acceptable use or compliance issues and restrict the use of, or access to, resources and applications which may be harmful to the organization indirectly. Examples of common policy-based checks may be to disallow the use of peer-to-peer software or instant messaging.

The upcoming section on *Access Management versus Threat Management* explores how the four components of NAC and the two sub-components of endpoint integrity fit in the access versus threat model.

> **SIDEBAR | Why People Consider NAC**
>
> Only a small percentage of those seeking NAC solutions are looking for endpoint integrity. Based on a variety of surveys from print and online media (and my observations and discussions), port access security and guest access management are among the two highest-ranking features of interest. Endpoint integrity isn't even a close third in most races.
>
> Many organizations may choose to implement a NAC solution or NAC like features with other feature components and reduce cost and complexity by omitting endpoint integrity all together.

4. Behavior Monitoring

Are you behaving strangely on the network?

Discussing behavior analysis as a component of NAC is where the most eyebrows get raised. It's imperative that we include it in the list since a handful of current vendors essentially have entire NAC solutions built around behavior analysis, and I believe it will become a more significant piece of NAC solutions of the future.

Behavior monitoring (or analysis), like other feature components, can be attained through a variety of means. It may happen in the form of flow analysis (from technologies such as sFlow and NetFlow) that samples traffic on the network, it may happen by other network behavior anomaly detection (NBAD) methods or even by monitoring from an IDS or IPS device that's trained to match behavior against a baseline of expected network traffic. In certain cases, log management and security event management (SEM) can provide various levels of anomaly detection as well. In the most extreme cases, behavior monitoring may include a component that identifies and interacts with malicious traffic, such as answering reconnaissance and scanning applications.

Behavior analysis, in whatever form it materializes, will usually identify both malicious behavior (attacks, ping sweeps, failed login attempts) as well as potentially harmless but unusual actions on the network (traffic over strange ports, or two devices talking that don't usually communicate).

SIDEBAR | Behavior Monitoring and NAC in Education

Many educational institutions use NAC solutions that leverage behavior analysis. Especially in higher education, the IT staff of the school has no right (or desire) to install and manage traditional heavy NAC agents on laptops owned by students and faculty. In an environment where there are thousands or tens of thousands of endpoints with a variety of operating systems and configurations, managing endpoint software would be a nightmare. Instead of using preventative systems with heavy agents to monitor endpoint posture, these systems take a slightly more reactive approach by continuously monitoring the network and connected devices for anomalous behavior. If a device is misbehaving, it's knocked off the network or isolated until it can be examined.

Access Management versus Threat Management

The concepts of NAC are really meant to address access management, threat management or a combination of both. Access management controls who gets on the network and what resources they have access to once they're connected. Of the four feature components, access management generally encompasses Authentication and Access Rights as well as some aspects of Endpoint Integrity.

Threat management addresses direct security liabilities on the network such as protection against viruses, malware and other malicious attacks or activity to or from a device. Of the four feature components, threat management includes most Endpoint Integrity checks and Behavior Monitoring.

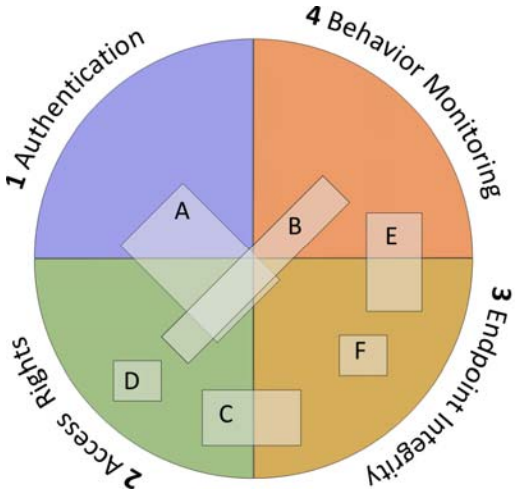
We can apply the access management versus threat management model to a variety of security technologies outside the scope of NAC.

Access Management		Threat Management	
Authentication	Access Rights	Endpoint Integrity	Behavior Monitoring
-Certificates/Tokens -IEEE 802.1X user auth -MAC-based auth -Web-auth	-Virtual LAN (VLAN) -Access control list -Firewall policy -Application-aware device	**Health Checks** -Anti-virus status -Anti-spyware -No trojans **Policy Checks** -Allowed software -Required apps	-Flow analysis -NBAD -IDS/IPS -Log management/SEM

Table 1 Access management vs threat management

Mapping the Relationships

If we map the relationship of the four feature components using key building blocks of NAC functions, we see most functions are connected to, or situated around, the Access Rights quadrant of the circle. We can redraw the relationship mapping quadrant diagram and show the interrelations in a different format for clarification.



Relationship Mapping
A) User or device identification
B) Traffic flow and analysis
C) Resources to be secured
D) User or device rules
E) Policies for health compliance
F) Applications on endpoint
...

Figure 3 Feature quadrant mapping

The relationship mapping shows us what areas of the feature components customers should focus on (or omit) based on features they're most interested in. We can also see which dependencies can be dropped while still achieving other pieces of the solution.

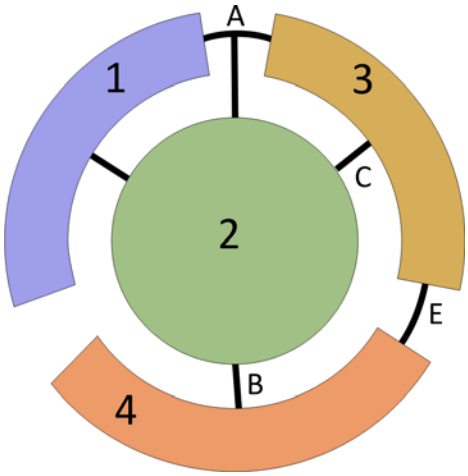


Figure 4 Feature nucleus mapping

Using the mapping to reduce complexity

Parts of a solution may be dependent on other pieces. For example, we can't have granular Access Rights (green 2) without the appropriate level of Authentication (blue 1). Frequently our Endpoint Integrity rules (gold 3) are also based on Access Rights (green 2), which, as we just noted, generally depend on Authentication (blue 1).

