Interested in learning more about security?

SANS Institute InfoSec Reading Room

Your Pad or Mine? Enabling Secure Personal and Mobile Device Use On Your Network

Sponsored by ForeScout Technologies, Inc.

"Your Pad or Mine?"

Enabling Secure Personal and Mobile Device Use On Your Network

Essentials on Applying NAC to Secure Guest Networking, CYOD (Choose Your Own Device), BYOD (Bring Your Own Device) and Endpoint Compliance

2nd Edition, Updated May 2013

A SANS Whitepaper

Introduction

Many of today's endpoints are neither known nor protected. According to Gartner, enterprises are aware of only 80 percent of the devices on their networks.[1] Those 20 percent of unknown devices are inside the perimeter of the network, are unmanaged and provide users with access. They are small, varied and highly mobile, and they are loaded with their own applications, can act as WAPs, and often contain outdated firmware or are easily jailbroken. Even as the devices are accessing personal applications on the web, they are also accessing corporate resources such as e-mail—all from the very same unmanaged devices, which have not been vetted by the security organization. Smartphones, notebooks, netbooks, iPads, e-readers, personal Wi-Fi and more—the list of personal devices attempting access to employer networks seems to grow every day in what's come to be known as the IT consumerization era of network computing.

Gartner predicts by 2017, half of employers will require employees to supply their own devices for work purposes.[2] IT consumerization has disrupted conventional IT endpoint security, whether the selection of smart mobile devices are corporate provided, as in CYOD (choose your own device), or owned by the employee, as in BYOD (bring your own device). While this level of ubiquitous access produces gains in workforce productivity, it also represents new layers of risk for which traditional endpoint controls are unsuitable. As such, Gartner predicts that by 2013, 80 percent of organizations with BYOD policies will see botnet compromises increase by 100 percent inside their networks.[3]

Because the mobile OS platform versions and features widely vary, they pose various risks—especially when the OS is rooted. Not to mention, the limited processing capacity of devices makes it difficult to support an arsenal of security apps hosted on the devices. Intrusions and exploits are occurring through many means, including users browsing malicious sites, clicking malicious links in e-mail and SMS messages, and installing malicious applications, jailbroken rootkits[4] and Wi-Fi connections. One has only to review the ontology of Shady RAT[5] to appreciate the impact that one user and one bad e-mail can have on your enterprise.

With the introduction of BYOD, CYOD and these associated new threat vectors, network access control (NAC) has emerged as an important solution for mitigating the risks of IT consumerization.[6] NAC can be used to provide secure guest networking services and management to these devices. This paper discusses policies and approaches for using NAC to support guest networking and BYOD to complement and enable other mobile security controls such as Mobile Device Management (MDM).

---

1 Strategic Roadmap for Network Access Control," Gartner, October 2011, by Lawrence Orans and John Pescatore, www.arubanetworks.com/pdf/Gartner-Roadmap-for-NAC.pdf

2 Bring Your Own Device: The Facts and the Future," Gartner, May 2013 by David Willis, www.gartner.com/newsroom/id/2466615

3 "Predicts 2011: Infrastructure Protection Is Becoming More Complex, More Difficult and More Business-Critical Than Ever," Gartner, November 2010, by Avivah Littan, Neil MacDonald, John Girard and Ray Wagner

4 www.wired.com/threatlevel/2011/03/android-malware/

5 www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

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

Building Guest Networking, BYOD and Endpoint Security Policies

Developed as a response to deficiencies in Wi-Fi protocols, NAC's original function was to pass user and device credentials to a policy control point, where permission to connect to the network was approved and sent back to the policy control point to allow or deny device access. With NAC, organizations can identify and apply security policy to all types of users and network devices attempting to access network resources, whether they are wired or wireless, PC or mobile, managed or unmanaged.

In particular, NAC enables guest networking for wired and Wi-Fi access requests coming from endpoints that don't fall within the realm of what the network considers "normal." A good and current use case would be unmanaged personal mobile devices. NAC enables employee, contractor and visitor choice by moving the control to where and when the endpoint connects to the network, acting as the port of entry for that endpoint. By using NAC at the port of entry, a device is assessed before it's allowed access. The check attests to the level of trust associated with the device, location, user or user type requesting access.

