Long derided as an overhyped concept, network access control (NAC) has emerged as an important solution for mitigating the risks of consumerization. Network and security managers will use NAC to retain control of the network in a "bring your own device" (BYOD) environment.

Key Findings

- The most successful NAC policies will be those that provide the flexibility to support BYOD, yet still provide network and security managers with the means to protect the network from unapproved and risky endpoints.
- "Limited access networks" will be implemented to support employee-owned devices. The limited access network (a wireless LAN, in most cases) will function as a third network zone for most organizations, because it will be distinct from the production network and the wireless guest network (which only offers Internet access).
- Enterprises are only aware of 80% of the devices on their networks. "Profiling" technology is needed to discover the unknown devices and identify them.
- NAC will also be implemented to protect wired and remote access networks from unauthenticated and noncompliant endpoints.

Recommendations

- Work with business team leaders to develop policies in support of informal (grassroots) and formal BYOD programs. Use NAC to enforce these policies.
- Implement NAC policies in phases. Start with basic policies (for example, device authentication), and add more advanced policies (for example, device configuration or role-based access) as NAC matures in your environment.
Strategic Planning Assumption
By 2016, 60% of large enterprises will implement limited access network zones to limit the connectivity of personally owned mobile devices.

Analysis
NAC is the basic ability to detect when a device connects to your network and to enforce security controls based on knowledge of the risk status of the device and/or its user’s role in the organization. NAC had been overhyped, but Gartner believes that it has matured and will be one of the key mechanisms enterprises will need to use for mitigating the risks of the BYOD phenomenon. An environment of heterogeneous endpoints that are owned and operated by employees introduces new risks that were not present in the era of corporate-owned and managed Windows PCs. Consumerization is an unstoppable trend, and most organizations need to demonstrate flexibility and allow employees to use their personal devices for work. But, they also need to establish limits and not permit every device, every operating system and every configuration. Although approaches such as server-based computing and virtualization will also be used to deal with consumerization, NAC provides the flexibility that enterprises need in a BYOD environment, while providing the controls that enable network and security managers to retain control over the network. Figure 1 outlines a strategic road map that enterprises can use to achieve these goals.

Figure 1. NAC Strategic Road Map Overview

<table>
<thead>
<tr>
<th>Future State</th>
<th>Current State</th>
<th>Gaps</th>
<th>Migration Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Supporting &quot;bring your own device&quot; becomes the primary driver for network access control (NAC).</td>
<td>• Most NAC implementations focus on monitoring endpoints and forgo quarantining.</td>
<td>• Network authentication for wired and wireless LANs.</td>
<td></td>
</tr>
<tr>
<td>• Limited access networks enable connectivity for tablets, smartphones and other personally owned mobile devices.</td>
<td>• Wireless guest networks provide Internet access to visitors.</td>
<td>&quot;Profiling&quot; to identify and monitor endpoints.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Many wired networks are unprotected (no authentication).</td>
<td>• Enforce (not just monitor) NAC policies.</td>
<td></td>
</tr>
</tbody>
</table>

Source: Gartner (October 2011)
Current State

Since it emerged in 2003, NAC has always been about protecting the network through policies that govern network access. The policies have changed over time in response to changes in the threat landscape and changes in endpoints. Figure 2 highlights the three waves of NAC policy.

Figure 2. The Three Waves of NAC Policies

- **First wave** — At the peak of the worm era (Sasser in 2003; Blaster in 2004), NAC policies were focused on blocking risky laptops from accessing the network. In the early days of NAC, a common goal was to establish a policy dictating that endpoints must have up-to-date patches and antivirus signatures, and must be protected by a personal firewall, to gain access to the network. Common obstacles to NAC during this era included complexity, costs and operational concerns about blocking employees from accessing the network.

- **Second wave** — In addition to the obstacles outlined above, the threat landscape was changing. Stealthy, financially motivated attacks replaced noisy, mass worm attacks as the primary threat. Enterprises also improved their endpoint patching and configuration management processes. NAC shifted to simpler authentication-based policies.

Source: Gartner (October 2011)
Us" became the primary focus, as enterprises sought to limit access to corporate-owned and managed devices. Endpoints that failed authentication were restricted to a guest network, where they were limited to Internet access only.

- Third wave — In response to the consumerization trend, enterprises are turning to NAC to enforce policies related to BYOD programs. For example, some employee-owned devices may be allowed, whereas others will be blocked (see the Expected Future State section).

