The Critical Security Controls: What's NAC Got to Do with IT?

Sponsored by ForeScout

The Critical Security Controls: What's NAC Got to Do with IT?

April 2013

A SANS Whitepaper

Written by G. Mark Hardy

Introduction

Enterprises are leveraging virtualization, wireless, mobile and cloud technologies. These technologies advance service delivery, but can increase operational and security risks. Why? Access to corporate resources and data, as well as these types of devices and applications, has become more diverse and dynamic. In turn, the perimeter continues to become more porous and blurred, which affects IT security policy enforcement and risk management. Given the operating dynamics and diversity, most enterprises are aware of only 80 percent of the devices on their networks, according to a 2011 Gartner report.[1] As a result, many endpoints are unmanaged, unprotected or unknown.

Even with host-based protection and system management being the cornerstone to maintaining endpoint integrity, many approaches to IT security often rely on endpoint software that can be inactive, uninstalled, corrupted or nonexistent—leaving IT with significant visibility and compliance gaps.

Growing data loss and compliance risks introduced by so-called IT consumerization—in particular, enterprise mobility combined with employees using their personal mobile devices and applications at work—further exacerbate these issues. As a result, organizations are employing a variety of security mechanisms to enable the secure use of employees' personal smart devices (known as BYOD for "bring your own device"), as well as a range of corporate-provisioned devices (CYOD, "choose your own device.")

Such mechanisms are found in a range of tools and technologies, including mobile device management (MDM), network access control (NAC), virtual application containers, and Virtual Device Interface (VDI). Unfortunately, a recent SANS survey of mobile security[2] indicates that most organizations are forgoing technical solutions and relying most heavily on user education for prevention, thereby leaving a window of opportunity for data leakage, unauthorized access, malware and phishing-based attacks.

There are many options for building a defense-in-depth strategy. One is to invest in an arsenal of security tools. Another is to leverage governance, risk and compliance (GRC) standards and best practices to optimize security operations and manage risk. These approaches are not mutually exclusive, but without a mature framework, implementers can still leave holes or gaps in coverage.

In 2008, the Office of the Secretary of Defense asked the National Security Agency for assistance in prioritizing security controls. With an emphasis on fixing known problems, the resulting control set was significant in that every control could be shown to stop or mitigate a known attack. The NSA agreed to share attack information with the Center for Internet Security (CIS) and the SANS Institute. The result was the consortium that developed the Critical Security Controls.[3] Every 6 to 12 months, the consortium reviews new attack information to ensure that controls are updated to reflect current threats.

1 "Strategic Roadmap for Network Access Control," Gartner, October 2011, by Lawrence Orans and John Pescatore.

2 www.sans.org/reading_room/analysts_program/SANS-survey-mobility.pdf

3 www.sans.org/critical-security-controls/history.php

Within the context of the CSCs, NAC tools offer a robust suite of capabilities that manage risk and reduce exposures found in today's extended networks. Next-generation NAC platforms can deliver visibility and security profiling of all devices on the network and provide role-based monitoring and flexible enforcement capabilities to support a variety of controls that can be mapped across the CSCs. From protecting the network against rogue devices and insecure access, remediating endpoint configuration and security violations, to segmenting wireless and wired sessions in the network, NAC can now automate many tasks listed in the CSCs. Proven security best practices and the capability to automate good behavior when possible are at the heart of the CSCs.

This paper reveals what NAC can do today, how it stacks up to many of the CSCs and what strategies are needed for successfully leveraging NAC to reduce risk, improve compliance and meet the key automation and integration requisites cited in the controls.

What Is NAC?

NAC is a policy-enforcement mechanism originally designed to authenticate and authorize systems attempting to connect to a network. Early NAC implementations relied on 802.1X,[4] the IEEE standard for authenticating the communications between the network and a managed endpoint to offer port-based NAC. First published in 2001, 802.1X specified a means to validate a connecting device via client software (usually referred to as an *agent* or *supplicant*) with an authenticator, typically an 802.1X-enabled switch. The session is comprised of a device requesting access to the network, and the switch, in turn, forwarding the request to an authentication server. Depending on the results of the validation process, an appropriate production or guest port connection to the network would either be granted or denied.

This binary go/no-go decision worked well in a homogeneous and static network with managed endpoints. However, today's enterprises, which include BYOD clients, network printers and a variety of other networked devices, can introduce greater administrative overhead for pure 802.1X-based NAC.

Next-Generation NAC

Modern NAC platforms go far beyond the core functionality of providing trusted network access for known hosts and guest access for unknown hosts. NAC enables 802.1X and alternative authentication mechanisms to secure device access and, by using a variety of methods, to determine if the endpoint meets security standards. NAC can enable this with or without requiring the use of persistent agent software on the devices being inspected.

