BRADFORD NETWORKS
the smart edge

DATASHEET

NETWORK SENTRY

Bradford's Network Sentry™ greatly enhances security and automates IT operations, enabling organizations to effectively manage security policies and secure critical IT assets.

Bradford's Network Sentry™ network access control solution integrates with IT infrastructure and correlates network, security, endpoint device, and user information to provide total visibility and control over every user and device accessing your network.

Easily integrated into existing network environments, Network Sentry's out-of-band architecture leverages the inherent security capabilities of existing network equipment along with authentication and authorization technologies such as 802.1X, RADIUS and Active Directory for identity management. By leveraging existing technology investments, organizations can quickly add advanced visibility and security capabilities to their current networks and avoid the need for expensive forklift upgrades or the scalability and management challenges of adding in-line equipment.

Through an easy-to-use web interface, Network Sentry provides powerful administrative tools for managing network and security operations. Its inherent flexibility lets IT organizations gracefully evolve their security projects from initial trials to pilot rollouts to full deployments to ensure effective security policy implementations with minimal impact on user experience.

Network Sentry can be deployed either on a dedicated hardware appliance, as a virtual appliance or "in the cloud" via SaaS (Security-as-a-Service). The same functionality is delivered in all deployment models ensuring that Network Sentry can adapt to the unique needs of any network environment.

THE BRADFORD DIFFERENCE

The 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 network equipment and connecting devices eliminating the network blind spots that can introduce risk.

Drawn from Bradford's extensive experience delivering secure network access, first to educational institutions and then to organizations across all industries, Network Sentry has evolved to offer exactly what customers need:

- Visibility
- Advanced Policy Management
- Guest Access
- Device Profiling
- Secure Onboarding
- Endpoint Posture Assessment
- Centralized Management
- Flexibility
- Investment Protection

Key Benefits:

- Gain complete visibility and control over who and what is accessing your wired and wireless networks at all times
- Improve network security and asset protection
- Reduce the risk of onboarding devices
- Enable Bring-Your-Own-Device (BYOD) policy
- Streamline regulatory compliance and reporting

SARASOTA MEMORIAL
HEALTH CARE SYSTEM

"While iPads and other mobile devices are an important component to providing convenience and accessibility to clinicians and staff, this cannot come at the expense of security or compliance. A key part of our success is leveraging Bradford's NAC solution. With Bradford, we are able to provide secure and convenient network access for personal devices while achieving compliance with industry regulations such as HIPAA and HITECH."

VISIBILITY

IDENTIFY WHO AND WHAT IS ON YOUR NETWORK

Network Sentry provides visibility of every user and every endpoint device that attempts to access the network on any wired or wireless connection. Because it is tightly integrated with the entire network environment, Network Sentry provides complete visibility across the network infrastructure, right down to individual switch ports, wireless access points, and even remote connections such as VPN. An easy-to-use, web-based administrative interface features a highly-customizable "dashboard" view of vital network information, allowing administrators to "drill down" with a mouse click for more details.

- Centralized administration and reporting from one console
- Visibility of all network devices, users and endpoints
- Unique search/locate function to quickly find a device or user

ADVANCED POLICY MANAGEMENT

PROVISION AND ENFORCE GRANULAR SECURITY POLICIES

Network Sentry allows custom network security policies to be created and enforced automatically and consistently throughout the network to protect critical data and IT assets, and to ensure compliance with internal policies as well as industry and government regulations.

- **Identity-based** policies provision access based on user identity (Employee, Guest, Contractor, etc.)
- **Device-based** policies provision access based on device identity and type (IP phone, Printer, Handheld, etc.)
- **Endpoint compliance** policies allow or prohibit access based on the endpoint security posture (Up-to-date OS, Patches, Anti-virus/Anti-spyware, etc.)
- **Time-based** policies provision access based on time of day, day of the week
- **Location-based** policies allow or prohibit access based on the connection point (wired port, wireless access point)

This is just a sample of security policies that can be managed with Network Sentry. Unique policies can be created and deployed to meet the specific needs of any organization.

GUEST ACCESS

AUTOMATE AND SIMPLIFY NETWORK ACCESS FOR GUESTS

Network Sentry ensures secure network access for guest users, while simplifying and automating the creation and administration of guest accounts. Authorized sponsors can easily provision individual guest accounts as well as group accounts for meetings and conferences, removing the daily burden of guest account management from IT staff. Self-registration capabilities further simplify the workflow, allowing guests to request network access "on the fly" with sponsor approvals and account setup processed automatically. Unique login credentials (username/password) can be delivered to guests via SMS text or email on their mobile devices.

