TOP 4 NETWORK SECURITY CHALLENGES IN HEALTHCARE

Addressing Them with Secure Network Access Control

- Executive Summary .............................................................................................................1
  - Top 4 Network Security Challenges
  - Addressing Security Challenges with Network Access Control
- An Evolving Network Environment .............................................................................2
  - Securing and Provisioning Medical Devices
  - Securing Network Access for Guests and Visitors
  - Securing Access to Patient Information
  - Achieving Compliance with Regulatory Standards
- Adaptive Network Security ..........................................................................................4
  - Integration
  - Correlation
  - Automation
  - Visibility and Control
- Bradford Network Sentry Family ..................................................................................5
- Addressing Network Security Challenges .......................................................................6
- Conclusion .......................................................................................................................7
- About Bradford Networks .............................................................................................8
**EXECUTIVE SUMMARY**

**Top 4 Network Security Challenges**

CIO’s and IT professionals in healthcare organizations are tasked with achieving a balance between the demand for universal access to information and the need to ensure security. In particular, four critical challenges these organizations face in terms of striking this balance include the following:

<table>
<thead>
<tr>
<th>Critical Challenges</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURING AND PROVISIONING MEDICAL DEVICES</td>
<td>The proliferation of medical devices on the network and the increasing Bring Your Own Device (BYOD) trend present unique challenges in securing and provisioning network access for these devices – ensuring that known, authorized devices are able to connect to the network, and that unknown/unauthorized devices are not.</td>
</tr>
<tr>
<td>SECURING NETWORK ACCESS FOR GUESTS AND VISITORS</td>
<td>A diverse population of guest users on the network – including visiting doctors, clinicians, and specialists, as well as patients and other &quot;guests&quot; – rely on anywhere/anytime connectivity. IT must ensure the security of the network while minimizing the administrative burden that can accompany guest management.</td>
</tr>
<tr>
<td>SECURING ACCESS TO PATIENT INFORMATION</td>
<td>Provisioning appropriate access for network users is crucial to ensuring that each user has access only to those resources for which he or she is authorized. The need for differentiated access based on each user’s “role” can place a significant management burden on IT staff.</td>
</tr>
<tr>
<td>ACHIEVING COMPLIANCE WITH REGULATORY STANDARDS</td>
<td>Healthcare organizations are subject to a number of industry and government regulations for securing electronic information. Examples include the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS). Compliance with these and other regulations requires effective systems and processes to be in place to ensure protection of confidential data.</td>
</tr>
</tbody>
</table>

Evolving security requirements in healthcare IT environments have lead to today’s network security landscape being scattered with isolated solutions deployed over time to meet specific security challenges. Each solution – including firewalls, intrusion detection and prevention systems (IDS/IPS), network access control (NAC), and others – resolves a portion of IT’s overall security objectives. However, these solutions function independently and must be individually managed, which creates additional challenges for IT organizations.

**Addressing Security Challenges with Network Access Control**

An adaptive network security approach to securing network access is a strategy for integrating various security solutions in place today – from the desktop (or “endpoint”) out to the network and security infrastructure – allowing disparate security systems to be leveraged together in a cohesive security architecture. An adaptive network security platform can be deployed into any network without having to upgrade or replace existing systems, enabling network-wide visibility, security management, and policy control functionality.

Bradford Networks’ adaptive network security platform – the Network Sentry Family – that allows healthcare IT organizations to effectively address each of the four key network security challenges, while also allowing IT staff to operate more efficiently.
AN EVOLVING NETWORK ENVIRONMENT

Studies have indicated that over 80% of all healthcare organizations have adopted wireless technologies, and over 50% are using handheld wireless devices. More than 60% are using industry-specific wireless healthcare applications. The trend to bring these applications online will continue at a rapid pace, as healthcare providers are eager to invest in technologies that promise to improve patient care. With the aggressive adoption of new wireless applications by healthcare organizations, network managers are challenged to ensure that they can deliver the reliable, highly available, and secure network infrastructure required by mission-critical applications involving patient care.