NAC provides a range of endpoint discovery, assessment, enforcement and remediation capabilities that combines to automate a variety of operations falling within the CSCs. Today's NAC offers integrated functionality that supports continuous endpoint monitoring and mitigation of incorrect configurations or issues with host-based protection and management software. NAC, in conjunction with wireless access and RADIUS-based authentication, is often used in combination to support BYOD and CYOD security strategies.

Fundamentally, NAC offers a mechanism for consistent policy enforcement that begins with real-time discovery, authentication and classification of devices attempting access and those that are on the network. A NAC rules engine can base its decisions on predefined policies regarding user, location, time, device type, configuration and security posture attributes. With this level of policy automation, NAC is useful for readily identifying when new and unknown or rogue devices are attempting access. Using role-based device inspection, granular policy regarding endpoint configuration and security compliance can be applied against known and unknown systems requesting access.

Depending on the user, device and severity of the violation or security issue, next-generation NAC offers a variety of control options based on policy. These options, depending on how the device can be classified and managed, range from allowing, blocking or limiting device access to remediating endpoint security and configuration issues using different methods, including such options as access control lists (ACLs), firewall- and router-level traffic restrictions, script execution and VLAN switching.

NAC can also be set to simply monitor policy adherence and generate alerts, tickets and reports only when violations arise. Some NAC platforms can interface with third-party tools.

4 http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

Here are some examples of what NAC can do today, many of which fall under the purview of the CSCs:

- **Discover devices, including nontraditional devices connecting to the network**
- **Identify type, location and attributes of devices connecting to the network**
- **Inspect devices for configuration (installed software, patches, etc.) and compliance levels before granting access**
- **Report and remediate clients that fail to meet security standards**
- **Provide granular access controls as dictated by business needs**
- **Identify rogue devices, such as wireless access points (WAPs), without the need to walk around with a laptop and directional antenna**
- **Enforce customized policy for personally-owned devices that connect to the network, including integrating with other controls such as data loss prevention (DLP), MDM or VDI**
- **Provide bidirectional data integration with other security and business systems such as security and event information management (SIEM) tools**

Given the breadth of continuous monitoring, reporting and remediation functionality, NAC represents an invaluable tool to automate GRC mechanisms—automation being one of the main tenets of the CSCs.

Applying NAC to Operational Risk and Compliance

For most organizations, the primary drivers for selecting security technology are to manage IT operational risk and to adhere to internal, industry or regulatory compliance mandates. Although they sound simple, risk reduction assessment, mapping compliance requirements and evaluating controls can be complex processes—particularly on an integrated, automated level. To appropriately apply security technologies to support IT GRC efforts, an organization has to ask itself the following questions:

- **What operational risks affect business processes and requirements?**
- **What is the consequence of a threat or vulnerability to the set of infrastructure and applications delivering a business service?**
- **What compliance mandates apply to our company?**
- **What combination of policies, processes and controls are best suited to measure, mitigate or reduce risks and vulnerabilities, and contribute to compliance?**
- **What tools can we apply to effectuate and automate security controls?**
- **Is the risk reduction cost-effective? Does it optimize resources?**

NAC offers IT organizations immediate operational intelligence and automated control: from knowing who and what is attempting access to (or is already on) the network; to knowing how devices are configured and whether requests are authorized, unauthorized or do not meet configuration policy; to taking action to mitigate or remediate violations and issues; and finally, to reporting on these activities.

This level of network asset information and policy-based response not only reduces risks, but also can support documentation and demonstrate adherence with government and industry regulations. NAC can map to many compliance standards and guidelines: Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and Federal Financial Institutions Examination Council (FFIEC) principles and standards. NAC capabilities for mobile security, endpoint compliance and threat prevention, as well as access control, are applicable across multiple compliance frameworks depending on organizational needs.

The Critical Security Controls

Automation with integration, resource optimization and visibility are critical elements in making any layered defenses effective. These support the two guiding principles of the CSCs: "Prevention is ideal but detection is a must" and "Offense informs defense." A consortium of information security professionals from government and industry first drafted the CSCs in 2008. Revised to version 4.1 as of March 2013, the CSCs (maintained today by the SANS Institute and consortium experts) offer a control methodology to help organizations keep up with modern-day threats, including the challenges presented in this paper.

The specific controls are shown in Figure 1.