NAC's capacity to classify network users and their devices gives the enterprise greater choices regarding how they're going to treat new devices as the industry pumps them out. Instead of making decisions on a case-by-case basis, the enterprise can now set NAC policy that states what kinds of devices can be used and what respective security policies must be in place on a device if an employee or guest wants to connect a personal device to the enterprise network for work-related applications and resources. Depending on the device, NAC can be leveraged to ensure that the endpoint has the latest updates, working host-based protection, approved applications, and more. The following example shows how NAC is leveraged to support BYOD.

Case Study 1: Municipality Supports BYOD with Guest Networking

A Canadian municipality supporting a community of more than 110,000 constituents needed to enable the BYOD needs of its 2,000 city workers, while at the same time meet Payment Card Industry Data Security Standards (PCI-DSS) and Health Insurance Portability and Accountability Act (HIPAA) regulatory compliance. The city assembled a cross-organizational team to assess NAC solutions against its requirements, including the following:

- **Visibility into all devices and the status of devices accessing the network**
- **Visibility into all updates—including Windows update status**
- **Simplified guest networking through self-serve policies**
- **Means to enable noncorporate device use on guest networks**
- **Self-remediation and user education**
- **Accuracy, speed and automation**

Using NAC, the organization now has full visibility into roles-based access and other activities from endpoints, giving it the ability to classify device types entering the network and segregate resource access based on user and device profiles. The NAC implementation provided end-to-end guest networking, which integrated into the organization's wireless network, enabling city workers, contractors and VIPs to self-register and use their personal devices in courtyards, the lunchroom and other designated areas without direct access to rest of the network.

Automating the process of guest networking also provided a secondary benefit of better accuracy and cost savings. This process was managed manually before, with no guarantee the devices accessing the servers were safe, and administrators had to remember to manually disable the guest port. The self-help features for guest networking also significantly reduced help desk costs associated with requests for manually established new connections.

Plan in Phases

Prior to implementation, NAC requirements need to be in order. At the beginning of the implementation phase, resource requirements, budget, procurement and activation schedule are the drivers. Functionality and policy compliance become more important as the project enters the operational phase. After deployment, policy-compliance metrics and tuning tend to dominate the discussion.

When it comes to policy, consider the following before and during deployment:

- NAC policy begins with assessment-of-use case scenarios: What types of devices are being brought in by employees (or should employees be provided), how to handle contractors and guests; what operating state and types of applications can and should be allowed; what security provisions must be in place; and, when, where and what access will be granted, denied or limited?
- Once users and devices accessing the network are understood, use NAC policy to determine who and what devices to allow on the network, what applications the devices should or should not be running, and the security state they should be at before any access is granted.
- Policy and procedures should also include exception management, the process for guest registration and authorization, and how to handle issues.

Between these policy layers are additional subtleties to consider:

- What do you do with a corporate device that no longer complies with the corporate policy?
- What is the process for guest authorization and management?
- How can you automate or semi-automate mitigation and remediation actions?
- How do you convey and capture acceptable use for policy creation?
- What do you do with devices not owned by the corporation?

NAC capabilities can address these and other questions, which should all be considered at the onset of a NAC deployment project.

Determine Prerequisites for Granting Access

After you gather and assess the information on device usage, you can make an informed decision regarding how the device should be allowed to connect. Full, partial or guest access can be granted based on the assigned level of trust. Trust is based on the device's compliance with many policy questions: Is the device owner known (for example, user authenticated or company owned)? Does the device have the requisite security controls, such as antivirus, firewalls, VPN, encryption, data leakage and strong authentication, which you may require prior to allowing access to critical enterprise resources? In many cases, legacy and noncorporate devices may not have some of these controls available, but that is part of the decision process.

After you decide on the required controls, you can move on to making decisions concerning the existence of forbidden or high-risk applications. For example, is the endpoint running an unwanted application that can create an unauthorized communication channel or share files? Are there peripheral devices being used on the endpoint that may pose a data leakage or other threat?