However, the challenge doesn’t begin and end with wireless networks. Requirements for 24x7 access to patient information have forced healthcare organizations to push the edges of their networks out to doctors’ homes and offices, using Virtual Private Network (VPN) technologies. Wired hospital networks are impacted as well, as switched Ethernet ports have been extended to all corners of hospitals, providing accessibility to any device with an Ethernet adapter.

Additionally, with the growth of BYOD, there is now 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.

As an 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?

With all of these new points of access to the network comes increased vulnerability to security threats, and increased risk of unauthorized access to confidential data. The evolving nature of healthcare networks creates a set of unique challenges for IT organizations in terms of securing and provisioning network access, enabling secure access for guests and visitors, securing access to patient information, and the ever-present challenge of compliance with regulatory standards.

Securing and Provisioning Medical Devices

In many healthcare networks, it is not uncommon for networked medical devices to outnumber traditional networked devices such as PCs, laptops, and printers by three to four times. A wide range of patient monitoring systems, medical imaging devices, diagnostics equipment and other medical devices require uninterrupted network connectivity.

Many of these devices are “mobile” (they are frequently moved around throughout a facility) and may be connected to the network either via wireless LANs or wired Ethernet. With this proliferation of devices, provisioning network access presents unique challenges to IT organizations in terms of network visibility, security, and asset management.

IT requires visibility throughout the network environment to know about every device that attempts to connect. Securing the network then requires that each device can be identified and that only authorized devices are able to connect successfully. Network access must be provisioned for each device type to enable connectivity to appropriate resources, and IT must have the ability to track and locate all devices throughout the network for effective asset management.

Key requirements for securing and provisioning medical devices:

- **Visibility** - Know about every device attempting to access the network
- **Security** - Ensure that only authorized devices are able to connect
- **Asset Management** - Provision network access and track devices throughout the network

Securing Network Access for Guests and Visitors

An increasingly diverse and mobile population of guests and visitors on the network makes it more difficult for healthcare IT organizations to secure their environments. Wireless networks in particular have become a necessity for visiting doctors, nurses, clinicians, specialists, as well as for patients and other “guests” who rely on anywhere/anytime connectivity.

The devices used by guests and visitors to access the network are outside of the direct control of the IT staff, and the security posture of these devices is oftentimes suspect. For example, do they have current security patches for their operating system? Are they running appropriate antivirus protection, anti-spyware protection, and firewall mechanisms? In order to minimize potential security threats, the security posture of these devices should be verified prior to allowing network access.

IT must secure the network by requiring each guest user and device to be identified and ensuring that only those that are authorized are able to connect. Network access must be provisioned for each guest or visitor to allow access to appropriate resources. Finally, guest management processes must be simplified and automated to minimize the burden placed on IT staff.
Securing Access to Patient Information

A diverse population of users and devices on the network creates challenges for healthcare IT organizations to manage the network and provision appropriate access for each user and device. Once on the network, users and devices should have access only to those resources for which they are authorized.

Users have different requirements for information, and some information (such as confidential patient data) should be accessible only on a very limited basis by users like doctors and nurses who require it. Securing patient data and other confidential information requires effective provisioning of network access privileges.

The challenge for IT organizations is that the network needs to be easily accessible to everyone and everything that belongs on it, while at the same time ensuring the security of this information. It must secure the network by requiring each user and device to be identified and ensuring that only those that are authorized are able to connect. After connecting, users must have network access provisioned based on their individual need to access specific resources and information, and this must be accomplished without placing undue management burden on IT staff.

Achieving Compliance with Regulatory Standards

Healthcare organizations are subject to a number of industry and government regulations associated with securing information on the network. Examples include the Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy rules, and the Payment Card Industry Data Security Standard (PCI DSS).

HIPAA Security and Privacy rules and their associated requirements address three important aspects of information security: identity and access control, ensuring that access to Electronically Protected Healthcare Information (ePHI) is provided only to authorized users, and systems activity reporting.

PCI DSS applies to organizations that process electronic payments. Healthcare providers frequently process electronic transactions and have patient credit card data transmitted on their networks and stored on network computers and servers. This data must be protected to the standards defined by PCI DSS.