We'll see next, in section IV *Reducing Cost and Complexity,* how we can safely omit certain pieces of the relationship to simplify the overall solution. Mapping the features, functions, components and interdependencies

for each solution or customer environment will give you great insight into the design and a deeper understanding of where you can safely pare down.

IV. Reducing Cost & Complexity for Widespread Adoption

With vendor integration and standards, we can offer the feature sets consumers are seeking while reducing cost and complexity in NAC to help catapult it up the technology adoption curve and make it a viable solution. For a vendor to maintain a technology, it has be profitable enough to sustain continued R&D efforts. NAC just isn't there yet, which is why it's caught in this horrible cycle of failing NAC products and vendors. The technology isn't easy enough, so it's not being widely implemented, and because it's not widely implemented, the vendors don't have the sales to warrant more R&D to make it easier. Catch 22.

Moving to Tornado

Revisiting the Technology Adoption Lifecycle

If we take a look at a more detailed version of the technology adoption lifecycle we can visualize what we're shooting for: the blue and green areas. If you're reading a black printout, we want to move into the upswing of the curve where we see the bowling alley and tornado.

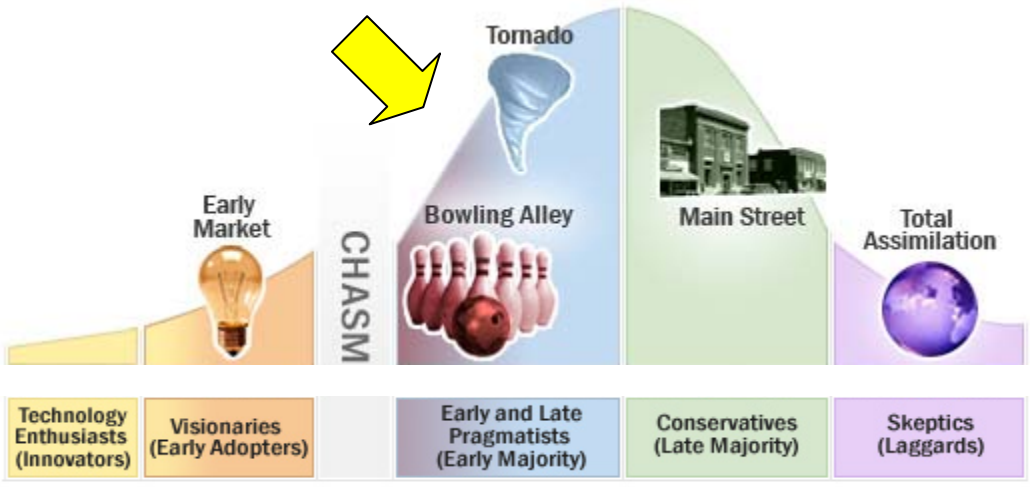


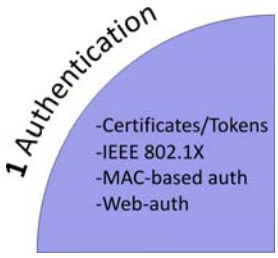
Figure 5: New Technology Adoption Lifecycle from the Chasm Institute

Cleaning up each of the four components

To get the most out of the following sections, I'm preserving the format used earlier and presenting each solution set by feature component: **Authentication**, **Access Rights**, **Endpoint Integrity** and **Behavior Monitoring**. Outlined are a variety of ways to streamline or evolve each component for an overall reduced cost and complexity. Some recommendations involve upcoming standards; others are things we can start working on today.

Several concepts presented here contain technical components and apply concepts that may not be familiar to non-technical readers. Explanations are included to assist in explaining key concepts. For further information, please see the terminology appendix or research the resources provided.

1. Cleaning up Authentication



Authentication is one of the most critical clean-up spots. Although some of the feature components can work independently, many times they rely on authentication before further decisions can be made or enforced.

For example, how can you impose Access Rights to a user if you don't know who the user is? Even if you're not distinguishing one authenticated user from another on the network, you're likely distinguishing authenticated uses from guest users (you certainly should be if you're not). The same holds true of some Endpoint Integrity policies. Perhaps corporate executives are allowed a grace period for remediation before their laptop is quarantined. Again, we can't make that decision or apply those rules if we can't identify the person logging in.

Right now, our two principal methods of Authentication are **IEEE 802.1X** and **MAC address-based** authentication. Other methods are either rarely used or are not standard. The problem is we have two extremes – two opposite ends of the security/complexity spectrum. On the one hand, **MAC address-based** authentication is extremely easy to implement, but inarguably exceptionally insecure. A trip to Walmart and $10 are all you need to spoof MAC addresses. On the opposite end we **have IEEE 802.1X**, which is incredibly secure but remarkably difficult to implement.

> **SIDEBAR | The Issues with IEEE 802.1X**
>
> I love 802.1X. In fact, I even have a shirt proclaiming my love of it. The truth is it's ridiculously difficult to get it up and running. IEEE 802.1X offers port-based security on switches by allowing the switch to talk to RADIUS and authentication servers to decide who should or should not get access to the network. The switch enforces the decision returned from the server and implements any additional commands passed back such as a VLAN assignment. Integrated systems of switches, servers and endpoint devices are exceedingly difficult to get going in the first place. Once they're up and running, they're just as difficult to maintain since even the most minor change in any of the components can disrupt the delicate ecosystem. In reality, even a firmware upgrade on a switch or an OS patch could break the communication chain and force reconfiguration of the system.

a. Leverage current network logins

If we could achieve secure logins without implementing 802.1X to pass credentials back and forth from switches to servers, we could greatly simplify the authentication component. What this would mean is finding another way to package and send user or device credentials to the network.