Figure 1. The CSCs (interactive for online readers)

5 "Critical Controls for Effective Cyber Defense: Version 4.1" page 2; www.sans.org/critical-security-controls/cag4-1.pdf

NAC Applied to the Critical Security Controls

Many of the controls in the CSCs relate to access, identification and management of endpoints, asset intelligence and configuration and other functions that NAC can complement and automate. Table 1 provides a more detailed listing of the specific CSCs that NAC is best suited to support.

Critical Security Control	NAC Capability	Advice for Automation
1 Inventory of Authorized and Unauthorized Devices	NAC can obtain the identity, device, network and authorization attributes of systems connecting to (and connected on) the network. NAC responses to detected devices include the capability to classify, assess, alert, report, segment, enforce and mitigate.	Use NAC to identify and classify what's requesting access to network resources; then focus on devices that you haven't authorized to determine if they are wanted or unwanted. NAC policy can block or reassign unknown devices to a segmented LAN for further investigation. NAC can generate tickets and report on such events.
2 Inventory of Authorized and Unauthorized Software	By inspecting a device and comparing its configuration against policy (on access request, post-access or at polling intervals), NAC can fingerprint installed and running software and assess if the system configuration adheres to policy.	Use NAC to maintain and enforce a blacklist or whitelist of approved software versions. Provide automated response based on policy in the event of unapproved application use, such as a noncorporate IM or P2P tool. NAC can generate tickets and reports on such events.
3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	By virtue of identifying and enforcing OS patches and host-based protection before a device connects to network resources, NAC reduces the attack surface by closing vulnerabilities attackers look to exploit.	Define policies for what is an acceptable configuration based on device type and usage. Maintain secure configurations through NAC-initiated scans as devices attempt access. Automatically execute remediation if the device is out of compliance. Integrate MDM device-level controls (device, application, data) with NAC network-based controls to secure BYOD/CYOD devices.
4 Continuous Vulnerability Assessment and Remediation	NAC can identify and remediate or block suspicious and vulnerable nodes. NAC can be leveraged to initiate an immediate vulnerability assessment (VA) scan on new network devices.	Tune NAC enforcement policies based on device, user, resource request and configuration or host-based protection violation scenarios. Integrate NAC with vulnerability assessment tools to trigger vulnerability scans of new devices attaching to the network and to isolate and remediate vulnerable systems.
5 Malware Defenses	NAC complements host-based protection to ensure malware defense is installed, active and up-to-date when requesting network access. Some NAC platforms offer post-network admission behavior analysis to respond to suspicious or malicious behavior. For example, it can check the state of active antivirus or DLP software on the device. If the software is out of date or absent, NAC can automatically isolate the device from the network until it is brought into compliance.	As above, dictate policy for when NAC discovers host-based protection issues or suspicious behavior; integrate NAC events with other reporting systems such as SIEM. Use NAC as a first-line "circuit breaker" defense to stop zero-day malware propagation.
7 Wireless Device Control	NAC works with WAPs and wireless networks to enable guest management and role-based device authentication with or without relying on an 802.1X-managed supplicant on the device. NAC can identify and isolate rogue WAPs and provides network-based enrollment, on-access profile checks and network-based enforcement, which fortifies MDM-based device, user, data and application controls. NAC enforcement also supports WLAN reassignment.	Leverage NAC-related features with wireless network and MDM platforms in place in your organization. Through integration with MDM suites, automatically enforce controls on devices across the network that would be enforceable only by MDM across the cellular network. (An increasing number of MDM vendors offer NAC integration capability.)
8 Data Recovery Capability	Host-based backup protection software cannot always ensure that it is installed, running and up-to-date. NAC endpoint security policy can provide a complementary control to ensure such protection is active.	Configure NAC to automatically verify installation and run state of host-based backup and encryption software.

Critical Security Control	NAC Capability	Advice for Automation
11 Limitation and Control of Network Ports, Protocols, and Services	Role-based access control (RBAC) enforcement explicitly allows only trusted network traffic using valid protocols to cross through ports and services that are approved as per policy. NAC complements endpoint protection to ensure that host-based firewalls and filtering tools are installed and running.	Enable NAC to restrict network traffic to known devices and valid profiles based on device, configuration and role. Use NAC to identify and eliminate unapproved protocols, ports and services on devices requesting access and post-admission to the network. Enforcement can range from alerting to limiting or blocking access.
13 Boundary Defense	NAC can identify users and devices connecting remotely, such as devices gaining access via VPN and that are in need of configuration, patching or software update.	Enable pre-admission NAC monitoring and defenses to take action on out-of-spec devices. Isolate, report and remediate automatically. Integrate NAC as much as possible with other event correlation sources, including firewalls, SIEM systems and VPNs.
14 Maintenance, Monitoring, and Analysis of Audit Logs	NAC can verify, activate and update logging applications, services and settings on endpoints. Beyond NAC events being sent to logging systems, NAC can also send endpoint configuration details to SIEM platforms.	Configure NAC to integrate with the current logging or SIEM platform. Enable NAC profile check to verify and remediate endpoint logging. Determine if and where SIEM can leverage NAC endpoint mitigation capabilities.
15 Controlled Access Based on the Need to Know	NAC can fortify and enforce role-based access control leveraging directory services and VLAN network segmentation. NAC can also assure the installation and use of host-based DLP tools.	Phase in NAC enforcement controls and enforce the use of DLP client software. Integrate NAC with DLP tools as they become active to include the status of these DLP tools during endpoint scans.
17 Data Loss Prevention	NAC can assure the installation and use of host-based DLP security on the endpoint.	Phase in NAC enforcement controls and enforce the use of DLP client software and the use of storage peripherals.

