In an era of IT consumerization, IT departments need to effectively manage both corporate and employee-owned devices.

BYOD **Deluge**

Network access control and mobile device management tools work together to create a blueprint for BYOD success.

EXECUTIVE SUMMARY

Corporate IT departments are struggling to manage and secure an influx of handheld mobile devices—both corporate and employee-owned. Two technologies best positioned to help include network access control (NAC) and mobile device management (MDM). While there is minor overlap in capabilities, the two technologies bring different management and security features that complement each other to ensure full visibility and control of the network and mobile devices. This white paper will explore the two technologies, how they differ, where they overlap, and how they complement each other—ultimately revealing how the use of these technologies together can enable IT departments to effectively oversee devices and the network in this new era of IT consumerization.

BRADFORD networks

NETWORKWORLD Custom Solutions Group

COMPLEMENTARY TECHNOLOGIES HELP IT MANAGE MOBILE DEVICES AND SECURE THE NETWORK

First it was a trickle; a few BlackBerrys for the executives. But as prices came down and appreciation of the productivity benefits went up, waves of smartphones started flowing into the organization. Still, it was manageable because they were mostly accessing e-mail. Then the iPhone and Android phones hit the market, followed by a variety of tablets, and employees started bringing their own devices to work in droves. Now, users with all sorts of powerful mobile computing devices want access to all parts of the corporate network. As a result, corporate IT is swimming hard against the tide to manage and secure all these mobile devices.

By 2014 some 90% of organizations will support corporate applications on personal devices.

—Gartner Research

IT managers face a two-fold problem here: protecting the corporate network and managing the end devices. And they have two technologies to address different aspects of the problem: NAC and MDM. At its simplest, NAC focuses on the network while MDM focuses on mobile devices. Perhaps because the technologies overlap to a degree, some IT managers assume these technologies do the same things and therefore adopt only one of them. In fact, each technology brings its own advantages. Used together, they complement each other and provide the most effective management and security of both the network and the mobile devices.

THE PROBLEM

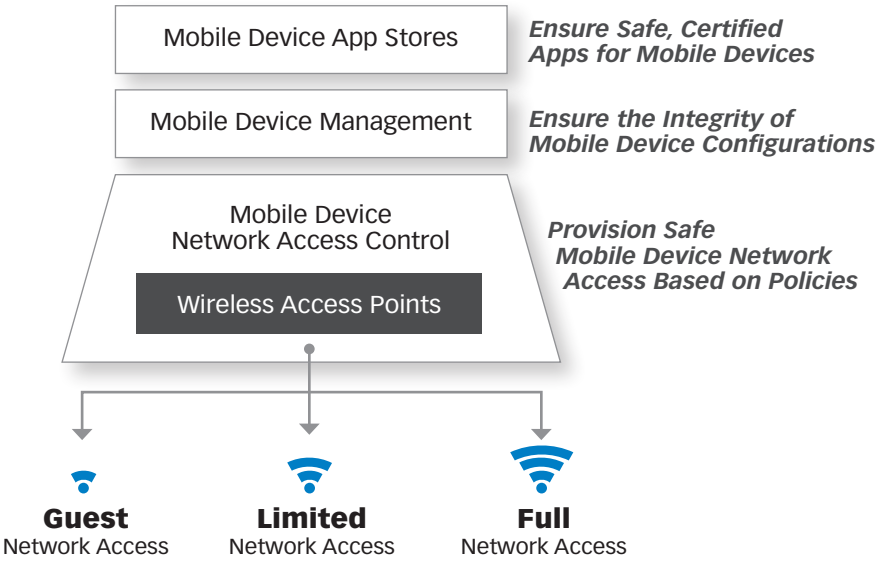
Because of the explosion of different devices and the consumerization of IT, there are many issues to consider in protecting today's corporate networks.

First, there is no standard device or operating system. Gone are the days when all IT had to worry about were stationary, standard Windows-based desktops. Now, the devices come from a variety of manufacturers with different operating systems, including Apple's iOS, Google's Android and Microsoft's Windows Phone 7.

Second, the devices aren't necessarily owned by the company. The bring-your-own-device (BYOD) phenomenon has washed quickly over corporate America. A 2011 survey by IDC revealed that 40 percent of the devices used to access business applications were consumer-owned, up from 30 percent in 2010.[1] Gartner Research predicts that by 2014 some 90% of organizations will support corporate applications on personal devices.[2] The most common scenarios are likely to include laptops, tablets and smartphones.

Third, it's not just the plethora of mobile devices that are connecting to the corporate network. An increasing variety of IP-based equipment, such as security cameras, medical equipment, cash registers and numerous other devices are sending data over the network. They need to be managed and secured, too.

Manage Risk with a "BYOD Blueprint"



A BYOD BLUEPRINT FOR SUCCESS

In order to ensure holistic network security with a BYOD policy, organizations need to consider all parts of the BYOD ecosystem starting with the obvious: Mobile Device Application Development (MDAD). In this phase, the IT organization needs to be sure that apps employees are using on their mobile devices are trusted—tested and internally vetted for security. Once the quality and integrity of these apps has been established, focus needs to move to device use. This involves ensuring the integrity and secure configuration of endpoint devices (which is in the realm of MDM for mobile devices such as tablets and smartphones), and securing the network by controlling access to resources based on pre-established access policies (a primary focus of NAC).

HOW NAC PROTECTS THE NETWORK

NAC technology enables IT to define and control how devices and users gain access to network resources. It first emerged as a way to authenticate and authorize endpoints (primarily PCs) on the network using simple scan-and-block technology—either allowing or blocking network access based on set security

[1] Source: IDC, June 14, 2011

[2] Source: "Opportunities and Conflicts Loom in the Wake of Google's Motorola Mobility Deal", Gartner, October 7, 2011

The challenges created for IT are two-fold: ensuring the integrity and secure configuration of endpoint devices and securing the network by controlling access to resources based on pre-established access policies.

policies. NAC later evolved to address emerging demand for managing guest access on corporate networks by facilitating limited network access for external users such as visitors, contractors and business partners.

Today, NAC has evolved further to enable more sophisticated access policies and, perhaps even more important, to provide automatic discovery and full visibility of every device and user attempting to access network resources on both wired and wireless LANs. NAC encompasses traditional network endpoints including PCs, laptops and printers, along with newer mobile devices such as tablets and smartphones as well as an extensive number of other devices.

According to Gartner, the NAC market has recently been revitalized by the need to manage employee-owned devices. "The BYOD phenomenon is driving growth in the NAC market as organizations seek to apply policies specific to personally-owned mobile devices," says Gartner in its Magic Quadrant for Network Access Control, Dec. 2011. The NAC market grew only 3 percent from 2010 to 2011, to about $206 million, according to Gartner. In 2012, however, the research firm expects market growth of 10 percent, primarily because of the BYOD trend.[3]

In general, here's how NAC works: With a NAC solution in place, all points of access to a secure network—wired ports and wireless access points—are typically isolated to prevent unauthorized access. When a device tries to connect to the network, the NAC solution identifies the device and its type (which may involve dynamic profiling or classification), identifies and authenticates the user of the device (if applicable), and scans the device to determine if its configuration is compliant with pre-established security policies. If the device (and user) is authorized to access the network and passes the compliance scan, NAC automatically enables network access based upon device- and/or user-specific policies. For example, a specific virtual LAN may be set for the connection. However, if the device or user is unauthorized or fails the compliance scan, NAC will automatically restrict or prohibit network access—again based on the pre-established security policies.

NAC's ability to create limited access zones is particularly useful in containing the risks of BYOD. Because these mobile devices are personally owned, IT usually has no ability to mandate how they are configured, secured and managed. And yet more and more employees want to use corporate applications on these devices. Some NAC products are capable of profiling the device by determining whether the endpoint is an iPad, Android tablet, iPhone, etc.; whether it is corporate- or employee-owned; and whether it has access rights. That way, personally-owned devices can be given limited access to an appropriate subset of corporate network resources.

In the real world, a hospital might use NAC technology with hospital-owned iPads in the emergency room, where doctors and nurses can admit patients via the hospital's patient care network. Meanwhile, doctors' iPads could be given access to e-mail and the Internet at the hospital, but nothing more. In addition, the hospital may provide a general WiFi network in its emergency room lobby for all to use. Using NAC, IT would detect publicly-owned iPads as unauthorized devices and limit access to the guest network.

HOW MDM MANAGES DEVICES

MDM solutions have emerged recently in response to the ubiquitous adoption of handheld mobile devices in corporations. MDM focuses on the end device rather than the network, using client software on the devices. By communicating with the client software, the MDM server enables IT to manage these devices. Specifically, MDM can keep an accurate inventory of the number and types of mobile devices. It can ensure the devices and the data on them are encrypted. It can remotely install, remove or patch applications and operating systems. And it can track devices using geolocation, and lock or wipe data off a device hard drive if lost or stolen.

Revenue from MDM products amounted to about $150 million at the end of 2010, and is expected to grow at a compound annual growth rate of 15 to 20 percent over the next several years, according to Gartner.[4]

[3] Source: "Magic Quadrant for Network Access Control", Gartner, December 8, 2011

[4] Source: Magic Quadrant for Mobile Device Management Software", Gartner, April 13, 2011

NAC provides an umbrella of protection across the entire network for all types of devices connecting.

Some MDM products are specific to a single platform, like Apple's iOS, while others support a variety of devices. Some can do selective wipes, erasing all corporate information while leaving personal information, for example, which is useful for employee-owned devices. Similarly, some MDM products are capable of only full-disk encryption while others are more granular, allowing IT to implement folder-level encryption to protect sensitive corporate information.

Here's where MDM comes into play in our hospital example. With MDM client software on devices owned by the hospital as well as the doctors, IT keeps an accurate inventory of devices and whether they are patched and up to date. If an iPad goes missing, IT can erase all the data, potentially saving the hospital from a breach of HIPAA regulations.

NAC AND MDM TOGETHER

One reason for confusion over NAC and MDM is that a few overlapping capabilities have emerged. For example, some NAC products can do a general scan of a mobile device's posture, identifying applications and operating systems similarly to MDM products. Both solutions can also provide an inventory of mobile devices in the enterprise network environment. Beyond these similarities, however, the two technologies differ substantially and each offers distinct advantages.

First, NAC is focused entirely on the enterprise network (wired or wireless), but does not have visibility or control of devices outside of the enterprise network. For example, NAC has no visibility of an iPhone accessing corporate applications over AT&T's cellular network. This is a scenario in which MDM can help, because its server will communicate over the cellular network with the device (via client software).

Second, NAC will identify a mobile device, determine its operating system and possibly inventory the applications on the device, but it generally will not add or remove applications, encrypt data or wipe the device. Configuration changes on the mobile device and the ability to perform a remote wipe of sensitive data are in the realm of MDM.

Third, a comprehensive NAC solution encompasses *every* endpoint device that connects to wired and wireless networks, while the scope of MDM is limited to handheld mobile devices. NAC provides an umbrella of protection across the entire network for all types of devices connecting—including not only mobile devices but also desktop PCs, laptops, servers, printers, IP phones, security cameras and all other IP-based endpoints. This is an important consideration in the age of IP-everything in which mobile devices represent just a fraction of what's connecting to the network. IT must still manage and secure the rest of the network as well.

Here's how these complementary features could work at a hospital. NAC protects the network by enforcing access policies for a wide range of devices—including PCs, mobile devices (corporate and personal), security cameras and heart monitors—so each device and user has access only to appropriate resources. When a doctor accidently loses an iPad at a conference, IT uses MDM to locate and wipe the device.

THE TOTAL SOLUTION

As endpoint devices, both mobile and fixed, continue to proliferate, and the line between corporate- and personally-owned technologies continues to blur, IT will need effective tools to manage and secure both the network and the endpoints. The combination of NAC and MDM provides the perfect solution. NAC looks from the corporate network outward, enabling IT to better understand what devices are trying to access the network, whether to allow them to connect and how much access to give them. MDM, on the other hand, looks at what's on the mobile device itself and gives IT control over the data and applications on that device.

Bradford Networks' Network Sentry product is the first network security offering that automatically identifies and profiles all devices and users on a network, providing complete visibility and control across all brands of equipment and devices. For more information on Bradford Networks and its products, go to www.bradfordnetworks.com. ■