There are some proprietary systems that offer a bastardized version of this, often sniffing traffic not intended for them to listen for successful domain logins. Personally, I have a problem with anything that's making a decision based on data *overheard* and not intended for a specific system's consumption. Although any long-lived solution would need to be standards based, not proprietary, this might be a stepping stone in the right direction. Ideally, the authenticating system would be in planned two-way communication with the enforcement device(s) of the NAC system, whether that's software or a piece of hardware or switch.

Result: If we can leverage another authentication system (domain login or single sign on) instead of using 802.1X to pass credentials to the NAC enforcement point, we can greatly reduce the complexity of NAC. Direct cost would be comparable.

b. Move to 802.1AR (Device ID) under 802.1X-REV instead of MAC-Auth

Unique device identification is coming in the next iteration of the IEEE 802.1X standard. This new device ID leverages public key infrastructure to produce cryptographically unique hardware device IDs that are not easily spoofed like current MAC address based authentication. This unique device ID would provide ease of MAC-based authentication with a level of security equivalent to a certificate infrastructure.

Result: A genuinely unique and un-spoof-able device identification solution could reduce the complexity of authentication by allowing organizations to immediately and securely identify and authenticate a connecting device without user interaction or complex configuration of 802.1X.

c. Drop Authentication completely by registering devices only and monitoring behavior

Several of the current NAC solutions employ systems that white list devices (usually by MAC address) then black list that device and disallow network access if a behavior monitoring system deems it a threat.

White listing devices can be automated with the help of purpose-built software, as can the communication to the behavior monitoring solution(s). Currently, these types of systems are generally making use of proprietary communications; however the frameworks and standards for NAC have recently incorporated pieces that would allow for standards-based communication between NAC devices and a host of other security devices on the network.

Result: Dropping Authentication has obvious rewards in reducing cost and complexity. Security may be sacrificed, making it not ideal for some organizations. Registering devices can be tedious, but the cost and management overhead is still usually much lower than fully authenticated systems.

> **SIDEBAR | More on the TCG/TNC IF-MAP Framework**
>
> The Trusted Computing Group's Trusted Network Connect framework for NAC communications has recently announced the use of IF-MAP for inter-device communications which allow network security devices such as firewalls, IDS and IPS to communicate with NAC management systems and feed information that will aid in the decision-making processes of a device's posture. Large companies, including Boeing, are using IF-MAP in production now to meet a host of specific needs.

d. Increase universal interoperability of 802.1X

The industry moved from external NICs and drivers to a fully capable plug-and-play platform, 802.1X components must be more widely integrated and universally interoperable. We've initiated the movement toward this goal in the way of recent operating systems having built-in 802.1X supplicants (or agents). Also, most network devices, including switches and access points, have some level of support for 802.1X authentication. When the level of support is alike across the board from vendor to vendor and product to product, we'll see a much easier implementation in the way of authentication.

Result: By demanding universal support and interoperability of 802.1X in endpoints, operating systems and hardware, we'll force the standards and framework groups (such as IEEE, IETF and TNC) to continue working on more robust standards.

e. Create centralized management for 802.1X enforcement points

Many of the organizations looking at NAC really only need or want the features of port based security that 802.1X can deliver. Even for the organizations that do want more, there are no real central management tools for pushing 802.1X configurations to hardware devices (switches and wireless access points).

Some vendors offer tools in their management console to help with 802.1X configurations on switches and APs, but they're usually extremely limited at best, and I have yet to see a single solid product that can manage a variety of manufacturers – something that can configure 802.1X on Cisco, HP ProCurve, Extreme and other brands.

Result: With a centralized management tool for 802.1X switch configurations, the complexity and time resources to initiate and manage a NAC or 802.1X project are decreased drastically.

f. Increase support and features outlined in IEEE 802.1X

Consumers of the technology and vendors should be demanding more coverage of the IEEE 802.1X standard. While I feel the new 802.1X-Revision (due out late 2009 or early 2010) will resolve many of the issues we have with the current standard, we were left hanging for many years with a standard that wasn't quite up to snuff from a real-world integration perspective.

We have needs and uses cases for 802.1X that are not addressed and specified in the current standard version. What happens, then, is that these uses cases not outlined in the standard are handled on a case-by-case basis by the manufacturers; one switch might handle situation Y this way, and another might do something completely different. The response even varies from firmware to firmware on the same switch model. The result is a completely erratic set of results from the devices and unreliable behavior.

Result: By beefing up the standards used in NAC authentication, their behavior is more stable and therefore, more likely to be viewed as a reliable and scalable solution in an enterprise. If standard uses cases are not supported, the perception that it's *not ready for prime time* will dissolve any interest in rolling out the solution.

> **SIDEBAR | Off-standard uses cases for 802.1X**
>
> Some examples of uses cases not addressed by the current standard include mixed-device authentication, frequently seen in VoIP environments where a computer is daisychained behind a phone. It's very common for the computers in an environment to authenticate using 802.1X while legacy VoIP phones need to use MAC address-based authentication. In addition to mixed authentication types, even standard multiple device authentication using the same protocol can sometimes yield unreliable results, as can null VLAN assignments returned from RADIUS servers during authentication.

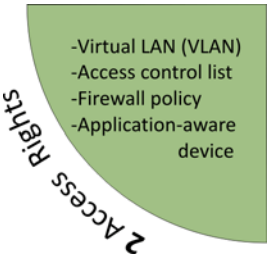
g. Use behavior analysis and monitoring only

We can completely cut authentication from the NAC solution as long as we have some means in place to monitor behavior and control access rights if a device is a rogue or behaving badly. Many organizations use authentication for (if nothing else) the peace of mind in knowing everything on the network at least has a body attached to it that's authorized to be accessing resources. There are ways we can employ granular monitoring with behavior analysis and access rights management to identify new and unauthorized devices and manage their access.

Result: If we omit authentication altogether, that feature component is obviously simplified, but the resulting work on the back end will add its own complications.

2. Cleaning up Access Rights

Access Rights, like Authentication, is another feature component that will benefit greatly from the new revision of the IEEE 802.1X standard (802.1X-REV). The new functions possible with 802.1X-REV will simplify traffic segmentation and communications, even with multiple devices on connected to the same physical port. What this means is that these use cases we have with computers daisy chained through VoIP phones (and similar scenarios) will be much easier to support without the hassles of traditional 802.1X.



SIDEBAR | About the Upcoming 802.1X-REV

The IEEE working group for 802.1X decided to re-open the standard for a full revision, hence the references to 802.1X-REV, which is the revision in progress at the moment. When it's complete it will be labeled with the year it was passed as a standard, ie 802.1X-2010.

The new revision will incorporate new features including a Secure Device Identification (802.1AR) that will likely take the place of less secure MAC address-based identification. 802.1X-REV will also integrate the MACsec encryption (802.1AE) as well as the key exchange protocol for MACsec (802.1af). The integration of the MACsec into 802.1X will provide a platform to segregate and secure device traffic from multiple devices on a single port, thereby allowing a new concept of Network Advertisements, which work similarly to wireless SSIDs, allowing users to select to which network they wish to connect.

a. Simplify network segmentation with 802.1X-REV Network Advertisements

At present, the only way to serve multiple network access types from a single port (or even across multiple ports) is to use per-port settings for VLANs and/or manual IP addressing on the connected devices and control access using ACLs. Some vendors offer proprietary solutions with in-line devices, but from a standard solution, this is what we're forced to do currently.

With the IEEE 802.1X-REV of 2009/2010, the standard includes a feature called network advertisements, which works similarly to wireless SSIDs, letting a connecting user select the network type or segment they wish to connect to. And like wireless, each network advertised on the port may have a different level of security attached, meaning different authentication method and/or encryption. With this configuration, we would not be limited to serving one untagged (access) VLAN and multiple tagged VLANs.

Result: Using network advertisements in the environment will allow organizations to serve multiple types of networks from a single port, thereby simplifying common tasks such as guest access and VoIP environments. This both increases security and reduces complexity.

b. Redesign VLAN use, provisioning and mapping

The majority of organizations employing VLANs in the network today are using them to secure management traffic, to segment geographically and to break up networks in areas for DMZ or routing on the WAN. There are some organizations using VLANs for role-based access rights, but the vast majority haven't made it this far.

Result: If we can rework our thinking of VLAN use and set aside the resources needed to redesign our existing networks, we can clean up layers 1 through 3 and have a more solid base on which to build Access Rights. With role-based VLANs already in place, using port-based security technologies (such as 802.1X) to provision Access Rights will be much less complicated.

c. Make use of firewalls inside the network

Firewalls provisioned smartly in a LAN can offer cleaner points of segmentation and definition of Access Rights. If they're placed well, an internal firewall can reduce the tediousness of ACLs in switches and routers, thereby eliminating decision points in the network.

In certain environments, internal firewalls are cost prohibitive, due to the costs associated with high-throughput filtering devices. However, most organizations will see a favorable ROI when they take into account the management overhead of maintaining multiple access control devices throughout a network.

Result: Removing additional decision points in the network (such as ACLs on switches) and tidying up network segmentation with internal firewalls can greatly reduce the complexity of Access Rights. In addition, simplifying the system also reinforces security by reducing the chances of rogue routes, mis-configured ACLs and misdirected traffic.

d. Offer an on/off only solution

This is exactly what most organizations with any type of basic Access Rights are doing; providing an *on/off, yes/no, black/white* access to the network. If you authenticate, you're put on the production network; if you don't, you're placed in a segment that has guest access or no access. It's certainly not the most secure option, but it's better than nothing and proves a great starting point.

Result: Designing a very binary *on/off* Access Rights solution undoubtedly reduces both cost and complexity in NAC.

e. Secure with a safe instead of a moat

In security we frequently talk about the *moat* versus the *safe* model in protection. A *safe,* here, meaning a secure lockable box used for securing objects or resources. If you think about it quite literally, we can either build a moat around the network to restrict access or we can put our valuable data in a safe, lock it up and put in place Access Rights only to that specific resource. Most organizations use a mixture of moat- and safe-like technologies to secure network resources.

Result: If we scrap network-based Access Rights and put controls in place immediately in front of the protected resource, we can greatly reduce the complexity of Access Rights. You see this method implemented today in application firewalls, document management systems and various types of servers.

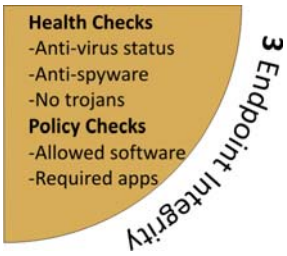
f. Use behavior analysis to track communication on the network

Another way to reduce complex Access Rights configurations is to take the previously-mentioned *on-off* scenario one step further by tracking access behavior. With this type of behavior monitoring, we're not looking for malicious traffic or attacks; instead we're keeping an eye out for traffic paths that are outside the normal patterns.

In this case, we might use flow analysis (with sFlow or NetFlow) or firewall logging to see which users or devices are unexpectedly accessing sensitive servers or segments of the network.

Result: This type of solution would be reactive (versus preventative) but would afford an IT staff more time to review and research traffic and make decisions about Access Rights management. By not enforcing rules real-time, we can reduce the complexity of configuring Access Rights.

3. Cleaning up Endpoint Integrity



Endpoint Integrity is peddled as the *meat* of most NAC solutions. It's what most peoples' minds first jump to when you say "NAC," With that in mind, let's look at some of the ways we can reduce cost and complexity within Endpoint Integrity.

a. Scrap agent-based endpoint integrity for managed endpoints

Most consumers seeking Endpoint Integrity features are checking for a few basic things; operating system and application patches, antivirus definitions and host firewall settings.

Organizations with robust directory services, patch management and anti-virus consoles can frequently enforce these common Endpoint Integrity rules on endpoints without intervention from a NAC management device. In cases where they cannot enforce Endpoint Integrity, they can usually at least inventory and report on the status of the endpoint, including what applications and versions are loaded and running.

Result: Leveraging the resources we already have in the network for Endpoint Integrity checks can give us the same or a similar level of security. By removing the requirement for Endpoint Integrity features in a NAC solution, we also remove the necessity of expensive endpoint agents. Omitting Endpoint Integrity agents that have to be deployed to each endpoint greatly reduces the intricacy of the NAC solution as well as the expense, since agent licenses are frequently the big ticket items in a solution.

b. Simplify and broaden endpoint integrity rules

Occasionally, network managers get a little power crazed when they first take over the controls in a NAC solution. Suddenly they have unwieldy power over the entire network including all connecting devices. The control can be good, but often the network security team will put in place Endpoint Integrity policies that are entirely too restrictive. Policies that are too specific are counterproductive, limiting access to devices that should be allowed, or becoming out of date in a short amount of time. Either way, the management overhead associated with specific Endpoint Integrity rules is huge.

As an example, a reasonable Endpoint Integrity rule might say devices on the production network must have antivirus installed and definitions no more than one week old. In most organizations with managed endpoints, we could even say devices on the production network must have Vendor X installed, because that's what we put on all company-owned laptops. A policy that is too restrictive and would be outgrown might read any devices on the production network must have Vendor X, Version AB.2 installed. When the next version of Vendor X's software comes out, you'll have to rewrite your policies. In addition, there may be endpoints in the environment with operating systems that don't support specifically Vendor X, Version AB.2; maybe two dozen devices have to stay on Vendor X, Version AA.1 for some reason.

Result: We can broaden Endpoint Integrity rules to be a little more forgiving without sacrificing security. Simplified Endpoint Integrity rules reduce costs in management overhead and time resources to manage and maintain the system.

c. Use built-in agents for endpoint integrity testing

One way to ease Endpoint Integrity pains is to leverage built-in testing and reporting agents, such as those provided in the Microsoft NAP infrastructure. Built-in agents might not be as robust out of the box as purchased agent licenses, but they meet most needs and offer extensibility with third party plug-ins. The Microsoft NAP solution is surprisingly easy to set up and would be a good candidate for any Windows environment. Some (non-Microsoft) NAC solutions can integrate with Microsoft NAP and use reports from the

NAP agent to make policy decisions. This type of integration will continue to grow as we see the frameworks and standards develop.

Result: Using an Endpoint Integrity agent (such as Microsoft NAP agent) already built in to the endpoint reduces both cost and complexity in a NAC implementation. We omit the need to push out and manage additional agents on the devices and we greatly reduce the solution cost since, as I mentioned earlier, Endpoint Integrity agent licenses are commonly the most expensive piece of the solution.

d. Monitor behavior instead of implementing endpoint integrity checks

A different approach to cleaning up Endpoint Integrity might be to exclude it completely from the NAC solution. Like other recommendations, this one is unquestionably more reactive than preventative, but still effective.

If we completely omit Endpoint Integrity checking on the endpoints using preventative methods, we can turn to behavior monitoring to fill in the gap. Behavior Monitoring (more on that topic next) watches endpoints and traffic patterns for abnormal or anomalous behavior patterns then takes action or reports to a management console for further investigation. Again, many educational organizations use this type of a solution to avoid messy configurations for Authentication and agents.

Result: Skipping Endpoint Integrity checks completely and relying on reactive monitoring relieves an assortment of headaches when designing a NAC solution. We omit the need to purchase Endpoint Integrity agents, manage and update policies and maintain the agents once they're installed. Cost and complexity of NAC are both significantly decreased when we go this route.

e. Use standards and frameworks for endpoint integrity enforcement

Standards and frameworks are vital because no solutions in this market will succeed without solid standards around which to design the products. Microsoft NAP in conjunction with TNC's framework is a great example of integration in NAC that's working. Other systems can successfully take posture reports from the Microsoft NAP agent and make enforcement decisions based on that data.

If each vendor - including operating system manufactures, switch vendors, security application vendors and even security hardware vendors – had been on board *sooner* with one or more frameworks, we would already have seen larger number of successful NAC installs. Using standards for communications and decision-making policies in NAC opens up the field to more vendor interoperability and less pigeon-holing by limiting a solution to a single vendor set.

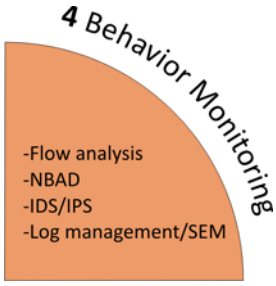
Result: The freedom of interoperability will reduce long term costs and short term complexity of designing and implementing NAC solutions. NAC solutions will have a longer life span, making them more efficacious and sustainable in the long run. NAC is an expensive undertaking, both in time and resources. Organizations want to know the technology and solution will be around as long as they need it.

f. Use firewalls or application-aware devices to stop undesirable activity

In situations where an organization plans to implement Endpoint Integrity checks for the purpose of restricting use of specific applications, we have other options besides NAC available for enforcement. Similar to the *moat versus safe* concept discussed earlier; instead of putting controls on the endpoint, we can suppress application activity using firewalls and application-aware devices on the network. These products filter specific applications at layer 7 and will be just as effective for any application that can be controlled within the network, or on its way out of the network (at the gateway).

Result: Again, by offloading the Endpoint Integrity requirements from the NAC system, we can free up resources and reduce complexity. Depending on the needs of the organization and the device selected to substitute for Endpoint Integrity, this solution may (or may not) be more cost-effective.

4. Cleaning up Behavior Monitoring



Behavior Monitoring is the last of the four feature components we're addressing. There's not really much to clean up here, since most behavior monitoring solutions are built on solid foundations and the concept is pretty straight forward. Tweaking behavioral systems that rely on base lining can be tricky, but that's outside the scope of this document.

In our discussion here, **Behavior Monitoring** technologies are anything that can **watch**, **monitor** and **report on abnormal or anomalous behavior** of devices on the network and of the network as a whole. These solutions usually rely on flow sampling, traffic base lining, IDS/IPS signatures and similar technologies to detect oddities on the network. In advanced systems, we can also use this data to trigger events and take steps to remediate a concern.

Behavior monitoring is also a great supplement to any endpoint integrity driven NAC solution, as it provides reliable data on actual endpoint behavior, without relying on statement of health replies from a potentially compromised endpoint.

a. Integrate frameworks for reporting (such as TNC IF-MAP)

We're having more discussions about standards. If we have dependable standards, we can make key pieces of the network talk to one another and make our security infrastructure integrate cleanly. Frameworks like TNC's IF-MAP are already being used for successful communications between firewalls, IDS/IPS devices and NAC management consoles. NAC solutions using this technology can send and receive information to and from the *eyes and ears* of the network and have reliable information to use in deciding whether a connecting device is safe or hostile, healthy or infected. The implications of TNC's IF-MAP are far greater than what can fit in this document.

Result: As with all other discussions of standards, these integrated communications will allow us to leverage security devices already in the network. Each product can then focus on its core competency and make data available to participants in the security infrastructure for decision making purposes. While this prospect seems more complex than a simple drop-in solution, the fact is standards make things interoperable and interoperability makes things less complicated.

b. Use switches and infrastructure tools already in place

Several vendors in the network security space have products available that integrate their hardware and software for a system that allows the network to monitor and take action on endpoints that seem to be misbehaving. Currently, these communications and interactions are proprietary, but with the standards forming, we should see more of this interfacing in the future.

With standards in place, consumers and vendors of NAC have a variety of options available when architecting solutions. Network switches and management tools that monitor behavior and take part in remediation can provide automated behavior monitoring without layering additional hardware and software.

For example, we can configure our switches to sample traffic and alert our switch management software if something is amiss. The switch can then take corrective action, by shutting of the port of an offender, locking out a device's MAC address or sending an alert to the network team for investigation.

Result: Using the hardware and software already in the network offers several advantages. The costs associated with additional products are reduced or omitted. We have a system that is receiving feedback directly from hardware that's already in a position to watch traffic without offloading it or sending it through a bottleneck. Lastly, we're simplifying the design by reducing the number of components participating in analysis and reporting.

c. Use firewalls/IDS devices internally to investigate signature-based attacks

Most enterprises have a variety of traditional gateway security devices within the network – including firewalls, UTMs, IDS and IPS devices. These devices, wherever they are placed, can participate in traffic analysis and signature matching then report back to the network access infrastructure or NAC console.

For example, we can configure switches to mirror suspicious traffic to a firewall or IDS device for signature analysis. If it sees malicious traffic, it can alert the switch and let the switch take corrective actions.

Result: Systems built on open communication and collaboration are more cost effective and reliable. This type of collaboration offers a comprehensive integration by the most basic and trusted security components of a network. Overall, both cost and complexity are reduced in the long term.

d. Use centralized log management and visualization to track trends

If an organization does not have, or does not wish to leverage flow analysis from LAN devices, another option is the use of a centralized log management system in combination with good reporting or data visualization tools. Log management systems can be used to centrally collect log information and monitor the state of the infrastructure as a whole. In combination with reporting and data visualization tools, these log repositories can be used to debug issues, troubleshoot incidents and proactively identify mis-configured devices.

Result: By visualizing the information, administrators are given a tool to quickly navigate the current events, explore relationships and identify the root cause of an incident or anomaly. Simple scenarios include reporting on failed logins and evidence of port scans to uncover reconnaissance activities. More sophisticated visual analysis can help analyze traffic patterns to discover covert channels or simple mis-configurations of hosts and network devices.

SIDEBAR | Security Visualization

Data visualization techniques offer an effective and insightful way of analyzing the log data collected from networked devices. The detection of security issues and the forensic investigation of possible attacks greatly benefit from these visualization techniques. Detecting security issues is not a simple task, as attacks can rarely be identified from raw log data. In cases of abused privileges, the attacker can easily hide his or her trail. However, clever visualization techniques can expose these suspicious activities and help uncover the perpetrator.

For more information on security visualization, I recommend *Applied Security Visualization* by Raffael Marty. It's a great resource for visualization and includes frameworks as well as step-by-step processes to help get readers started. In addition to the book, I encourage you to also look into the SecViz portal (http://secviz.org), a community portal that provides further resources and examples of security visualizations.

V. Moving Forward

I'm convinced there's a genuine need for NAC-like solutions and I think when we get it right, we'll wonder how we ever secured our networks without it. We have some changes to make before we can fully realize all the greatness of future NAC technology and there are calls to action for the industry, the vendors and consumers of the technology.

How the industry is cleaning up NAC

The industry is heading down the right path integrating the technical components with various frameworks and standards from TCG's TNC, IETF's NEA and IEEE's 802.1X. Several vendors are moving forward with R&D efforts focused on integration, including integration with Microsoft's NAP framework and TNC's framework.

The frameworks are growing and as they're adopted as standards, we'll begin to see more consistency in terminology, feature sets and implementations. Providing clear descriptions and concepts of NAC for customers and vendors alike will pave the path to a better understanding of the technology.

Bringing accountability to vendors

The industry as a whole has certainly contributed to the mayhem of NAC technology, but vendors have only added to the confusion by polluting the market with meaningless words and acronyms. Vendors want to stake their claim as the primary market leader and they'll do just about anything to get more of their NAC products sold.

Manufacturers of these technologies must stop marketing their NAC products as a solution for needs it was not designed to directly address. For example, regulatory compliance reporting, user tracking, guest access and port security may not actually require a full NAC rollout, but vendors will pitch their product to meet any needs they perceive as a potential fit, regardless of whether it's the right thing for the customer.

Vendors also need to stop feeding the perception that NAC is difficult and unmanageable; a realization exacerbated when manufacturers push their NAC products in a customer environment in which it cannot possibly succeed. There are many variables involved in choosing the right NAC solution and vendors are too quick to assure potential customer that *their* solution is the right fit, even if it results in an impossible feat of engineering.

In addition to remediating their tendency to push a square peg into a round hole, vendors should help NAC move forward by taking the initiative to participate in the standards and frameworks available. These standards groups are open for all to participate, and it's time for manufacturers to focus their efforts here for greater integration.

With existing standards for RADIUS, EAP and SNMP, product designers have a variety of options for communications between NAC management and network devices such as switches and access points. The addition of new frameworks such as TNC's IF-MAP gives vendors added integration and information sharing to and from other security devices, which could (and should) be used in place of proprietary communications between NAC management and firewalls, IDS, IPS, flow analyzers, authentication servers and network scanners. When mainstream vendors adopt this level of integration, the technology as a whole will have a greater longevity, be more widely supported and be a better investment all around.

Inciting customers to demand more

The final piece of moving forward must be driven by consumers of the technology. Consumers *must* demand standards and interoperability from the vendors. Otherwise, the vendors will continue to churn out product-based solutions in an effort to meet stringent sales goals.

How can consumers demand more from vendors? Consumers should ask vendors which standards and frameworks they're leveraging in their solution. They should ask specifically about interoperability with the other products in the environment – including the customer's anti-virus vendor, switch vendor, IDS/IPS vendor and anything they may wish to incorporate in the future.

Consumers should also ask their vendors for a formalized roadmap showing their planned efforts in NAC development for the next 12 to 36 months. If a vendor can't provide that to you in writing, chances are they don't have a business case for continuing R&D in that area, which means the product will likely be abandoned in the near future. Product technologies (such as NAC) that require extensive evaluation and network redesign are not a good investment for customers if they aren't accompanied by long term roadmaps.

Renaming NAC

In order to clear up some of the misunderstandings of NAC solutions and NAC features, I'm of the opinion that NAC should be renamed. The fact that several vendors have recently begun renaming and rebranding their NAC solutions is evidence to me that they've reached the same conclusion. There's a volume of confusion around the term NAC in and of itself, in addition to added misinterpretation of the various vendor terms and acronyms.

Ideally, I'd like to see the framework organizations (such as TCG/TNC or even IETF) create a naming methodology for NAC solutions based on the feature components they offer. There would still be some clarification needed as to how the features are implemented and the security enforced, but that could also be addressed using standard terms outlined by the framework.

With an unambiguous view of the feature sets being offered by vendors, consumers of NAC technologies would have a much easier task of comparing and evaluating competitive solutions to see which best fit their needs. If we make these steps easier for the customers, we're already on our way to simplifying the overall solution and helping NAC move forward.

VI. About the Author

Jennifer Jabbusch is a network security engineer and consultant with Carolina Advanced Digital, Inc. Jennifer has more than 15 years of experience working in various areas of the technology industry. Most recently, Ms. Jabbusch has focused in specialized areas of infrastructure security, including Network Access Control, 802.1X and Wireless Security technologies.

Jennifer has consulted for a variety of government agencies, educational institutions and Fortune 100 and 500 corporations. In addition to her regular duties, she participates in a variety of courseware and exam writings and reviews, including acting as subject matter expert on Access Control, Business Continuity and Telecommunications, and lead subject matter expert in the Cryptography domains of the official (ISC)2 CISSP courseware (v9).

Ms. Jabbusch speaks about network security at a diverse mixture of national and international conferences, including INTEROP, SecTor, Infosec World, ISSA, Techno Security and government-hosted events by the FBI and US Secret Service.

You can find more security topics on her security blog at http://SecurityUncorked.com and at LinkedIn http://www.linkedin.com/in/jenniferjabbusch.

About Carolina Advanced Digital, Inc.

Carolina Advanced Digital, Inc. (CAD) is a woman-owned, veteran-owned and privately-held small business specializing in IT infrastructure, security and management solutions. For more than 25 years, CAD has been the leading engineering service and product provider for federal, state and local government agencies as well as healthcare, education and corporate markets. Most of CAD's professional services and products are available via open market, federal GSA and various state contracts.

Contact

Carolina Advanced Digital, Inc.
Cary, NC | 919.460.1313 | 800.435.2212
http://www.cadinc.com

Appendix A: Index

802.1AR 21
802.1X ..... *See* IEEE 802.1X, *See* IEEE 802.1X
Access Management versus Threat Management 16, 17
Access Rights 14, 15, 19, 20, 23, 24
Authentication 14, 15, 19, 20, 21, 23, 26
Autonomic Networks 13
Behavior Monitoring 14, 16, 17, 19, 26, 27
Black Hat 8
Bradford 11
Caymas Networks 13
Check Point 13
Cisco 11, 12, 13, 22, 34, 36
Consentry Networks 13
Crossing the Chasm 10
data visualization 28
Endforce 13
Endpoint Integrity 14, 15, 19, 20, 25, 26, 27
Enterasys 11
feature components 14, 16, 20, 27, 30
firewalls 14, 21, 24, 26, 27, 28
  application firewalls 24
ForeScout 11
HP ProCurve 11, 22
IEEE 802.1X 12, 14, 20, 21, 22, 23
  802.1X-REV 21, 23, 28
IETF 12, 21, 29, 30
Juniper 11
Lockdown Networks 13
log management 28
McAfee 11
Mirage Networks 13
NBAD 16
Nortel 13
Perfigo 13
Security B-Sides Conference 8
Sophos 13
StillSecure 8, 11
Sygate 13
Symantec 11, 13
Technology Adoption Lifecycle 19
Trusted Computing Group 12, 21
Trusted Network Connect 12, 21
  IF-MAP 21
Trustwave 13
Vernier Networks 13
VLAN 20, 22, 23
Zone Labs 13

Appendix B: Terminology

Behavior monitoring

Behavior monitoring or behavior analysis involves gathering and analyzing network traffic, usually by sampling. Expected behavior is used to create a baseline, a background on which anomalous behavior can be easily identified. Behavior monitoring provides the unique ability to identify not only malicious traffic, but legitimate traffic that may be undesired for other reasons. For example, a lab employee suddenly accessing an HR server, or a CEO visiting job search sites might be precursors to other events of interest.

Data visualization

Data visualization is the process of collecting raw data and representing it in a more familiar visual format, which may include two-dimensional or three-dimensional representations, graphs, models and even animations. Visual representations make it easier to identify trends and anomalous behavior when analyzing security data from networked devices.

IEEE 802.1AE

IEEE's MAC Security standard (MACsec) was finalized in 2006 to enhance layer 2 security with confidentiality and integrity. The standard specifies layer 2 encryption, using AES, but does not include the key exchange (outlined in P802.1af). The P802.1af will be rolled up with other projects and standards and integrated in the 802.1X-REV.

IEEE 802.1af

IEEE's Media Access Control (MAC) Key Security standard is the key exchange (MACsec key agreement) for use with 802.1AE. Very basically, it specifies the key exchanges used for encryption and identification in 802.1AE. The 802.1af project was merged into the 802.1X-REV.

IEEE 802.1AR

IEEE's Secure Device ID (DevID) specifies truly unique per-device using cryptographically-bound identifiers. The DevID will provide a more secure way to identify devices than traditional MAC addresses, which are easily spoofed. Other standards bodies, such as the IETF, have identified uses for DevID in their standards for network infrastructure, including ARP.

IEEE 802.1X

IEEE's 802.1X is a standard for port based security. It was recently renamed port based network access control, which occasionally leads to confusion of NAC with 802.1X.

802.1X, in its current form (802.1X-2004) outlines authentication for wired and wireless devices to the network using device or user identification and authentication in the way of login credentials, certificates, tokens, MAC addresses, or combinations of the above. 802.1X has been opened for revision and is currently 802.1X-REV in draft format.

IEEE 802.1X-REV

IEEE's 802.1X standard for port security is currently in a revision status, undergoing an overhaul. When it is finalized, it will be renamed, appending the year of standardization; 802.1X-2009 or 802.1X-2010.

The current 802.1X-REV includes a variety of added functions not currently available in 802.1X-2004. New functions include MACSec encryption, MKA key exchange and Network Advertisements.

IETF NEA

Internet Engineering Task Force's Network Endpoint Assessment standard (in draft current) that addresses portions of endpoint posture assessment. At this time, primary participants of the working group are Cisco, Juniper and NIST.

The current draft of IETF NEA is derived mainly from components outlined in the TCG's TNC framework but only addresses portions of the framework, making IETF NEA an inadequate solution at this time.

NBAD (Network Behavior Anomaly Detection)

Network behavior anomaly detection (NBAD) is a specific implementation of behavior monitoring in which network devices are either directly or indirectly (via management software) analyzing traffic and identifying strange behavior. Typical NBAD solutions are implemented using flow data fed from switches and identify common anomalies such as spoofed MAC addresses, duplicate IP addresses, TCP and UDP fanouts and excessive connections.

SEM/SIEM (Security Event Manager)

Security event managers, sometimes referred to as SIEM (security information and event managers) are central repositories of log data. Most SEM tools parse raw log data and use custom filters and searches for event correlation. These tools are especially useful for incident response and tracking security events through a network, where more than one device is involved.

TCG (Trusted Computing Group)

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms. The TNC frameworks are under TCG.

TNC (Trusted Network Connect)

TCG's Trusted Network Connect (TNC) network security architecture and open standards enable implementations of network security, including NAC, with extensive interoperability and support for multi-vendor environments.

The TNC frameworks are what most vendors are currently integrating. The components are robust and well-defined, making it the best (and currently, the only complete) NAC framework for interoperability. TNC is also interoperable with Microsoft's NAP solution.

TNC IF-MAP

TNC's IF-MAP describes a database service that contains information (metadata) about systems and users currently connected to a network.

The goal of IF-MAP is to facilitate sharing of security-related information throughout the network infrastructure. Solutions integrating IF-MAP can talk to components such as firewalls, switches, SIEMs, DHCP and authentication servers and other devices with information pertinent to painting the bigger picture of the network's posture. This information sharing allows the network to make intelligent decisions based on a full set of records, instead of a single data point.

Appendix C: Resources

Bradford Networks
Company site at www.bradfordnetworks.com

Chasm Group
Company founded by author of Crossing the Chasm, referenced in this paper, www.chasmgroup.com and www.chasminstitute.com

Cisco
Company site at www.cisco.com

IEEE
Primary site at www.ieee.org

IETF (Internet Engineering Task Force)
Primary site at www.ietf.org and NEA working group information found at http://tools.ietf.org/wg/nea/

Juniper Networks
Company site at www.juniper.net

Security Uncorked
Blog site at www.securityuncorked.com

SecViz Portal
Online peer portal for sharing security data visualization at www.secviz.org

StillSecure
Company site at www.stillsecure.com

Symantec
Company site at www.symantec.com

TCG (Trusted Computing Group)
Primary site at www.trustedcomputinggroup.org

TNC (Trusted Network Connect)
Information on TCG's TNC framework at http://www.trustedcomputinggroup.org/solutions/network_security