Rather than implement a full-blown NAC solution, most organizations have taken a shortcut approach and established wireless guest networks in common areas, such as visitors’ centers and conference rooms. This tactic has largely been effective in keeping guests off the corporate network, but mostly by only providing Internet access to guests via Wi-Fi. In many cases, some guest access to the corporate wired network is required. Enterprises that need to protect the wired network need stronger controls.

**Expected Future State**

Although NAC capabilities will still be used for basic security purposes, the primary justification for NAC will be to meet business demands for allowing employee-owned devices (both corporate-sponsored programs and grassroots informal adoption) to connect to corporate resources, while mitigating risk. BYOD risks include:

- Data loss — Managed endpoints invariably include a configuration management and security software suite, which provides visibility into data flow and potentially protections, such as data loss prevention. Employee-owned devices lack this protection, and the flow of sensitive data onto unmanaged devices often leads to expensive data exposure events, both accidentally and through attacks.

- Malware — Employee-owned laptops are more likely to be compromised by malware than managed devices, because most employees don’t have the knowledge and the resources to adequately protect them.

- Network instability — Employee-owned devices present a greater risk to the network than do managed devices. For example, endpoints or rogue wireless access points that provide Dynamic Host Configuration Protocol (DHCP) services can cause instability on the network.

A variety of technologies will be used to mitigate these risks and safely enable the use of employee-owned personal devices. For example, MDM will be used to provide control over smartphones and tablets, but will not be widely used on laptops. Server-based computing and virtualized desktop infrastructure create a secure environment for hosting applications and data but are very restrictive and don’t meet user requirements in many cases, such as where off-network computing and/or the native use of non-Windows operating systems are required. NAC’s role is to provide flexible mechanisms for protecting the corporate network, while allowing a wide variety of endpoints to be used.

Network protection will come in the form of a limited access network, which will give them the flexibility to support some employee-owned devices and restrict access from others. For example, an organization may choose to allow Android v.2 and v.3 on the limited access network, but block
access to Android v.1, simply because it does not have the resources to monitor vulnerabilities and maintain configuration guidelines on older operating systems. Some organizations may choose to explicitly block endpoints that have no place on corporate networks, such as gaming consoles. Most limited access networks will include wireless LANs as the primary access mechanism, as employee-owned smartphones and tablets will generally connect via Wi-Fi. A limited access network will function as a third network zone for most organizations, because it will be distinct from the production network and the wireless guest network. Whereas the guest network allows only Internet access, the limited access network will allow access to a subset of applications and data. NAC policies will limit access to sensitive applications and data, depending on the device and possibly the user’s role.

The use cases that drove adoption in the first wave (endpoint baselining) and the second wave (guest networking) of NAC, and the remote access use case, will still be widely implemented (see “Network Access Control in 2009 and Beyond”). However, these scenarios will often be implemented after the limited access network has been established (see the Road Map section). Gartner expects that, by 2016, 60% of large enterprises will implement limited access network zones to limit the connectivity of personally owned mobile devices.

Gap Analysis and Interdependencies

Enterprises will need to become proficient in the following three technologies in order to implement and operate an NAC environment in the era of consumerization:

- **Authentication** — Organizations that are highly security-conscious will choose to authenticate devices to their wired and wireless networks. Although nearly all wireless LANs require users to sign in with a user ID and password, most wired and many wireless implementations don’t require device-based authentication (example credentials include machine certificates, MAC addresses and special registry keys). Authentication will be a first line of defense for enterprises whose goal is to ensure that only corporate-issued and managed devices are granted access to the production network. IEEE 802.1X can be an inexpensive approach for implementing authentication, if the infrastructure already supports it (see "Case Study: 802.1X-Based Guest Network for a Wired LAN"), but interoperability issues can complicate deployments in mixed-vendor environments. Most enterprises use commercial NAC solutions to authenticate endpoints (for example, an NAC agent can serve as an authentication credential).

- **Profiling** — Gartner estimates that the typical enterprise is aware of only 80% of the devices that are active on its network. The basic goal of profiling is to establish a continual process for discovering and identifying all the devices on the enterprise network. Once the endpoint has been identified, the appropriate NAC policy can be enforced. For example, iPads and other tablets can be placed on the limited access network, and essential non-PC endpoints (for example, printers, security cameras and IP phones) can be included on an exception list of devices that are granted unconditional network access. The consumerization trend has amplified the need to include profiling as part of an NAC implementation. Profiling technology can be acquired through independent vendors (sample vendors include Great Bay Software, Insightix and Lumeta), and many NAC vendors have developed their own profiling capability.
Enforcement — Enforcement is a core component of all NAC solutions, and it can be accomplished via several options, including access control lists, virtual LAN steering, packet filtering, DHCP and other techniques. Most enterprises will start with relatively simple enforcement that enforces three access "zones" — full access, limited access guest access. As those capabilities mature, more granular and dynamic access will evolve, based on user identities or groups and changing security conditions.