Scale Your Policy Actions

The policy should also be able to scale to include new forms of mobile devices requesting access as users continue the trend toward BYOD. A policy could be as simple as putting all devices on a guest network until the user and device have been authenticated, possibly only allowing VPN access. To keep policy simple, some organizations may allow only certain laptops, smartphones or tablets to connect to their networks. Ultimately, however, personnel use most personal mobile devices regardless of IT acceptance, so the device use needs to be accommodated. For example, perhaps Apple and Android devices should be granted access only to a segregated guest network that allows Internet access. For more fine-grained access controls, users and their endpoints are authenticated through Active Directory, where group assignments and other entitlements can be provisioned. NAC can be used to enable device authentication and endpoint configuration policy.

After a level of trust is associated with an endpoint, NAC can support a broad range of access and endpoint compliance actions, including: port control, guest management, remediation or denial of access (a last resort due to its potential impact on productivity). For example, if a system is contractor owned, the policy would enable restricted enterprise access only after it passes a security check. If that check reveals that policies are not met, the device requesting access can be sent to a remediation VLAN, from which the user can remediate or, possibly, consent for the NAC to auto-remediate as possible.

Many organizations require employees and contractors to load some standard or company-specific security controls onto their endpoints. Connection time is a perfect opportunity to verify not only compliance with policy, but also enforcement of any agreements made between the parties during a connection. These controls could ensure that the cellular network connection is turned off prior to connecting to the corporate network or that the smartphone or tablet is using a prescribed MDM application.

If the system is employer owned and controlled, policy might include to what network segments, resources and respective applications the device is allowed to connect. For example, why would a developer's notebook connect to your finance network? Another example might be restricting endpoints within health care administration from being able to use external mobile storage peripherals, such as USB drives. Although security control capabilities vary, the capability to enforce these levels of action is critical as more and different types of devices connect to the network.

Have a Remediation Plan

NAC policy should also include conditions under which remediation is required, such as when there is a policy violation involving an unknown device or endpoint exhibiting unwanted behavior. Remediation can include:

- Blocking or removing the unknown or malicious device from the network
- Reassigning the device to a different and often segregated network (such as a quarantine network)
- Installing, updating or activating software applications or services on the endpoint
- Initiating enrollment into a security control such as MDM
- Blocking the use of certain applications and peripherals
- Shutting down an endpoint completely

Policy should be mutually agreed upon by security and network operations to cover when remediation is appropriate, what remediation choices are available, and how to track violations and remediation events. Integrating a solution with your SIEM (security information event management) and trouble-ticket system can help you understand the scope of violations, why devices are being remediated, and where to refine your policy for improved overall security, compliance and user experience.

Architectural Challenges and Considerations

A well-planned system can also provide remediation processes and support visibility and governance of access from multiple types of devices. However, there will still be challenges to which the following advice applies:

- Understand your legacy networking capability and your ability to adapt to new forms of access and the NAC solution:
  - Determine whether the present network infrastructure is robust enough to support the bandwidth and authentication demands presented by the influx of mobile devices.
  - Keep in mind that everything is connected. Take the time to find and analyze those connections.
- Understand where your business-sensitive and regulated data exists, as well as who should have access to this data and under what conditions access should be granted.
- Support protocols beyond 802.1X in the authentication process.
- Involve business units, such as support, legal, developers, architects, users and other stakeholders, with development, implementation and ongoing user education.
- Leverage directory services to enable roles-based policy assessment and enforcement.
- Keep polices well-defined and up to date, because device uses and applications continue to evolve.
- Automate. You are about to introduce a very large amount of decision-critical information that must be collected, assessed and acted upon far faster than any human mind can comprehend.
- Supply consumable management metrics. If your telemetry says that 9 percent of your guests are really employees with noncompliant devices, what does that mean for productivity, and what will it cost to fix it?
- Phase in policy enforcement while phasing out noncompliant devices. Start by granting BYOD access only to the guest network and only with specific device types. As capability improves, migrate more compliant guests to internal networks and so on.
- Include remediation! Make sure it works, it's painless and that you can get reliable direction from the NAC system.
- Integrate where possible. Technology should never stand on its own, so enable a flexible system that integrates and correlates well with other controls for detection, security event management, vulnerability management, forensics and optimization.

The following case study shows how a health care IT organization used NAC to help classify and inventory all systems and monitor BYOD policy.

Case Study 2: Securing Personal and Mobile Device Use for Better Patient Care

IT staff at a large medical facility in the U.S. had employed NAC to monitor and control its network devices and to facilitate guest management. The NAC system classified systems and users, monitored policy and enforced security of hospital-issued systems and devices (as well as 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 that prohibited such devices. Management recognized that a ban on BYOD was untenable, given the popularity and proliferation of devices. It ruled 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**
- **Limit access of jailbroken devices**
- **Restrict applications such as screen captures, recording or unauthorized IM**
- **Report device access attempts and block or remediate as appropriate**
- **Manage access by devices with or without agents**

In some cases, the level of security provided by MDM would be too strong for adoption by those who were not employees of the hospital. NAC provided the appropriate level of visibility and control that the IT department could more easily apply and manage. By leveraging NAC and MDM platforms, the health care facility reduced the risk 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.

Access and Endpoint Security: Agent, Agentless or Hybrid?

NAC architectures include network, client and hybrid (agent and network) controls for assessing endpoints and establishing access based on results of those assessments. Policy depends on a number of questions:

- Should you rely on the network to make all the decisions?
- Can you offload manual policy enforcement onto trusted endpoints?
- To what extent is it necessary to determine if an endpoint is trusted?
- How can you monitor and enforce policy, and tie into existing access control structures?
- Under what conditions is it difficult or impossible to manage or support agents?
- How can you support and secure personal and mobile device use in the workplace?

Ultimately, to achieve a comprehensive and flexible level of endpoint control and guest networking, organizations will use a combined network, agent and or agentless approach, which is examined next.

NAC with Agents

Organizations with little control over the network devices, such as personal mobile devices, can still gain significant control of the endpoints by requiring the use of an agent at the endpoint as users request access. Agents can be persistent or nonpersistent (meaning they are placed on the endpoint during each session request). An active agent on an endpoint can assess the status of the endpoint, gather information, report, take action based on instructions provided by a management server and, most importantly, take proactive steps to ensure that the endpoint remains compliant with pertinent security policies.

Agentless NAC

In network-based NAC, requests for access associated with specific devices are routed, switched or relegated to the bit bucket based on rules enforced by network infrastructure devices as discussed previously. You can also employ VLAN capability in a NAC architecture in order to provide security segmentation. By assigning guest devices to a separate VLAN, you can put untrustworthy devices in a network that does not have access to the corporate network. In some advanced cases, you can use dynamic VLANs to stratify traffic based on user, data or resource sensitivity.

Other networking methods, such as the use of DHCP (Dynamic Host Configuration Protocol) and the ARP (Address Resolution Protocol), as well as Active ACL modification, TCP reset and other networking protocols, can support a NAC architecture and policy-based enforcement.

The following case study describes how a university uses agentless NAC to assess BYOD and managed devices, as well as enable guest networks even during peak use times.

Case Study 3: Facilitating the Higher Ed BYOD Explosion with Agentless NAC and Virtualization

School and higher education IT departments were the first organizations, by nature of the environment, to manage guest networking and BYOD policies. To protect against an ever-increasing number of Trojans, bots and other malware attempting to get into the network, the director of IT services and development at a prestigious college in the United Kingdom began a NAC overhaul in 2010. The system needed to regulate student network use and protect against malware emanating from any device attempting access into the network, not just internally managed computers.

The school was experiencing an explosion of mobile devices among the 1,000-member student body. Now, many students have three devices each, all used for accessing the network, including a smartphone, tablet and laptop. The campus must monitor 4,000 devices belonging to employees and students for guest-access compliance and violations. The campus also hosts open nights for parents and visitors to access school resources, during which up to 2,000 additional guest devices might attempt to access the network.

In this environment, a persistent agent solution wasn't practical on endpoints, so the director of IT services made the decision to go with an active scanning (agentless) solution to enforce policy from the network. The school was able to take advantage of its new NAC tool's built-in policy templates to address the diversity of the student population and the devices connecting to the network. Active scanning occurs against the devices wanting access. Those devices that don't meet policy are quarantined until they can be remediated. The system can also monitor for suspicious and unwanted post-connection behavior, for example, if one of the shared bank of printers begins to operate as a Windows machine or if a new personal rogue WAP connection appears.

