IT organizations struggle to get a handle on mobile device proliferation.

**EXECUTIVE SUMMARY**

With the proliferation of mobile devices and the consumerization of IT, corporate networks are becoming more challenging to manage and more at-risk every day. The days of a static, one-size-fits-all policy applied to company-owned assets are over. Today, IT departments need to understand what devices are trying to connect to their networks, so they can provide convenient, secure access to those that are authorized, including personal iPads and smartphones. This white paper describes the growing problem and explains how IT departments can implement a practical and secure strategy and offer the convenience and business agility that mobile devices provide.

**THE EXPLOSION OF MOBILE DEVICES HAS BEEN BOTH BOON AND BANE TO ENTERPRISES.** These devices, which are powerful yet inexpensive and easy to use, help employees to be more productive no matter where they are. They can increase collaboration and the flow of information, enabling an organization to react more quickly to market conditions and customer needs. And they are becoming so ubiquitous that corporations often don’t even have to buy the devices—employees are bringing their personal smartphones or tablets to work.

While use of mobile technologies has potential to transform business, making it possible for an organization to be more agile in serving its customers, it can also disrupt IT. The new generation of employees expects complete freedom to use mobile devices, regardless of...
whether they are company-owned or employee-owned. Most IT departments are struggling to define and implement a bring-your-own-device (BYOD) strategy. To a large extent, they still use the old command-and-control model of Windows-based device management, trying to dictate what devices employees can use and how they can use them. But the old model doesn’t work anymore. Not only are new devices flooding the workplace, but today’s mobile devices bring a variety of new operating systems, such as iOS and Android, and many applications to contend with.

In fact, by 2014 some 80 percent of professionals will use at least two personal devices to access corporate systems and data, according to Gartner Research. The most common scenario is likely to be a laptop, tablet and smartphone. “Saying ‘no’ to business use of smartphones, tablets and similar devices in the enterprise is no longer an option,” said John Pescatore, vice president at Gartner Research. “These mobility trends point to network access control (NAC) as a critical capability for supporting business demands while managing the risk of allowing a wide range of devices access to sensitive networks and information.”

**TAKING BACK THE REINS**

The consumerization of IT is happening faster than anyone expected, thanks to Apple, and threatens to overwhelm corporate IT departments. According to a recent survey by IDC¹, IT groups typically underestimate by 50 percent the proportion of employees using their own devices for company business. The survey revealed that 40 percent of devices used to access business applications are consumer-owned, up from 30 percent in 2010. That percentage surely won’t drop. If anything, it will grow even more quickly in coming years.

Until this recent tsunami of IT consumerization, IT’s method of managing mobile devices was an extension of how it had always managed PC desktops. Laptops and other portable devices were owned by the corporation and issued to authorized users. NAC originally sought to verify whether users were authorized to access the network based on factors controlled by the network administrator, resulting in a rigid and limited system. Access was binary, allowed or denied, based on the identity of the user and the security posture of the PC. “It was not designed to provision varying access to different VLANs based on the risk profile of the device,” says Frank Andrus, chief technology officer at Bradford Networks.

Now, however, there is a mixture of corporate and personal devices, computers and phones, some of which use Windows and some of which use iOS, Android or other operating systems.

In a hospital, for example, emergency room doctors and nurses may use hospital-owned iPads for real-time access to patient information. They need to be connected to the hospital’s patient care network. However, personally-owned iPads are not allowed on this information-sensitive network because of compliance regulations. And yet, the hospital may provide a guest network in its emergency room lobby for all to use. How does the IT department distinguish among hospital-owned iPads, iPads owned by hospital employees and iPads being brought in off the street?

Instead of command and control, IT needs to enable secure network access for any device, while controlling risk.

The first challenge is visibility. As the statistics suggest, IT often is unaware employees are using their personal devices on the corporate network. The first step is to establish a baseline of connected devices by conducting an initial inventory, discovering all the devices on the network, classifying them and then setting network access policies based on the risk profile of the device. Subsequently, any new devices that connect to the network are automatically assigned a policy depending on risk profile. That translates into secure, convenient access for authorized devices, while providing appropriate limited access for unauthorized devices.

In the hospital example, this approach could allow hospital staff to connect to the patient care network with corporate-owned iPads. It could also allow IT to detect and identify which doctors or nurses might be bringing in their own iPads for use at work (perhaps making notes on patients and treatment), and allow IT to create device-specific policies for such devices. For example, IT might allow limited access,
Accurate, up-to-date information on all the devices on the network can enable both IT and the business to make better decisions.

such as email and Internet, for these devices, but deny access to the corporate network where sensitive patient information is retained. But if a patient or guest brought in an iPad, IT would detect that this was a foreign device, and limit its access to a guest network.

**INTEGRATED MANAGEMENT AND SECURITY**

Identifying all the devices on the network is only half the battle, and probably the easier half. The real challenge is ongoing management and integrated security. As network technology evolved and security needs increased, IT often deployed best-of-breed vendor-specific technologies independently to address various problems. The result: many of today’s networks, management and security functions operate within their own security silos. These include:

- **ENDPOINTS (TYPICALLY PCS AND LAPTOPS):** Platforms and operating systems are standardized, patched and kept up to date with the latest antivirus programs.
- **NETWORK INFRASTRUCTURE:** Network equipment such as switches, routers, wireless controllers, firewalls and VPN concentrators have security features built in.
- **SECURITY INFRASTRUCTURE:** Security products like intrusion detection and prevention, deep packet inspection and network behavior analysis systems provide additional levels of security.

What’s more, the traditional approach to security is focused on blocking the bad guys, locking everything down to keep outside threats from penetrating the network.

But the traditional approach is ill equipped to deal with the increase in and diversity of mobile devices, personal as well as corporate. Today’s networks need transparent, nondisruptive, integrated management and security. They face constantly evolving threats from increasingly sophisticated hackers, so the focus of security should no longer be solely on the perimeter. In fact, today’s threats are just as likely to come from inside the perimeter, whether from an unsecured personal iPad of a physician or a laptop of a patient awaiting treatment in the emergency room.

It all adds up to security risk. IT staff spend an inordinate amount of time trying to keep endpoints and infrastructure secure, yet security holes remain because they lack an integrated approach. Rather than fight a battle that IT is likely to lose, the strategy needs to shift to continuous discovery, information gathering and integration. The solution to these problems is a security policy engine that breaks down silos and leverages and integrates endpoint security, network infrastructure, and security infrastructure solutions, without requiring the huge investment of a wholesale redesign or forklift replacement of existing solutions.

The fundamental challenge is how to make networks both more accessible and more secure. The new approach needs to shift focus from command and control to policy-based provisioning that is flexible and can deal with personal mobile devices. After the initial inventory of devices and application of policies, a central security policy engine provisions the appropriate level of network access to corporate-owned and personal devices.

**BROAD BENEFITS FOR IT AND THE ENTERPRISE**

The benefits of such a shift in strategy are both tactical and strategic. The most obvious benefit is the information made available by automatic detection of all devices that connect to the network. The IT department can categorize the devices and then devise and apply appropriate network access policy to each category based on risk profile. Once a baseline inventory is conducted to detail an initial inventory of what’s connecting to the network, no new devices can connect undetected and unprotected. Instead, the appropriate policies can be applied whenever a device connects to the network, whether it’s a corporate or personal device, an iPhone or an Android tablet.
This not only ensures consistent security, but also saves the IT staff hours, if not days, previously spent fighting security brush fires. Rather than having to manually identify and provision each new device, IT staff is free to concentrate on important, more strategic projects that will further business goals.

An accurate and complete profile of the devices on the network enables better integration of those silos of security. IT need not rip out and replace equipment or buy expensive upgrades. IT staff can leverage the technologies already in place to create a more holistic security posture. Ideally, this integration enhances the effectiveness of previous technology investments.

The biggest benefit of this more capable NAC solution, however, is the strategic value of the information it gathers from the network. Accurate, up-to-date information on all the devices on the network can enable both IT and the business to make better decisions. By continuously watching trends and behaviors on the network, companies can make more innovative use of connectivity. “IT needs to understand the behavior patterns of the devices on the network and use that information to make better decisions,” says Andrus. “It’s no longer about control but rather about detection, pattern recognition, and policy definition.”

In addition, real-time reports as well as historic records of network and device activity can be invaluable for audits of compliance to internal policies as well as external government regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Sarbanes-Oxley Act of 2002 (SOX).

Ultimately, this data creates a big-picture view of ongoing network activity, helping IT and business leaders spot trends and devise ways to take strategic advantage of networks, mobile devices and IP-based infrastructure.

If we go back to our healthcare example, hospitals are subject to internal and external audits to ensure HIPAA compliance. Being compliant is not merely a point-in-time conformation with the regulations. Compliance is a day-to-day operational process that needs to be demonstrable at any given time. Therefore, establishing an automated way to discover and profile devices on a healthcare network and securely provision network access is essential to ensure sustainable compliance. Automated reporting and controls minimize the effort needed to operationalize compliance and respond to an audit.

**BYOD IS HERE TO STAY**

The proliferation of corporate owned and personal mobile devices is unlikely to abate any time soon. By 2014, in fact, Gartner predicts that 90 percent of organizations will support corporate applications on consumer devices. Corporate IT departments that try to keep up by using traditional NAC methods are not likely to succeed, and may in fact endanger management and security; they also risk putting their companies at a strategic disadvantage. But if they evolve by adopting technology that can detect new devices and dynamically adapt the network security posture, IT will improve network security and manageability, save IT staff time, increase employee productivity and gain strategic business advantage.

Bradford Networks offers the best solution to enable secure network access for corporate issued and personal mobile devices. Bradford’s flexible Network Sentry platform is the first network security offering that can automatically identify and profile all devices and all users on a network, providing complete visibility and control. Unlike vendor-specific network security products, Network Sentry provides a view across all brands of equipment and devices so nothing falls through the cracks. Hundreds of customers and millions of users worldwide rely on Bradford to secure their IP networks. For more information on Bradford Networks and its products, go to [www.bradfordnetworks.com](http://www.bradfordnetworks.com).