Table 1. How the Critical Security Controls Correspond to NAC and Where to Automate

See Appendix A for more detail and further examples of CSC enforcement with NAC.

Real-World Examples of NAC as Applied to the Critical Security Controls

Although implementing the entire set of CSCs at once is certainly a daunting prospect, many IT organizations have found success by implementing the CSCs in stages, or by focusing on key applications or areas of greatest risk. The following case studies of two such businesses show the value of NAC in day-to-day use.

Using NAC to Gain Real-Time Endpoint Visibility and Control

A Midwestern financial services company with more than 250 employees, 15 locations and a few thousand devices on its network wanted to improve IT security effectiveness as part of its claim to best-in-class banking services. The new CISO examined some common GRC frameworks and felt that the CSCs provided impactful, measurable and easily communicated "essential guidance and clear recommendations."[6]

His team reviewed which tools they could use to support the CSCs beyond the obvious ones contained in firewall, VPN and other host-based security systems. Ultimately, the CISO concluded that NAC would be able to provide the company with a more dynamic view of its network and assure the use of stronger access and endpoint configuration controls than would be otherwise possible.

Key considerations for the NAC implementation were ease of use and deployment, flexible policies, agentless device inspection and nondisruptive operation.

"In banking, we have a lot of thin clients and embedded devices," explains the CISO. "The use of agents could adversely impact performance and service delivery, and generally speaking, managing agents or exceptions for all devices adds administrative costs."

The deployment was straightforward, and the results were impressive. The implementation of NAC provided the CISO and his team with:

- **Full detail of all devices on the network in one view (Critical Control 1: Inventory of Authorized and Unauthorized Devices)**
- **Visibility into the state of those devices (Critical Control 2: Inventory of Software, Critical Control 3: Secure Configurations for Mobile Devices and Critical Control 4: Continuous Vulnerability Assessment)**
- **Achievement of a ground-level view of the scope of policy violations (Critical Control 7: Wireless Device Control and Critical Control 11: Limitation and Control of Network Ports and Services)**
- **Capability to prioritize and short-list potential rogue devices (Critical Control 1: Inventory of Unauthorized Devices and Critical Control 13: Boundary Defense)**

With the added visibility, the team could identify which devices were valid and approved, as opposed to older and unmanaged devices. They configured the NAC system to allow managed and secure devices to use a production or guest network, while certain new devices were classified, assessed and possibly flagged—automatically reassigned to a quarantine network for remediation.

The NAC's agentless and flexible nature supported device discovery and roles-based enforcement policies, thus satisfying the IT team's operating requisite. For added benefit, the company integrated NAC with its e-GRC and VA platforms. NAC-based device location and configuration detail also facilitated the company's help desk ticketing and troubleshooting processes.

"NAC allowed us to more readily track assets, see possible issues and address potential violations—a huge game changer for us," says the CISO. "We automated the management of endpoints and created reports and audit trails, which saved us hundreds of man-hours."

---

6 Quotes in this case study are from an e-mail to the author.

Enabling Better Patient Care Through Flexibility of Device Management, Without Sacrificing Essential Patient Data Protections

The IT staff at a large medical facility in the U.S. had employed NAC to monitor and control all network devices and to facilitate guest management. The NAC system classified behavior, monitored policy compliance and enforced security of hospital-issued systems and devices, including onsite and remote personal computers used by employees and authorized non-employee physicians. NAC also enabled the health care provider to monitor networked health care equipment, such as medicine dispensers, emergency case kiosks and video surveillance cameras.

The IT staff noticed that doctors and researchers were attempting to connect personal smartphones and tablets to the hospital network, in spite of existing policy prohibiting such devices. Management recognized that a ban on BYOD was untenable, given the popularity and proliferation of devices, and that a secured BYOD program held the possibility for increased productivity and better patient care.

To seek a balance between security and mobility, the project team investigated NAC as well as MDM solutions—ultimately integrating the two to ensure that allowing personally-owned devices did not introduce any additional risk to protected patient information. The implementation allowed the organization to use MDM with NAC to:

- **Enforce password and encryption standards (Critical Control 17: Data Loss Prevention)**
- **Limit access of jail-broken devices (Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices)**
- **Restrict applications such as screen captures or cameras deemed to be high risk (Critical Control 6: Application Software Security)**
- **Report device access attempts and block or remediate as appropriate. Manage access by devices with or without agents (Critical Control 1: Inventory of Authorized and Unauthorized Devices)**

Although MDM offered some level of device, application and data control over devices, in some cases, the level of security would be too strong for adoption by those who were not employees of the hospital. In addition, MDM lacked network-based enrollment, assessment and enforcement capabilities for managing mobile devices that would require network access. NAC provided the visibility the IT department needed for all endpoints, not just those with MDM agents. NAC can check antivirus and device configurations without an agent, and block devices until features and services such as cloud storage or Bluetooth are disabled.

By leveraging NAC and MDM platforms, the health care facility reduced the risk of allowing personally-owned devices to acceptable levels based on device and role, prevented data loss and established central management of the BYOD program—all without the need to increase helpdesk staffing.

Conclusion

NAC has evolved from a straightforward admission control tool to a robust set of security capabilities that map to a number of the Critical Security Controls. Most importantly, it provides a consolidated capability that can enforce all of the first four CSCs, which are rated as "very high" in effect on attack mitigation by the NSA.[7] NAC can integrate with other toolsets—host-based agents, patch management systems, vulnerability scanners and others—to provide a robust capability that enhances enterprise network security.

NAC provides a number of ways to control network access from new and unknown devices while achieving the goal of automation that is the philosophy behind the CSCs (see Appendix A). Today's NAC meets many of the CSCs and integrates with MDM and other tools to manage risk and compliance around an increasing array of mobile endpoints. Expect ongoing improvements in the functionality and integration of NAC as it rises to the security challenges of modern borderless computing.

7 www.sans.org/critical-security-controls/winter-2012-poster.pdf

Appendix A: Enforcing the Critical Security Controls with NAC

This section provides more detail on the importance of particular CSCs and how each maps to NAC features and functions. Quotes in this appendix are from the CSC document and are taken from the explanation of the respective control.[8]

Critical Control 1: Inventory of Authorized and Unauthorized Devices

Understanding what exists in a network is a critical first step and "quick win" for organizations mapping to this control, which advises that organizations:

> ***Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s).***

NAC appliances can capture all requests for network resources and can "fingerprint" a device using a variety of methods in order to classify and assess all endpoint information regarding what is connected to the network. An agentless NAC approach can compile detailed information on all discovered devices—not just those with an agent. Specifically, NAC meets the visibility/attribution element of Critical Control 1:

> ***Maintain an asset inventory of all systems connected to the network and the network devices themselves ...***

NAC systems can maintain a database of virtually the entire range of network devices referenced in the CSCs. In fact, the Critical Control 1 requirement *specifically* lists NAC as a means to achieve this goal (see Figure 2):

> ***Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.***

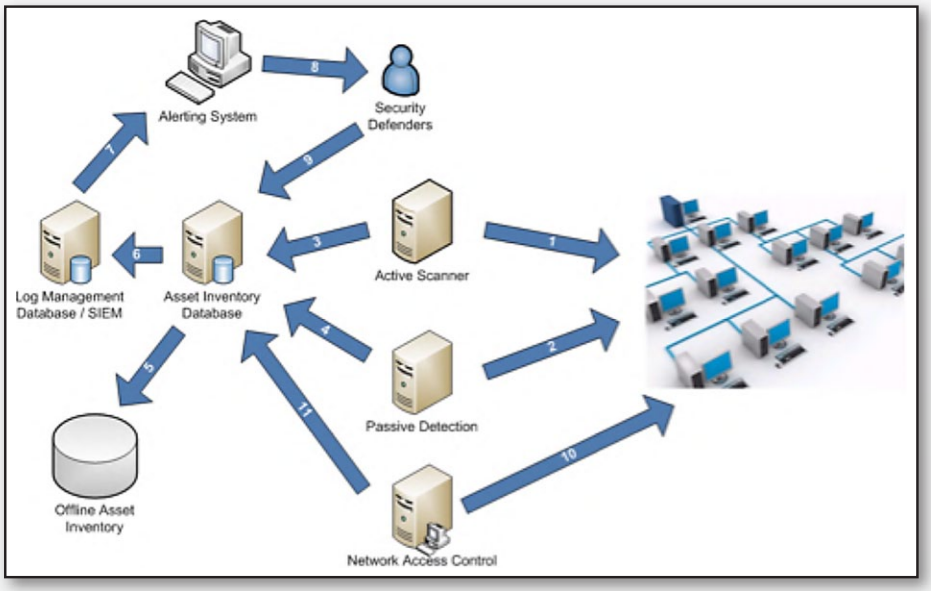

Figure 2. How Network Access Control Helps Accomplish Critical Control 1 (taken from the CSC document)