The requirements to address compliance challenges include a combination of those discussed above, including network visibility, security, endpoint compliance, asset management, provisioning, and ease of administration. In addition, perhaps the most important aspect of addressing compliance challenges has to do with access to security data via network monitoring, logging, and reporting capabilities.
Top 4 Network Security Challenges in Healthcare

Today’s Approach to Security Must Evolve
As healthcare networks have evolved, this has created a security landscape scattered with isolated solutions that operate within their own silos, with static solutions that each resolve only a portion of IT’s overall security objective.

Most security solutions are deployed as disparate systems with limited or no integration to other network or security systems. Without integration, these solutions are not able to apply security measures in context with factors such as who is on the network, what is on the network, or when or where. In addition, these solutions often require a great deal of manual intervention to be implemented and maintained, creating additional challenges to securing and managing networks.

In order to successfully address the top four network security challenges outlined previously, today’s approach to security must evolve to a more integrated, adaptive solution.

ADAPTIVE NETWORK SECURITY

An adaptive network security platform delivers integration, correlation, and automation, as well as visibility and control, across the entire network. Each of these functions is discussed briefly below.

Integration
Many security features exist in today’s networks that are rarely if ever utilized. Security features built into existing network and security infrastructure should be highly leveraged, as each provides a valuable contribution to a comprehensive system of security. For example, multiple points of policy enforcement can be enabled by leveraging security features inherent in desktop security software, network infrastructure devices (e.g. switches and wireless controllers), and traditional security infrastructure devices (e.g. firewalls and IPS). This not only allows for more effective security, but also allows both existing and new technologies to be more effectively utilized.

Correlation
A wealth of information is gathered as a result of this integration, and correlation allows the information to be put into a proper security context. For example, an IPS typically assesses security threats based on traffic patterns between source and destination IP addresses, but provides no knowledge of what endpoint device is represented by a particular IP address. Is it a printer? A server? A laptop? This is important information, and it exists on other systems in the network. Adaptive network security enables the correlation of information from various sources so that the “big picture” can be seen.

Automation
One of the greatest challenges facing today’s IT organization is that of trying to keep up with evolving network security challenges with very limited staff resources. Adaptive network security enables automation of various configuration and management tasks performed by IT staff today, such as provisioning network access for different users and devices. This not only frees IT staff to be able to focus on more important things, but also enhances security and efficiency with the ability to dynamically adapt to network threats and changes.

Visibility and Control
By integrating with and leveraging the entire network environment, adaptive network security is able to deliver end-to-end visibility of all users and devices on the network in real-time, as well as monitor and log all network activity over time for historical views and detailed reporting capability. Utilizing this information, adaptive network security then enables network-wide management and control for enforcement of security policies throughout the network – across wired, wireless, and VPN connections – to secure and protect the network and the organization’s critical information.

The combination of these powerful functions allows an adaptive network security platform to dynamically manage security policy across the entire network, enabling capabilities including:

- Providing network-wide visibility and tracking of all users and devices
- Automatically profiling devices on the network and grouping by type
- Provisioning network access based on user identity and device type
- Assessing security posture of endpoint devices
- Isolating, or quarantining, non-compliant devices and enabling self-remediation
- Enabling policy-based access to network resources
- Monitoring ongoing behavior and enforcing security policies continuously
- Simplifying management of guest access for patients, visitors, contractors
- Delegating administration functions to off-load work from IT staff
BRADFORD NETWORK SENTRY FAMILY

Bradford’s Network Sentry family is an adaptive network security platform that leverages existing network and security infrastructure investments to deliver extensive visibility and control capabilities. By integrating with systems already in place, and correlating information from multiple systems, the Network Sentry family enables automated policy controls across the network.

The Network Sentry family is a flexible, modular security platform that is particularly well-suited to the needs of healthcare organizations. Its out-of-band architecture leverages existing network and security infrastructure investments, eliminating the need to replace existing infrastructure for improving security. This architecture also removes single points of failure, insuring maximum availability in critical healthcare network environments.