DEVICE PROFILING

DYNAMICALLY IDENTIFY AND CLASSIFY ALL ENDPOINTS

Network Sentry automatically discovers and profiles all endpoint devices and classifies them by type, greatly enhancing visibility of what is on the network and providing additional policy conditions for provisioning network access. Profiling criteria may include a combination of IP range, location, DHCP fingerprint, TCP or UDP ports, active (NMAP) and passive (p0f) fingerprinting, and vendor OUI. Device profiles can also help streamline IT workflow with automated delegation of management responsibilities by device type.

EASYCONNECT SECURE ONBOARDING

AUTOMATE 802.1X ENDPOINT SECURITY SETTINGS

For "BYOD" and guest network environments using 802.1X, Network Sentry's EasyConnect feature simplifies the process of onboarding new devices by dynamically configuring security settings on Windows, Mac OS X, iOS and Android devices. In the event a device initially connects to an open (unsecure) wireless SSID, Network Sentry can automatically configure its security settings and transparently move the device to a secure SSID.

ENDPOINT POSTURE ASSESSMENT

VALIDATE SECURITY POSTURE AND REMEDIATE AT-RISK DEVICES

The security posture of an endpoint is crucial in managing access policies. An endpoint can be known and authorized, yet still at risk – for example, if its operating system patch levels or anti-malware tools are not up to date, or if prohibited applications are installed. Network Sentry enables comprehensive endpoint scans for assessing endpoint "health" and ensuring compliance with security policies. Endpoint policies can be defined and validated by OS type (Windows, Mac OS X, Linux), and Network Sentry offers flexible options for endpoint posture assessment, including persistent and dissolvable agents as well as agentless directory-based scanning.

Remediation of non-compliant endpoints can be automated through integration with patch management systems or can be achieved by educating the end users on why they are non-compliant and/or forcing the endpoint to an isolated or limited-access VLAN. Instructions for achieving compliance can be delivered via a captive portal or displayed on the user's desktop and access can be granted once the corrective actions have been taken.

CENTRALIZED MANAGEMENT

MANAGE SECURITY FUNCTIONS THROUGH A SINGLE INTERFACE

Network Sentry empowers IT administrators with extensive management and control functionality. Features built into the existing infrastructure can be leveraged to secure the network. Control features can be accessed via the web-based administrative interface. For example, any user or device on the network can be easily located and identified with a few mouse clicks. Potential threats can be mitigated by isolating suspect users or at-risk devices, or by disabling their access completely.

In addition, control of the network environment is greatly simplified with Network Sentry and its ability to automate administrative tasks. For example, if an unknown device were to connect to a switch on the network, this event could trigger an automated alert to IT staff and the switch port could be automatically disabled or the device quarantined to protect the network.

FLEXIBILITY

A SOLUTION TO MEET EVOLVING SECURITY CHALLENGES

Network Sentry enables organizations to adapt to a wide range of business and technology challenges, and has been architected to allow security solutions to be rolled out in phases, addressing the most critical needs to start with and then phasing in additional capabilities as required. Start in "monitor only" mode for network-wide visibility. Then enforce basic "friend or foe" access control policies to secure the network. Next might be Guest access and "BYOD" security policies, followed by more advanced policy management across the network.

INVESTMENT PROTECTION

LEVERAGE THE EXISTING NETWORK INFRASTRUCTURE AND SECURITY ECOSYSTEM

By integrating with the entire network and leveraging capabilities of the current network infrastructure, Network Sentry allows organizations to maximize the potential of existing IT investments. Network Sentry is architected to adapt to changing technology environments without requiring "forklift" upgrades, future-proofing today's investment for years to come.

With an increasing mobile workforce comes a dynamic edge to today's networks. The devices, once consistent and well–managed, are now diverse and can be owned by the employee. Network Sentry provides a deep understanding of the device type, its risk profile, and the user on the device. This information is typically not readily available to the security products that detect anomalies and identify the source as an IP address. The investigation cannot stop there. Network Sentry correlates the IP address to a device type and owner to provide the level of depth needed to truly investigate security anomalies. Network Sentry can also monitor, report, or block network access using the feed from traditional security solutions such as Security Information and Event Management (SIEM) and Intrusion Detection/Prevention Systems (IDS/IPS).

Network Sentry provides extensive integration with your network and security infrastructure, authentication and directory services, and endpoint security software.

Network Infrastructure	3Com, Aerohive, Alcatel, Aruba, Brocade, Cisco, Dell, D-Link, Enterasys, Extreme, HP, Juniper, Meru, Motorola, Ruckus, SMC, Xirrus, and others
Security Infrastructure	ArcSight, Fortinet, Lancope, McAfee, NitroSecurity, Nokia, Packeteer, Palo Alto, Sonicwall, Sourcefire, Stonesoft, TippingPoint, TopLayer, and others
Authentication & Directory Services	RADIUS: All standard RADIUS servers LDAP: All standard LDAP directories
Operating Systems	Desktop: Microsoft Windows, Apple OS X, Linux Mobile: Apple iOS, Android
Endpoint Security Applications	Avast, AVG, Avira, ClamWin, DrWeb , ESET, F-Secure, GDATA , Kaspersky, Lavasoft, McAfee, Microsoft, Norton, Panda , Softwin, Sophos, Symantec , Trend Micro, Vipre, and others

DEPLOYMENT MODELS

Flexibility extends to the way in which Network Sentry can be deployed in the network -- either on hardware appliances, as a virtual appliance, or "in the cloud" via SaaS (Security-as-a-Service). The same functionality is delivered in all three deployment architectures, ensuring that Network Sentry can adapt to the unique needs of any network environment.

HARDWARE APPLIANCES

Network Sentry can be purchased on hardware appliances tailored to your specific network environment. Several versions are available, including a single stand-alone appliance as well as appliances that can support higher capacities by splitting functionality between two paired appliances – an Application Server and a Control Server. This allows for increased performance and load sharing of hardware functions. All appliances include hot-swappable dual power supplies for redundancy, including RAID 1 disk redundancy and support for optional high-availability hot-failover configurations for environments requiring the highest levels of system uptime.

VIRTUAL APPLIANCES

Network Sentry can also be deployed as an application in VMware ESX and ESXi virtual server environments. Organizations can leverage existing server infrastructure investments and the benefits of virtualization, including reductions in capital and operating costs, improvements in power efficiency and space utilization, reductions in risk of server downtime and improvements in IT staff productivity.

Virtual appliance versions of Network Sentry are similar to the hardware appliance versions. Each version requires virtual server resources (CPU, memory, etc.) equivalent to those of the corresponding hardware appliance versions.

BRADFORD.CLOUD (SAAS)

Network Sentry can also be deployed "in the cloud" via SaaS (Security-as-a-Service). With no hardware on premise, the solution has the same capabilities as the appliance and/or virtual solution that is deployed on premise. The service is offered via Bradford Networks or Managed Service Providers (MSPs) who have added Network Sentry to their portfolio of cloud-based offerings.

FLEXIBLE LICENSING OPTIONS FOR WIRED AND WIRELESS NETWORKS

Network Sentry is available in three license options to suit different needs and budgets. The Secure Mobility license focuses on wireless LANs and is ideally suited to address wireless mobility and BYOD challenges. The Secure Enterprise license secures both wired and wireless LANs, and is offered in Standard and Advanced versions to align key features with the needs of the environment. Licenses are perpetual (one-time purchase) and are consumed based on the number of concurrent endpoint devices on the network. Licenses are available in increments of 500, 1000, 2500, 5000, and 10000.

	Secure Mobility (Wireless LAN Only)	Secure Enterprise (Wireless, Wired, VPN)	
	Advanced	Standard	Advanced
Wireless LAN	✓	✓	✓
Wired LAN		✓	✓
VPN			✓
Network Visibility	✓	✓	✓
Device Identity	✓	✓	✓
User Identity	✓	✓	✓
Provisioning	✓	✓	✓
Endpoint Compliance	✓		✓
Third-Party Security Integration	✓		✓
Device Profiling	✓		✓
Advanced Guest Management	✓		✓

HARDWARE APPLIANCE VERSIONS

Hardware Appliance	Type	Target	Capacity*
NS500RX	Standalone Appliance (Integrated Control Server and Application Server)	Small Environments	Manages up to 2,000 ports**
NS1200RX / NS8200RX	Standard Appliance Pair (Separate Control Server and Application Server)	Medium Environments	Manages up to 10,000 ports**
NS2200RX / NS9200RX	High-Performance Appliance Pair (Separate Control Server and Application Server)	Large Environments	Manages up to 20,000 ports**
NS550RX	Management Appliance (Provides centralized management when multiple Foundation appliances are deployed)	Very Large Environments (Multiple appliances)	Unlimited

** Network Size information is for general guidelines only, as each network environment is unique*
*** Network ports include edge switch ports and connection capacity of wireless LAN access points / controllers*

BRADFORD NETWORKS
the smart edge

Address One Broadway, 4th Floor, Cambridge, MA 02142, USA
Toll Free +1 866.990.3799
Phone +1 617.401.2515
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 network equipment and connecting devices eliminating the network blind spots that can introduce risk.

BN-003-01-005