8 "Critical Controls for Effective Cyber Defense: Version 4.1"; www.sans.org/critical-security-controls/cag4-1.pdf

9 "Critical Controls for Effective Cyber Defense: Version 4.1," page 10.

Critical Control 2: Inventory of Authorized and Unauthorized Software

Applications pose their own set of risks, particularly on mobile devices. The two quick wins for Critical Control 2 are:

> *Devise a list of authorized software that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be tied to file integrity checking software to validate that the software has not been modified.*

> *Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system.*

With a centralized database of approved software, NAC provides a means to accomplish both of these quick wins. NAC can also identify any applications that are not authorized, accomplishing the Critical Control 2 configuration/hygiene directive of:

> *The software inventory tool should also monitor for unauthorized software installed on each machine.*

If NAC detects unauthorized software on the device, it can take one of many actions, including alerting, trouble ticketing, sandboxing the system or attempting remediation.

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Secure configurations are standardized, hardened versions of operating systems and installed applications. Some sources for these templates include the National Institute of Standards and Technology (NIST), National Security Agency (NSA), Defense Information Systems Agency (DISA) and the Center for Internet Security (CIS). Of course, NAC does not generate these configurations, but by taking advantage of NAC device fingerprinting processes, it can be used to identify the presence of key components of a configuration template.

NAC systems can detect if patches, host-based protection and applications are installed and current and which applications are running, and can also detect other hardware and operating states of the endpoint. They can often share this information with other configuration- or event-management systems. If desired, NAC systems can inform ticketing and systems management applications on any configuration violation or take direct action to remediate the endpoint configuration issue.

NAC can also support emergency patch deployment on device access or validate system changes. Because NAC tools can integrate with existing security and systems management agents, as well as configuration management systems used in today's enterprises, NAC can ensure that management agents are installed and active and that configurations are up-to-date. The combination of endpoint compliance capabilities enforces the Critical Control 3 configuration/hygiene requirements:

Implement automated patching tools and processes that ensure security patches are installed within 48 hours of their release for both applications and for operating system software.

Utilize application white listing to control and manage any configuration changes to the software running on the system.

Implement and test an automated configuration monitoring system that measures all secure configuration elements that can be measured through remote testing ...

Either before or during a device's admission to the network, NAC can identify key elements that comprise a secure configuration state. If there is a problem, NAC can simply issue trouble tickets, direct the system owner to a remediation point before allowing access, segregate the user session from the rest of the network, attempt to fix the issue or take other actions.

Critical Control 4: Continuous Vulnerability Assessment and Remediation

In 2010, the U.S. government changed its network compliance approach from periodic assessments to continuous monitoring.[10] "Continuous" in this sense doesn't necessarily mean 24–7; instead, it means recurring assessments at an interval commensurate with the value of the information and the estimated level of risk. Federal publications[11] provide guidelines for determining the periodicity of assessment, based on criteria such as security control volatility, system impact levels, criticality of function protected and identified weaknesses.

Note that Critical Control 4 has a two-part requirement: *assessment* and *remediation*. In terms of assessment, the first Critical Control 4 quick win is:

Run automated vulnerability scanning tools against all systems on their networks on a weekly or more frequent basis ...

10 www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf

11 NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.

Next-generation NAC systems can check for key security settings and applications on an endpoint, as already described. Should one of these key security elements—a patch, antimalware, encryption, data leakage prevention or host-IPS—not be installed or be inactive, NAC can take action. Furthermore, NAC can integrate with existing vulnerability assessment suites and inform the vulnerability scanners that a new system is on the network and should be scanned, or enable the vulnerability scanner to trigger an action of the NAC. The combination of NAC and vulnerability assessment helps enforce stated tuning requirements:

Tune vulnerability scanning tools to compare services that are listening on each machine against a list of authorized services.

NAC can not only act in real time to identify key security or patch issues, but also can be coordinated with VA to enforce security policies and remediate systems based upon the results of scans. NAC's flexibility enables security managers to meet and exceed the Critical Control 4 configuration/hygiene directives:

Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis ...

Any vulnerability identified should be remediated in a timely manner, with critical vulnerabilities fixed within 48 hours.

Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe.

Critical Control 5: Malware Defenses

Critical Control 5 offers three quick wins relevant to the protection NAC offers:

Employ automated tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality.

Employ anti-malware software and signature auto-update features or have administrators manually push updates to all machines on a daily basis.

Limit use of external devices to those that have business need. Monitor for use and attempted use of external devices.

NAC integrates with host-based endpoint protection tools and can ensure that antimalware defenses are present, updated and operating before devices are permitted network access, and can revalidate this assessment to ensure that devices that fall out of compliance are either remediated or removed from access. Most NAC solutions integrate with the majority of antimalware vendors; such NAC systems can not only discover and report on host-based malware tool issues, but also can be tuned to install, re-activate, update and change the configuration of antimalware software and agents.

Furthermore, NAC solutions that offer post-admission behavior monitoring on endpoints can also detect when a device is exhibiting malicious behavior, such as a propagating worm or network polling, or when a device begins to act in a manner inconsistent with its permitted profile, such as a printer now communicating as a Windows system. Depending on established policy, NAC can inform IT or automatically isolate the offending device from the network—often stopping attacks or the spread of zero-day threats potentially before significant impact. This helps enforce the visibility/attribution requirement:

Ensure that automated monitoring tools use behavior-based anomaly detection to complement and enhance traditional signature-based detection.

Critical Control 7: Wireless Device Control

Enterprise mobility and wireless networks materially affect IT organizations. Critical Control 7 offers a number of quick wins that NAC addresses well, including:

Ensure that each wireless device connected to the network matches an authorized configuration and security profile ...

Ensure that all wireless access points are manageable using enterprise management tools.

Unauthorized (i.e., rogue) access points should be deactivated.

NAC complements wireless security controls with guest management, device authentication, WLAN reassignment and broader role-based access control features. With NAC, wireless users can be placed in a captive portal where, as determined by the user or device identity, device and authentication attributes can be assessed against policy to determine what wireless LAN and network resources should be made available.

The most advanced NAC suites are compatible with MDM solutions, representing a cost-effective means of maintaining devices (both company- and employee-owned) that may not regularly connect directly to the corporate network. NAC complements MDM security controls, as MDM tools work only on mobile devices that are formally under MDM management. NAC can facilitate policy-based enrollment versus user self-provisioning. Although MDM security controls cover the device, user, application and data, they do not extend to network security. NAC systems can be set to trigger an MDM security profile check on network admission and can be used to monitor and remove a mobile device from the network.

NAC addresses additional elements of Critical Control 7:

> ***Use [802.1X] to control which devices are allowed to connect to the wireless network.***
>
> ***Register all mobile devices, including [personal] devices, prior to connecting to the wireless network. All registered devices must be scanned and follow the corporate policy for host hardening and configuration management.***

Through wireless device control, beyond a simple go/no-go decision, NAC can provide granular controls, and based upon the assessment of the device, can *respond* dynamically by imposing restrictions on what resources or services are accessible. As already described, finding an advanced NAC that integrates with MDM (not all do) offers a tremendous advantage for securing enterprise mobility.

Critical Control 8: Data Recovery Capability

Attacks frequently result in changes to system configuration and software. Even the most careful efforts to restore compromised systems can inadvertently reintroduce malware, because system backups will contain code that has been present for longer than the backup media cycle time. For example, if an organization performs weekly backups and keeps four generations, malware that has been present for more than a month could be restored along with valid applications.

A compromise of network data recovery capabilities would make it impossible to achieve the quick win:

> ***Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software and data on a machine should each be included in the overall backup procedure.***

Tools that provide integrity checking in the form of checksums and digital signatures of valid code are, with backup and recovery tools, among the highest-value targets for attackers. Typically, an attacker would shut down these processes or services in an attempt to avoid detection. NAC endpoint security policy can provide a complementary control to ensure such protection is active, by automatically verifying installation and operation of host-based backup and encryption software, and sending a real-time alert if attackers stop or tamper with these processes.

Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services

As a core capability, NAC offers the capability to provide controls on physical network ports based on device configuration and security profile using role-based enforcement. Essentially, users must be authenticated before being granted network access, or NAC won't "unlock" the associated port on the switch (or similar device).

NAC facilitates limitation and control of network ports by complementing network authentication and authorization with more granular, role-based device level controls—including port assessment and deeper device inspection on network access request—limiting access to network resources according to policy. This prevents rogue, insecure or misconfigured devices from entering a network, without requiring intervention in terms of guest management, notification of IT or logging systems, or user-guided or automated remediation. NAC-based enforcement includes WLAN and VLAN reassignment, ACL modification and a variety of other mechanisms. NAC solutions that provide post-admission device monitoring help maintain port-level control. This capability helps enforce the Critical Control 11 quick wins:

Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.

Keep all services up to date and uninstall and remove any unnecessary components from the system.

NAC systems can identify and report issues, as well as block ports. NAC itself is not usually the vehicle to remove undesired applications; however, it does have the capability to do so.

Critical Control 13: Boundary Defense

Many VPN concentrators integrate with NAC suites in the same way a system might, by plugging into the internal network. This capability helps enforce the Critical Control 13 configuration/hygiene recommendation:

All devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels.

Although it seems for networks today that the perimeter no longer exists, the reality is that boundaries between networks remain, even if sometimes loosely defined. The most important boundaries are those between different trust levels—high to low, sensitive to public, and internal to external. NAC helps interdict this type of traffic, enforcing the Critical Control 13 quick win:

Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (white lists).

Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs

In the event of a successful attack, audit logs can help establish the extent of the damage and quantify the losses, or help identify the source of the attack. When attackers can change the logs themselves, they can conceivably erase all traces of their presence, making intrusion detection and damage assessment nearly impossible.

Through its capability to control every network access attempt and provide a record of that event, NAC can help achieve the quick win:

Verbosely log all remote access to a network, whether to the DMZ or the internal network (i.e., VPN, dial-up, or other mechanism).

In addition, NAC can verify, activate and update logging applications, services and settings on endpoints. Beyond NAC events being sent to logging systems, NAC can also send endpoint configuration details to SIEM platforms, providing centralized consolidation of all network access records, as well as evidence of actions of interest.

By configuring NAC systems to integrate with current logging or SIEM platforms, NAC can provide critical input to immediately identify when hostile access attempts occur or even when applications that perform logging are taken offline in an attack. NAC offers the capability to check user and device profiles to verify endpoint-logging processes are in place and remediate if necessary. These NAC-driven endpoint mitigation capabilities can leverage the functionality and utility of many SIEM platforms.

Critical Control 15: Controlled Access Based on the Need to Know

Limiting the interaction between people, computers and applications with information is best done by exception, but applying exceptions individually in an organization with hundreds of employees is complex enough; it simply can't be done in larger user pools. This is where role-based access control (RBAC) comes to the rescue.

Typically, a user will have a profile of permissible actions that relates to his or her role in the organization. For example, an accountant might be permitted access to financial records, but not software development libraries, whereas software developers who can modify code in the test environment are not allowed to make changes in the production environment. In both cases, RBAC constrains user behavior based on the user's "need to know."

NAC can fortify and enforce RBAC by leveraging directory services and VLAN network segmentation. This helps achieve the quick win:

Locate any sensitive information on separated VLANs with proper firewall filtering.

In addition, the logging capabilities of NAC (and its capability to integrate with SIEM platforms) offer support for the visibility/attribution goal:

Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.

NAC can also assure the installation and use of host-based DLP security. This helps achieve the advanced goal:

Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server.

By phasing in NAC enforcement controls and enforcing the use of DLP client software, NAC can be integrated with DLP tools as they become active, to include the monitoring and reporting on the status of these DLP tools during endpoint scans.

Critical Control 17: Data Loss Prevention

Information often represents the lifeblood of a modern organization. Although typically enterprises filter inbound information using tools including firewalls, spam filters and malware detection, many fail to check *outbound* information with the same level of diligence. As a result, information can be exfiltrated out of an enterprise, resulting in compromise of trade secrets, intellectual property and even classified information. Key to enforcing this is the use of DLP tools and software. Such tools provide a means of accomplishing the visibility/attribution objective:

Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.

It also accomplishes the configuration/hygiene objective:

Use network-based DLP solutions to monitor and control the flow of data within the network.

NAC is critical to the effective use of host-based DLP endpoint security by monitoring and verifying the presence, integrity and operation of such tools. The real-time reporting and alerting features of NAC platforms can indicate that an attacker has attempted (or succeeded) in disabling or inactivating a DLP client, and can initiate the automatic disconnection of a compromised endpoint until the affected system can be brought back to a suitable state.

About the Author

G. Mark Hardy is president of National Security Corporation. He has provided cybersecurity expertise to government, military and commercial clients for more than 25 years and is the author of more than 100 articles and presentations. He serves on the National Science Foundation's CyberWATCH Advisory Board and is a retired U. S. Navy captain. A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Master of Business Administration and a Master of Strategic Studies, and he holds the GIAC Security Leader Certification (GSLC), Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) credentials.

SANS would like to thank its sponsor:

Last Updated: December 11th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS Cyber Defense Initiative 2017	OnlineDCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced