WHITEPAPER

NETWORK VISIBILITY

What It Means, Why You Need It, and How to Make It Work

If you can't see what's on your network, you can't control it—and that makes your organization vulnerable. It's the same as someone sneaking into your business, strolling through offices, looking through files for company intellectual property, and benefiting from your unique capabilities.

But network visibility has become a lot trickier than in the old days, when devices were static and networks were wired and confined to a building. Wireless networks and mobile devices have become pervasive, and many employees now use their personal devices for work. Companies are finding more and more rogue, mysterious and unknown devices showing up on their networks. (Or, even more concerning, they may not be aware of these devices at all.) Who is using those devices, and for what? Do they belong to employees trying to do their job? Or is something more sinister going on? The number of unknown devices on a network is growing, and so are the risks—from rogue employees to cyber criminals and even some countries hunting for unprotected devices with vulnerabilities to exploit.

In this volatile environment, network visibility takes on new urgency. For network administrators and security professionals, the challenge is how to give legitimate users just enough access to the information they need, while protecting sensitive customer information, your intellectual property and your brand. You need to see every device trying to access your network, who it belongs to, and what segment of the network it is trying to access. With this information, you can allow authorized users to go deeper into your network while keeping unidentified devices at bay—either by limiting access (such as assigning them to a guest network) or blocking them altogether.

BRADFORD networks

WHY NETWORK VISIBILITY IS IMPORTANT

For Security

With wireless networks, network boundaries are not only invisible, they often extend far outside an organization's physical control. You need the ability to detect unauthorized devices and users, even if they aren't in the building, such as someone sitting discreetly in the parking lot.

The growing popularity of Bring Your Own Device (BYOD) creates additional security challenges caused by rogue employees potentially putting the network and sensitive information in jeopardy. Unfortunately the danger of insider threats is very real—a small number of employees do steal credit card information, personal data about co-workers, electronic medical records and company intellectual property. They're more likely to do it using their own highly portable personal devices (possibly because they think they can get away with it).

For Compliance

HIPAA, PCI DSS and other government and industry regulations mandate visibility into network access. You can't manage electronic medical records, credit card data and other sensitive information without it. Having a demonstrable audit trail of who has connected to your network, the device they used and when they connected is critical to passing any regulatory audit.

For Forensics

Visibility can track and record all relevant details about network access: the devices and users, the locations and access points, the times they connected and disconnected and the information accessed. The result is a complete audit trail in the event of a security incident—a capability that also discourages violations by employees who might otherwise be tempted.

To Prevent False Positives

Visibility can also identify where security policies needed to be adjusted, where for example an alarm goes off when a trusted user tries to access data they should be allowed, but can't because of how the policy is set up. Network visibility will identify the user, the device, time of day and data they're trying to access—the key parameters needed to revise the policy if necessary.

To Eliminate Network Blind Spots

When devices show up on a network, they are represented by a MAC address and an IP address. Forcing devices associated with BYOD to be registered ensures that all authorized devices have an owner. Then, when a company's IDS/IPS or SIEM software identifies activity from a mysterious IP address, the underlying device can be associated with a user—even when the device is employee-owned. This device/user correlation eliminates the blind spots and provides visibility to the "last mile" of your network—to the owner of the device.

HOW TO MAKE NETWORK VISIBILITY WORK

Visibility in a BYOD world has to address two competing goals: users need to access corporate information to do their jobs; the organization has to keep that information safe. To make it work, you need the ability to detect every device that attempts to connect to your network, and respond appropriately depending on what you know about the device. From a visibility standpoint, devices accessing the network will fall into two basic categories:

- Managed: a device that has been identified and accounted for (whether owned by the organization or the employee). A managed device will have a profile that associates it with a user and the information they are allowed to access, according to the policy you define.
- Unmanaged: a device that is unidentified and for which no profile exists. How you handle it (such as locking it out or assigning it to a guest network) will also be covered in the access policy.

The following is a roadmap for how to proceed.

Step 1: Classify your data

The first step is to classify your data based on type and risk level, and assign the different categories of data to different sub-networks within the corporate network. (You may have done this already.) For example, in a technology company, the Sales department may have highly sensitive customer contact information while Engineering may have equally sensitive product designs. The goal is to classify your data and assign it to different network segments so that authorized users will be able to access it, while keeping sensitive data off-limits to everyone else.

Step 2: Classify your users

The next step is to classify users that need access to the data categories you defined. In a hospital, for example, physicians may be granted access to sensitive information like electronic medical records, while administrators may get a much more limited view of patient data. Users not categorized in this way will be considered guests, and will only be allowed access to the internet or some safe area of the network (the "hospital lobby").

Step 3: Define network access policies

Once you've determined which users can have access to what data, the next step is to define a network access policy that associates users and their device with the network they are allowed to access. Developing this formal BYOD policy is critical so you can provision the right level of access based on the user's profile. Using a new generation of Network Access Control (NAC) technology, you can then enforce the policy that you have defined. When a user logs in, the NAC technology will identify the managed device and allow the user to access the data they are authorized for.

Step 4: Monitor and tune access

After the network access policy is in place, it's important to continually monitor the network for exceptions as well as possible violations. As usage patterns emerge, you'll be able to fine-tune the policy to make sure users are getting the access they need without compromising security. Since users will come and go, and access requirements will change, ongoing visibility and the ability to modify the access policy when needed will keep the organization secure, and users happy and productive.

SECURE BYOD WITH BRADFORD NETWORKS

Bradford Networks provides a new level of visibility and control for corporate networks, bringing secure BYOD within reach for organizations of all sizes. Our Network Sentry technology automatically discovers your entire network infrastructure and assesses the risk of every device that tries to connect to your network.

Network Sentry discovers your entire network infrastructure, creating a comprehensive inventory including:

- L2 and L3 switches
- Wireless AP / controllers
- Ports
- VLANs
- Firewalls
- Routers

Network Sentry monitors every device that tries to connect to the network and identifies:

- MAC address
- IP address/hosts/network adapters
- Device type
- Connect/disconnect time
- Managed or unmanaged (corporate-issued or personal device)
- User on the device
- Physical connection point (switch port or wireless access point)
- Jailbroken or not
- Antivirus running or not; latest version of antivirus signature file
- Operating system version
- Wireless AP / controllers
- Ports

This unprecedented level of network visibility is leveraged to provide a new level of network visibility and access control. The result is organizations can safely embrace BYOD while ensuring the right users and devices have access to the right information.

Discover how to make network visibility work for your organization. Contact Bradford Networks today.

BLOCK, CONTAIN, EMBRACE OR DISREGARD. WHAT'S YOUR APPROACH?

Gartner has identified four categories describing how organizations handle BYOD, which it calls *Block, Contain, Embrace and Disregard*[1] . These categories provide an interesting starting point for understanding your organization's current approach and future direction.

For most enterprises, a Block strategy is too draconian because it means that many activities will grind to a halt. The Disregard strategy equates to turning a blind eye to devices getting on the network, where the organization doesn't bother to make any policy or technology changes. (While this is obviously a poor choice, it's also the path of least resistance and thus surprisingly common.)

The Contain strategy has been the choice for many companies, where personal devices are put into a safe zone with limited network access. But for most enterprises, a more flexible approach is needed that allows *some* people to use *some* devices to access *some* network resources. Making it possible: visibility into network access, and the tools to put that visibility to work. Users get the right level of access while the enterprise stays in control—which ultimately is what the Embrace category is all about.

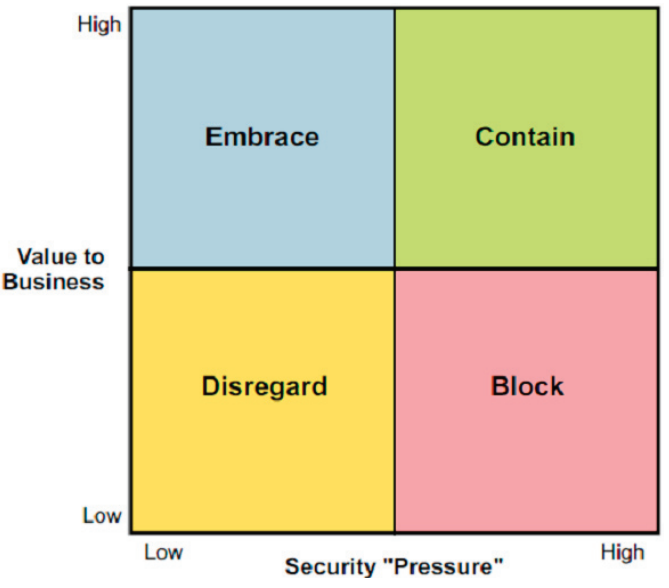

Figure 1. Mapping Security Responses to Risk and Business Value

1 Source: "NAC Strategies for Supporting BYOD Environments," Gartner, December 22, 2011

Address One Broadway, 4th Floor Cambridge, MA 02142, USA
Toll Free +1 866.990.3799
Phone +1.603.717.9333
Email info@bradfordnetworks.com
Web www.bradfordnetworks.com

Bradford Networks offers the best solution to enable secure network access for corporate issued and personal mobile devices. The company'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 connecting devices eliminating the network blind spots that can introduce risk. Hundreds of customers and millions of users worldwide rely on Bradford to secure their IP networks.

BN-001-09-001