With their NAC tool available as a virtual appliance, the organization leveraged the school's VMware investment to provide rapid NAC scalability for occasions such as parent night. Overall, the NAC platform provides a broad range of value: blocked insecure devices, eliminated most rogue traffic on the network, reduced unauthorized bandwidth consumption, reduced malware risks and more. Now, the IT organization can handle the ongoing need of its students, including guest networking for visitors and avoiding numerous security risks, all with lowered operating costs.

For those devices without agents, an intelligent scanning approach from the network is the first step in determining the security posture of the device requesting access. Detailed network scans of an endpoint can provide a wealth of information, including the type and number of services running and the type of operating system and processor installed. A network scan might reveal the presence of services that can provide more detailed information, such as the Windows Management Instrumentation (WMI), which itself can provide significant levels of detail with respect to system configuration, update and patch status, user information and security posture. The client scan, on the other hand, can provide more information—for example, what user is attached to the device, what applications are loaded, and verification of external scan and fingerprint information.

Hybrid

Whenever it is possible to implement, an agented response is the best choice because of the immediacy of authentication and information it can gather directly from the endpoint. If devices cannot support an agent, active scanning of the device from the network may be sufficient. The most practical and often implemented approach is the hybrid approach, which relies on either agent or agentless scanning techniques. Figure 1 depicts this hybrid approach from a networking standpoint.

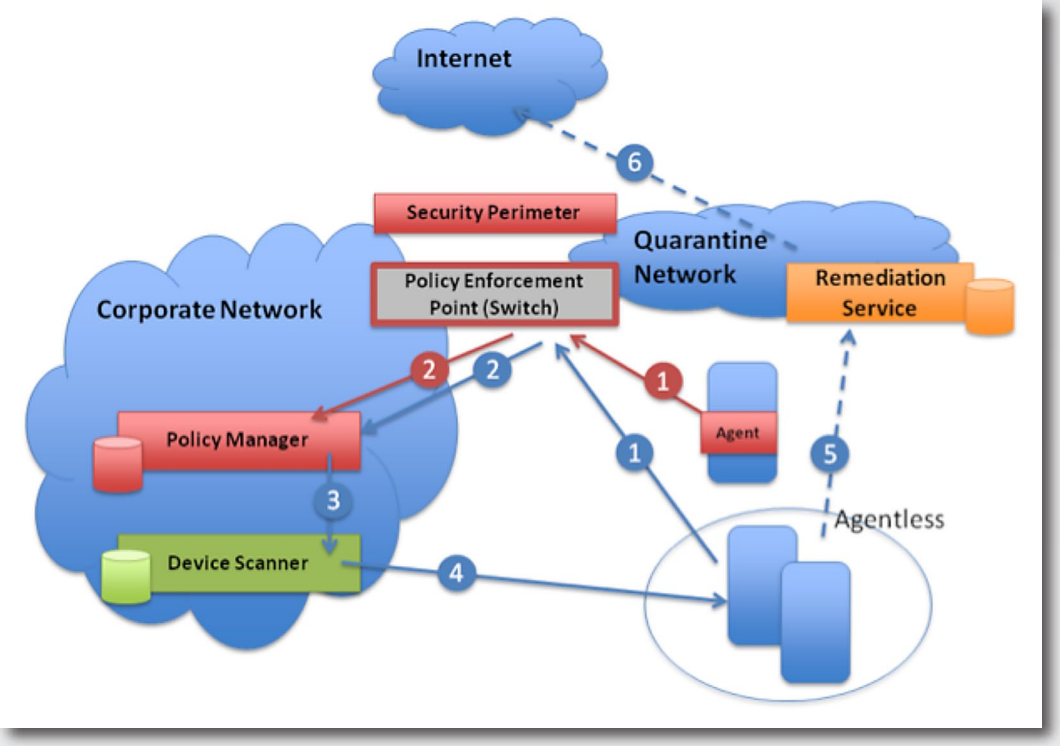

Figure 1. The Hybrid Approach

The NAC hybrid model provides the flexibility to cover the above architectural challenges and considerations and to more easily phase in policies to decide whether the presented system should be given full enterprise access, undergo remediation, be reassigned to a guest network or be denied access.

The NAC and MDM Control Combination

In order to enable users to use the devices they are most productive on, while enabling IT staff to reduce intrusion and data leakage risks, companies should consider a layered model that combines NAC and MDM. By employing NAC with MDM, organizations can achieve user, device, application data and network level protection while supporting a wider spectrum of security services appropriate to user type and risk level.

MDM is technology that allows IT organizations to better manage and address the risks of using corporate-provisioned and personal tablets and smartphones in the workplace. MDM provides lifecycle management of mobile devices, be they personal or corporate issued. An MDM system is comprised of a management server and an application on the mobile device that enables provisioning, user and device authentication, secure remote access, application management and data leakage protection. Advanced MDM platforms provide additional capabilities including containerization—the means to protect and segregate user and corporate data.

Complementary Controls

MDM needs a mechanism to trigger device enrollment, because MDM does not identify and assess unmanaged devices. NAC can identify smartphones and tablets at network connection and apply additional user authentication and device authorization controls to appropriately enroll and verify enrollment into MDM. An organization can establish an MDM security configuration profile used by the MDM server to scan a device frequently to check adherence—usually across longer intervals to preserve device battery life. You can use NAC to ensure that an MDM security check is initiated at network admission and to increase the frequency of checks while the device is on the network. If there is any security violation, the MDM can remove applications and data from the device. However, NAC can remove the device from the network, as well as quarantine the device and allow the user to re-establish a connection once the device becomes compliant. These are a few examples of using NAC and MDM security mechanisms to fortify BYOD and CYOD controls.

Case Study 4: Employing NAC and MDM for BYOD and CYOD in Financial Services

A financial services company with more than 100,000 endpoint devices across 200 locations had instituted NAC for the guest management and policy-enforcement of conventional Windows, MAC and UNIX personal computers. The organization had demand from business units to support personal mobile device use and to build out corporate mobile applications.

By defining discrete BYOD use cases, the company's IT staff reduced the risk of this enterprise extension. First, the company required all users with personal mobile devices to go through an automated registration process managed through the NAC system. Visitors were put on a segregated guest network with Internet-only access. Depending on the device type and user, NAC would employ different control mechanisms.

Those employees with personal smartphones and tablets, as determined through NAC device assessment and a guest registration process that integrated with directory services for employee authentication, would be allowed network access when the device was under MDM management. NAC facilitates MDM installation and on-access verification of security controls. MDM ensures device level controls such as prohibiting rooted or jailbroken device use and required applications.

Those employees with Windows or Macintosh systems would undergo a similar process, which would be fully managed by NAC. With NAC, endpoint compliance could ensure the these devices had appropriate OS version and patches; required antivirus, firewall, data loss prevention software running; and a NAC agent to expedite subsequent access and enable full post-admission monitoring.

The firm is well on its way to reaching its goal of 100,000 personal mobile devices by 2014. Initial results show that the demand for BYOD by employees is high, with 80 percent of employees choosing to accept the terms of the company, follow policy and install an MDM or NAC agent in exchange for corporate network access. In addition, the organization is introducing corporate-provisioned devices and mobile applications that leverage similar combined NAC and MDM controls.

Top 10 NAC Functions for Securing BYOD/CYOD

Inherent in the NAC process is the capability to capture, store, manage and act upon policy through the following functions that enable guest networking, BYOD and endpoint security controls:

1. **Device Fingerprinting.** Device fingerprinting is the process of scanning a network device and capturing detailed information regarding device responses to various protocol requests. Information about the device is correlated and compared to known device fingerprints.
2. **Standard and Alternate Means of Endpoint Authentication.** Some NAC systems rely on the 802.1X protocol that requires the device to be managed for any network access. In order to see and control unmanaged devices (such as personal mobile devices) and those devices that don't support 802.1X software (such as embedded systems), you can use alternative authentication methods based on device scanning techniques.
3. **Port Control.** Comparing a user's authorization level and the posture of the system making the request is a good foundation from which to make further network access-related decisions. For example, if John Smith has valid credentials, but his notebook lacks certain security provisions (it's not at the latest patch level), then John's access could be restricted until his system can be remediated. NAC-based application blacklisting and whitelisting can be used to prohibit unwanted applications.
4. **Guest Registration.** NAC can require a guest, which could be an employee, contractor or visitor, to register and accept terms in order to access a network. The registration and authorization process should be self-service, automated and as unobtrusive as possible. In some cases, users might need to install a permanent or transient agent or be subjected to an enumeration scan, depending on the level of access required.
5. **Asset Visibility.** IT staff needs to understand all the devices on their network, including corporate and personal mobile devices. NAC provides a level of real-time visibility to enable greater mobile intelligence, to support helpdesk, troubleshooting and investigation activities, and to incorporate mobile devices in audit and compliance tasks.
6. **Policy Enforcement.** Organizations also need to consider flexibility in their policies to accommodate different levels of risk, to enable desired user behavior and to facilitate exceptions in user and device access. Establish a process to ensure that desired policies are in place and verifiably functional, and responses to violations are appropriate, known and operationally approved.
7. **Self-Remediation.** A well-defined self-remediation process integrates with a guest access system in such a way that guest users are able to engage the remediation process for the purposes of the visit. It should also offer advice on security violations and means for resolution. In cases in which endpoint security policy issues can be resolved by the end user, the NAC system can redirect the user to a self-remediation site either inside or outside the corporate network.

8. **Auto-Remediation.** Ideally, remediation should be automatic and transparent. In many cases this is possible with corporate-provisioned systems only, because local laws may prevent you from changing the configuration of a system without the user's knowledge or permission. This process determines whether the system is a corporate asset or not, enumerates the system, identifies any deficiencies, queries the user (where required), attempts to resolve the remediation issue, continues with the NAC process, and then connects the user to requested network resources.
9. **MDM Integration.** NAC can integrate with MDM to secure corporate and personal mobile devices across user, device, application, data and network controls. This integration allows for a more uniform view of all users, devices and applications on a corporate network. It also allows organizations to apply a level of security appropriate for the type of user and degree of risk. As a result, network- and MDM-based security controls enable BYOD/CYOD.
10. **Access, Violation and Activity Reporting.** Compliance mandates require access control, host integrity and a record of activity on systems handling sensitive data. The capability for NAC information to tie into reporting and auditing efforts is critical. At a minimum, NAC reporting can provide a record of the following:
    - Timestamps
    - All requests to connect
    - Employee and guest acceptance of usage terms
    - Connection request results and status
    - All devices and configuration details (as applicable)
    - All violations; systems that contain policy deficiencies and the status of those deficiencies
    - All remediation events
    - User names
    - System IDs
    - IP and MAC addresses
    - Operating system types
    - Locations
    - Exception requests

The reporting function should also be trustworthy and employ a secure method for verifying and validating log entries and log sequences. Integration of NAC and other security platforms into SIEM is a best practice.

Conclusion

Clearly, the world is moving toward mobility, and the technologies that go with it are being carried in the pockets and purses of users. In a couple of years, we'll be referring to anything with a network cable as *legacy technology*. It isn't a matter of *if* we should integrate personal mobile technology into our networks, but how fast and how effectively we can do it.

Employees are bringing in their own devices, and IT organizations must enable their use while managing the associated security risks. Employers are looking to leverage consumer devices to increase worker productivity, expedite communications and facilitate resource accessibility.

BYOD/CYOD policies should encompass both wired and wireless devices across laptops, smartphones and tablets. Depending on the flexibility and intelligence of device interrogation, the comprehensiveness of the policy engine, the degree of interoperability with the operating environment and the means for enforcement and remediation, NAC can further enable trusted devices, PC or mobile, to join the corporate network and securely obtain the information they need based on predetermined levels of acceptable risk.

As NAC solutions enable the use of more diverse devices on the network, organizations should take the time to explore the use cases and risks, develop architectures and design for desired outcomes. They should also monitor results so they can build a trustworthy foundation for the use of personal mobile devices in the workplace.

SANS would like to thank its sponsor:

Last Updated: April 26th, 2018

Upcoming SANS Training

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

SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Doha 2018	OnlineQA	Apr 28, 2018 - May 03, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced