

WHITE PAPER



BIGFIX

THE FALL AND RISE OF NETWORK ACCESS CONTROL

By Amrit Williams, Chief Technology Officer, BigFix, Inc.

Few security initiatives have enjoyed as much hyperbole as network access control (NAC). Aggressively promoted by industry titans Cisco and Microsoft and adopted as a rallying cry by the majority of security vendors, NAC has almost eclipsed compliance as the most talked about security-related development of the past couple of years. In the real world, however, NAC technologies have experienced more than their share of delays, failed deployments, and over promised/under delivered solutions. Despite these difficulties the NAC concept is neither dead nor useless. With an initial phased approach, realistic expectations, proper planning, optimized (re) use of existing infrastructure, and integration into a comprehensive, pro-active approach to IT security policy management, NAC can be a valuable addition to an overall information security program.

WHITE PAPER

Why NAC?

Prior to the worm attacks at the beginning of the decade most organizations focused their security efforts on building a strong perimeter against external threats. Firewalls and anti-virus technologies became the most widely adopted measures and, when used correctly, did a pretty good job of rebuffing and containing attacks on networked resources. But soon the black hats accelerated the pace of “innovation” and the gravity of their attacks. At the same time, an increasingly mobile workforce, and more outside stakeholders – contractors, suppliers, partners, service providers, etc. – required enterprise network access. As a result, it became very difficult for most organizations to defend the integrity of their infrastructure. As threat-specific defense techniques became less effective, systems became more difficult to manage, and worms laid waste to network availability, the traditional security approach was about to be turned on its head.

The vectors for worm attacks shifted to managed assets that left the network perimeter and immediate control of IT managers, became infected, and then returned to the enterprise. Bypassing traditional security mechanisms the compromised device, and its uninvited guests, wreaked havoc as the infections sought other vulnerable hosts to exploit. Although the infected end-points acted as the carriers of infection, it was the network that bore the brunt of the attacks as the worms degraded network availability and transaction integrity. Under these circumstances, it became clear that protecting the whole was more important than protecting individual devices and that blocking suspect devices from network access would isolate threats before they could spread.

NAC's Achilles Heel

NAC technologies pose a number of implementation-level issues including resource requirements, lack of product maturity, management complexity, logistical challenges, little visibility into the identity of the users, ability for attackers to bypass controls, and

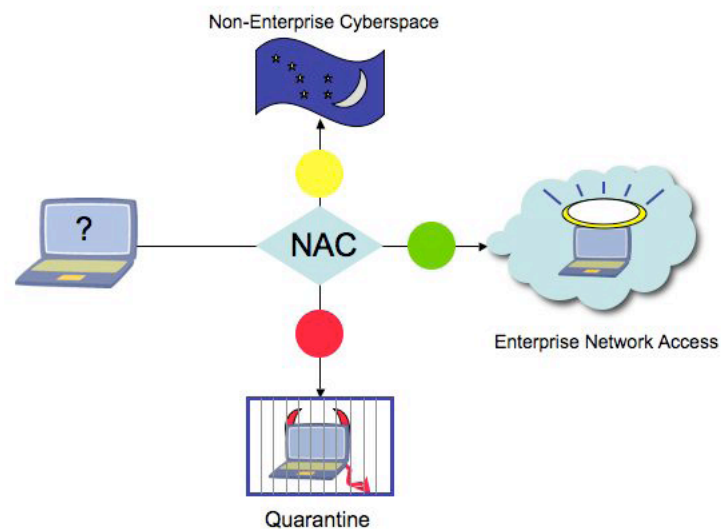


Figure 1: NAC solutions work by assessing computers against dress codes to determine whether they should gain full network access, limited access, or consigned to a quarantine.

process and technology integration. However NAC's biggest flaw is that it focuses on quarantining hostile devices rather than implementing mechanisms to prevent managed devices from becoming non-compliant or compromised in the first place.

The process of quarantining first and fixing a compromised device later can create many technical and organizational issues. Quarantining the CEO's laptop could be a career-limiting move, as would locking out a device a salesperson relies on to post an order or quarantining a device that delivers critical services. Quarantining is clearly a very blunt but effective technique whose use requires subtlety and skill to avoid unintended consequences.

Needed: A New Approach to NAC

Continuous policy enforcement, the ability to update security defenses, patch systems, and reconfigure devices, on or off the network is critical to moving an organization from reactive, fire-fighting mode to a mature security posture that puts the organization back in control of their systems. This is particularly true with NAC solutions where continuous policy enforcement can be used to assess and “pre-mediate” devices to conform to NAC dress codes before they log onto the network.

As workforce mobility increases and the ability of the IT organization to manage these assets decreases. Managed assets that leave the control of the IT essentially become unmanaged assets. Currently, the vast majority of system management solutions do not enable effective continuous policy management. Weaknesses for conventional system management technologies fall into three areas. First, they lack real-time information on managed device configuration state. This is particularly the case for scanning-based solutions where configuration information is only valid at the time of a scan, and a long interval between scans due to the workloads they impose on networks and managed devices. Even if an organization could scan its infrastructure daily for policy compliance, this gives managed devices 24 hours to drift out of compliance, get infected by malware and generally set themselves up as candidates for quarantine.

Second, most conventional solutions have blind spots that exclude significant classes of assets from effective assessment and remediation. For starters, it's common for many solutions to focus on only a single technology platform—usually Microsoft Windows. While Windows remains the biggest game in town, it's not the only game. Most organizations will also need to manage Unix and Linux devices and may also need to enable access for technology platforms not officially supported by the organization, but used by qualified outsiders or employees checking in from home or on the road, i.e. Mac OS.

Beyond that, the biggest blind spot for conventional approaches is poor management coverage of mobile laptop/notebook systems. This is perverse as these are the systems that are most likely to regularly request access to enterprise networks, fall out of compliance and pick up malware while roaming. It does not go too far to say that a security and configuration management solution that does not offer equivalent management service levels to both fixed and mobile assets is useless in supporting NAC solutions.

Third, since NACs are geared to making binary go/no go decisions on admitting devices logging on to the network, they tend to take a very shallow view of what makes a device eligible for access or not. This means, for example, a NAC may admit or exclude a device depending on whether it runs antivirus software or not, but lack the ability to assess whether the antivirus package is updated with the latest malware definitions. Needless to say, you can't block today's threats with yesterday's configurations and false confidence in device goodness instilled by low resolution device assessment can convert a NAC from a security asset to a liability.

Fourth, administrators must use multiple tools to remediate the wide variety of configuration settings and software (both operating systems and applications) that may be subject to a NAC dress code. This not only slows the process of assessing and remediating managed devices, but any additional complexity in technologies and processes creates opportunities for errors and inconsistencies.

BigFix NAC Support

BigFix offers consolidated IT security policy management capabilities that overcome the limitations of conventional security and system management technologies. These capabilities come from both the innate properties of the BigFix Core Services Platform and specific tools and capabilities that can be managed through the BigFix Console.

At the platform level, the BigFix single agent/single management infrastructure brings consolidated real-time visibility and control to enterprise-wide security and configuration management. The BigFix Agent provides real-time information on the configuration and state of every device it runs on—mobile or fixed—with no scanning required. The BigFix Agent also runs on Windows, Linux, Unix and Mac OS systems, with these devices visible and manageable through the BigFix console.

Perhaps the most important property that BigFix brings to NAC is the ability to manage both fixed and mobile computers at equivalent levels of visibility and control. Managing mobile laptop/notebook computers is a long-standing BigFix strong suit. The BigFix Agent remains resident on mobile computers whether they are connected to the enterprise network or not. Policies remain in force on mobile systems until changed by enterprise IT managers. Roaming computers can also be instructed to make contact with the enterprise network to transmit configuration change information and receive policy and management content (software updates, new policies, patches, etc.) any time the mobile device connects to the Internet.

WHITE PAPER

BigFix complements the capabilities of the BigFix Core Services Platform with a growing array of tools and capabilities that enable automated discovery, assessment, remediation, and enforcement of security policies. Current capabilities include asset discovery and inventory, antivirus, anti-spyware, personal firewall, vulnerability assessment and remediation, operating system and application software update and patch management, and technical controls compliance reporting.

Making NAC Work

Adding BigFix to a NAC solution should sharply reduce the number of devices caught in quarantine through BigFix's pre-mediation capabilities. For those caught in quarantine, BigFix can automate and speed the process of identifying device configuration deficiencies and correcting them.

Of course, not every machine attempting to access a network—particularly those used by non-employee business partners—will have BigFix installed on it. Here, assuming the machine's owner consents to this as a condition of doing business, it is possible to temporarily install a BigFix Agent on a guest computer, assess its configuration, remediate it, and uninstall the Agent when the machine exits the enterprise network.

The BigFix ability to report the latest configuration information on mobile computers makes it possible to anticipate which currently roaming devices will qualify for quarantine or require remediation before logging on to the enterprise network. This is a actually a process of logical elimination that Sherlock Holmes used as a standard practice. If you have a record of a mobile computer's configuration at the time it left the enterprise network, and admissions dress codes (inevitably) change, it follows that devices you haven't touched since their logoff will be blocked from access when they return. Furthermore, you will have a very good idea of what will need to be fixed before you assess the machine's configuration either at log in or when it phones home via the Internet when roaming. Having this kind of predictive information on machine configuration status speeds and simplifies the process of restoring it to good citizenship.

BigFix also opens the door to another intriguing possibility—implementing a BigFix solution that performs NAC-equivalent functionality without need to invest in additional dedicated NAC hardware and software. Since BigFix can continuously monitor and adjust device configurations in real-time, detect and isolate rogue and non-compliant devices, and generally provide functionality comparable to dedicated NAC solutions with less expense and management complexity, implementing a BigFix-based virtual NAC merits consideration by those who want to add a preemptive block-the-bearers-of-threats capability to their IT security program.

Bottom Line

NAC can only be effective when coupled with a program of continuous policy enforcement of managed systems. Quarantining devices should be a last resort and not the main method to secure an environment. Until recently, most security and configuration management solutions could not provide the comprehensive, continuous visibility and control required to enable managed devices to avoid unnecessary visits to quarantine limbo. BigFix, however, offers capabilities that can significantly enhance the effectiveness of NAC solutions. While after an initial burst of industry enthusiasm, NAC has lost momentum as the next big thing in enterprise information security, BigFix offers technologies and solutions that can revive the viability of NAC solutions by improving their flexibility and cost effectiveness.