Examples of capabilities delivered by the Network Sentry family include:

- Protecting healthcare networks from unauthorized users and devices
- Ensuring that security policies are established and enforced
- Detecting and profiling managed and unmanaged devices
- Allowing role-based access to network resources
- Provisioning and managing guest access
- Maximizing existing security systems and network infrastructure
- Eliminating endpoint vulnerability
- Logging and reporting of network activity for regulatory compliance (e.g., HIPAA, PCI)

The Network Sentry Family delivers complete visibility of all users and devices on the network – identifying who and what is on the network in order to keep unauthorized users and devices out, and ensure that network assets are safe.

ADDRESSING NETWORK SECURITY CHALLENGES

The Network Sentry Family allows healthcare IT organizations to effectively address each of the four key network security challenges introduced previously, while also increasing operational efficiency by simplifying and automating a variety of operational tasks. The table below summarizes benefits that can be realized:

Securing and Provisioning Medical Devices

<table>
<thead>
<tr>
<th>KEY REQUIREMENTS</th>
<th>NETWORK SENTRY BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>VISIBILITY Know about every device attempting to access the network</td>
<td>• Monitors the network to discover and identify all devices on wired, wireless, and VPN connections.</td>
</tr>
<tr>
<td></td>
<td>• Provides real-time and historical views of connection activity (successful and unsuccessful attempts to connect).</td>
</tr>
<tr>
<td></td>
<td>• Establishes device profiles, including device type, device name, MAC address, IP address, network location, time of access, and role associated with each device.</td>
</tr>
<tr>
<td></td>
<td>• Provides total visibility of all endpoint devices – networked medical devices, as well as iPads, PCs, laptops, smartphones, VoIP phones, etc. – including rogue (unauthorized) devices.</td>
</tr>
<tr>
<td>SECURITY Ensure only authorized devices are able to connect</td>
<td>• Allows registration of all authorized devices so network can be locked down to prevent access by rogues.</td>
</tr>
<tr>
<td></td>
<td>• Automatically identifies all devices attempting to connect, identifying both known and rogue devices.</td>
</tr>
<tr>
<td></td>
<td>• Dynamically enforces security policies to allow authorized devices to connect, while quarantining (isolating) unknown / unauthorized devices.</td>
</tr>
<tr>
<td>ASSET MANAGEMENT Provision access and track devices throughout the network</td>
<td>• Automates control and management of all endpoint devices.</td>
</tr>
<tr>
<td></td>
<td>• Simplifies workflow for adding new devices to the network.</td>
</tr>
<tr>
<td></td>
<td>• Dynamically classifies and profiles all devices and provisions network access based on device type and role.</td>
</tr>
<tr>
<td></td>
<td>• Provides monitoring of network connections and tracking of all devices across wired, wireless, and VPN.</td>
</tr>
</tbody>
</table>
### Securing Network Access for Guests and Visitors

<table>
<thead>
<tr>
<th>KEY REQUIREMENTS</th>
<th>NETWORK Sentry BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SECURITY</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Ensure only authorized guests/visitors connect to the network | • Allows registration of all guests/visitors so network can be locked down to prevent access by rogues.  
• Automatically identifies all users and devices attempting to connect to the network, and discovers all rogues.  
• Dynamically enforces security policies to allow authorized guest users and their devices to connect, while quarantining (isolating) unknown / unauthorized users and devices.  |
| **ENDPOINT COMPLIANCE** |                         |
| Ensure that endpoint devices comply with security policies | • Performs endpoint compliance validation by scanning devices to validate security posture.  
• Allows device scanning to be highly customized – from very simple system checks to in-depth assessment of:  
  › Operating system type, patch levels and hotfixes  
  › Anti-virus applications and definitions version  
  › Anti-spyware applications and definitions version  
  › Required and prohibited software applications  
  › Presence and status of particular files or file types  
• Enables non-compliant devices to be quarantined (isolated).  
• Allows users remediate non-compliant devices (e.g. update OS patches or anti-virus software) and regain secure network access without having to engage IT staff.  |
| **PROVISIONING**  |                         |
| Provide guests/visitors with appropriate levels of access | • Allows creation of guest and visitor user profiles along with specific access rules to enable role-based access.  
• Automatically discovers attempts by guests/visitors to access the network and restricts or prohibits network access until security compliance is verified (e.g., user logs on and endpoint device is scanned if required).  
• Automatically provisions network access based on user profiles and pre-established access policies.  |
| **EASE OF ADMINISTRATION** |                         |
| Simplify and automate administration of guest access | • Automates administration of guest/visitor network access.  
• Simplifies workflow for creating guest profiles, registering guests, and provisioning access policies.  
• Allows for delegation and off-loading of routine administrative tasks to authorized personnel (sponsors).  
• Provides a simple interface for sponsors to create and manage guest accounts.  
• Simplifies creation of groups of guest accounts for meetings, conferences, etc. with unique login per user.  
• Automatically quarantines non-compliant guest devices and enables users to address and fix policy violations themselves without engaging IT or helpdesk staff.  |

### Securing Access to Patient Information

<table>
<thead>
<tr>
<th>KEY REQUIREMENTS</th>
<th>NETWORK Sentry BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SECURITY</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Ensure only authorized users/devices connect to the network | • Allows registration of users and devices so network can be locked down to prevent unauthorized access.  
• Automatically identifies all users and devices attempting to connect to the network, and discovers all rogues.  
• Dynamically enforces security policies to allow authorized users and devices to connect, while quarantining (isolating) unknown / unauthorized users and devices.  |
| **PROVISIONING**  |                         |
| Provision access based on identity/role of individual users | • Allows creation of unique user profiles that can be given specific access rules to enable role-based access.  
• Automatically discovers attempts by users to access the network and restricts or prohibits access until security compliance is verified (e.g., user is identified by “logging on” and endpoint device is scanned if required).  
• Automatically provisions role-based network access based on user profiles and pre-established access policies, allowing access for each user to be restricted to only systems and data for which they are authorized.  |
| **EASE OF ADMINISTRATION** |                         |
| Simplify and automate administrative tasks to reduce burden on IT staff | • Automates administration of network access and enables centralized management of the network infrastructure.  
• Dynamically provisions role-based access to the network.  
• Simplifies workflow for creating user profiles, registering users and devices, and provisioning access policies.  
• Automates moves, adds, and changes in the network.  
• Automatically quarantines (isolates) unauthorized users and devices without requiring intervention by IT staff.  |
Achieving Compliance with Regulatory Standards

<table>
<thead>
<tr>
<th>KEY REQUIREMENTS</th>
<th>NETWORK SENTRY BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETWORK MONITORING</td>
<td>• Provides ongoing monitoring of all network connections on wired, wireless and VPN.</td>
</tr>
<tr>
<td>Enable continuous monitoring of network connections</td>
<td>• Delivers total visibility across the network, with tracking of all endpoint devices and all users connecting.</td>
</tr>
<tr>
<td>DATA COLLECTION AND LOGGING</td>
<td>• Provides detailed logging and reporting of all network access activity – all connections, all devices, and all users.</td>
</tr>
<tr>
<td>Gather and store data on all network connection activity</td>
<td>• Eases burden and minimizes cost/effort of complying with regulatory requirements.</td>
</tr>
<tr>
<td>REPORTING</td>
<td>• Provides access to real-time and historical data on access activity to help to satisfy requirements of HIPAA, PCI, and other regulatory standards.</td>
</tr>
<tr>
<td>Provide real-time and historical views of data for security audits</td>
<td>• Delivers standard reports and highly-customizable reporting to adapt to needs of different organizations.</td>
</tr>
</tbody>
</table>

CONCLUSION

Healthcare environments present unique security and management challenges for IT organizations in order to secure access to network resources, to protect confidential patient information, and to ensure the network is available to all who need it. Added to this is the challenge of achieving compliance with regulatory standards such as HIPAA, PCI, and others.

Disparate security systems – or silos of security – in today’s networks do not provide healthcare IT staff with an effective solution for taking on these challenges. An adaptive network security approach is needed in order to integrate and leverage various security technologies, correlate information from multiple sources, and automate network control and security policy enforcement.

Bradford’s Network Sentry family is the platform that allows healthcare IT organizations to effectively secure and manage network access to address critical security and operational challenges.