Enterprises that require more advanced NAC functionality will need to develop some or all of the following capabilities, all of which are described in more detail in "Network Access Control in 2009 and Beyond":

- Endpoint baselining — Determine whether an endpoint is compliant with its configuration policy (for example, whether patches and antivirus signatures are up to date).
- Remediation — Noncompliant endpoints that have been quarantined will need to be manually or automatically remediated, so that they can access the network.
- Identity-aware networking — This is the ability for the network to restrict access to certain resources, based on the user’s role.

Road Map (Migration Path)

Because NAC encompasses a broad set of use cases and technologies, one of the biggest challenges that organizations face in their NAC projects is deciding where to start. Often, projects get delayed in their early stages because of indecision and the NAC team’s inability to gain consensus on the most important goals. Gartner recommends that organizations establish NAC goals according to the following priorities (see Figure 3).
Figure 3. NAC Strategic Road Map Timeline

- Limited access network
- Add granular policies to limited access network
- Protect wired LANs
- Remote access policies
- Identity-aware network


- Consumerization
- Consumerization momentum
- Malware threats
- Mobility
- Advanced security requirements

Drivers

Source: Gartner (October 2011)

Highest Priority

- Implement a limited access network. As outlined in the Expected Future State section in this research, this is typically a wireless network zone (it may also be wired) that employees will access with their personally owned tablets, smartphones and other mobile devices. A combination of authentication, profiling and enforcement is needed to create this limited access network.

Driver:

- Consumerization remains a grassroots phenomenon, driven by business units demanding that users be allowed to bring their personal mobile devices to the office. Isolating these endpoints on a separate network helps to maintain data protection policies and network stability in the production environment.

Medium Priority

- Add granular policies to the limited access network. Baseline the endpoints to ensure that all mobile devices are compliant with the policies that your organization has specified. Policies may dictate operating system versions, endpoint agents (for example, MDM agents) or VDI software.
- Protect the wired LAN. All endpoints should be required to authenticate to the wired network. Endpoint baselining and configuration policies should be applied to Windows PCs, Macs and other endpoints. Policies should specify up-to-date patches and antivirus signatures, personal firewalls and possibly disk encryption. For baselining, most organizations will initially adopt a monitor-only policy, whereas highly security-conscious organizations will enforce quarantining for noncompliant endpoints (see "Network Access Control in 2009 and Beyond"). Quarantining adds complexity to the remediation process, particularly in use cases that call for automated remediation.

- Establish remote access policies. Endpoint configuration policies should also extend to remote devices that access the network via a VPN.

Drivers:

- Consumerization will gain momentum, as more employees choose to bring personal devices to work.
- The wired network needs to be as secure as the wireless network.
- Authorized endpoints must be compliant with corporate configuration policies. NAC adopters report that initial endpoint baselining scans reveal that many endpoints (up to 50%) are noncompliant, due mainly to operational issues, such as software distribution failures, script failures and problems with patch installation.
- The remote access use case is less urgent, because remote devices are isolated, and cannot directly impact the stability of LANs and wireless LANs. Remote endpoints that have been compromised can spread malware infections to other endpoints through a VPN connection, so endpoint configuration policies should also apply to these devices.

Low Priority

- Identity-aware networking — Once organizations have mastered the ability to administer basic authentication and device policies, they can consider adding identity-aware policies to restrict access to specific applications and resources based on a user’s role. For example, the network can allow employees in the HR department to access the salary database, but can block access by users from other departments.

Drivers:

- Organizations with weak or incomplete identity and access management infrastructures can add intelligence to the network to monitor user behavior and enforce coarse-grained authorization policies.
- Highly security-conscious organizations will likely make identity-aware networking a medium or even a high priority, because it provides an additional level of authorization for controlling access to critical applications.
Evidence

**Primary:** Discussions with Gartner clients over an extended time period (beginning in 2003, when Gartner initiated NAC coverage) about their requirements for NAC policies

**Secondary:** Discussions during the same time period with network security vendors as part of ongoing research for Gartner NAC Magic Quadrants and MarketScopes
Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

© 2011 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner’s prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner’s research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner’s Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see “Guiding Principles on Independence and Objectivity” on its website, [http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp](http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp).