

Adaptive Network Security™ Platform

NETWORK SENTRY™ FAMILY

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



Bradford Networks offers a comprehensive, extensible product line through its Network Sentry™ family. Bradford's Network Sentry family integrates with IT infrastructure and correlates network, security, endpoint device, and user information to provide total visibility and control over every user and device on the network. Based upon Bradford's Adaptive Network Security platform architecture, the Network Sentry family delivers powerful security solutions capable of addressing a wide range of business challenges.

For starters, the Network Sentry family provides complete visibility of all network users and network-attached devices, allowing organizations to secure their critical IT assets and prevent unauthorized network access. Authorized network users may include internal users (e.g., corporate employees, hospital staff, or university faculty) as well as guest users (e.g., visitors, business partners, contractors and the like). Network-attached devices may include PCs, laptops, handheld PDAs, IP phones, printers, HVAC systems, medical devices, and countless other IP-enabled devices on today's networks.

The Network Sentry family enables flexible security policies and network usage policies to be created and dynamically enforced network-wide for the highest levels of security and control. At the same time, the workload on IT staff is significantly reduced by automating a range of security functions that otherwise must be performed manually by highly-skilled personnel.

Real-time and historical network activity data are logged and stored in a central database, providing a wealth of information and reporting capability for network management, security threat analysis and regulatory compliance.

BENEFITS

- GAIN COMPLETE VISIBILITY AND CONTROL
- SECURE CRITICAL IT ASSETS
- ENFORCE SECURITY POLICIES
- AUTOMATE SECURITY OPERATIONS
- ACHIEVE REGULATORY COMPLIANCE

"By providing visibility into who and what is on our network, in real-time, Bradford has given our IT staff tremendous control over our environment. We have needed a solution with this capability for many years - and it is finally here."

Mark Watson
Administrative Director, Network Services/Telecom
Susquehanna Health

MEETING TODAY'S SECURITY CHALLENGES

Identify Who and What Is On Your Network

Bradford's Network Sentry family provides visibility of every user and every endpoint device that attempts to access the network, whomever or whatever they may be and wherever and whenever they may attempt to connect.

Because it is tightly integrated with the entire network environment, the Network Sentry family provides complete visibility across the network infrastructure as well, 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.

Dynamically Provision and Enforce Security Policies

The Network Sentry family allows custom 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 industry and government regulations. Examples include:

- **Identity-based** access policies that provision network access based on user identity (Employee, Guest, Contractor, etc.)
- **Device-based** access policies that provision network access based on device type (IP phone, Printer, Handheld, etc.)
- **Endpoint compliance** policies that allow or prohibit network access based on the security posture of endpoint devices (Up-to-date OS, Patches, Anti-virus/Anti-spyware, etc.)

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

Manage Security Functions Through A Single Interface

The Network Sentry family 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 the Network Sentry family 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 quarantined to protect the network.

Leverage Your Existing Network Infrastructure

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

Customize A Solution to Fit Your Security Challenges

Leveraging Bradford's Adaptive Network Security architecture, the Network Sentry family can be deployed in a variety of ways to address a wide range of business and technology challenges, and it can adapt dynamically to changing environments. The Network Sentry family has been architected as a modular platform that allows a number of distinct feature sets to be deployed individually or in combination to meet the requirements of different organizations. Its modular architecture allows security solutions to be rolled out in phases, addressing the most critical needs to start with and then phasing in additional capabilities as required.

www.bradfordnetworks.com/ANS

ADAPTIVE NETWORK SECURITY™

Today's IT organizations must make networks more accessible to both internal and external users and an ever-increasing variety of networked devices. This intensifies the demands placed on network security and complicates IT operations, driving the need for network security solutions that are dynamic and can adapt easily to changing environments. Bradford's Adaptive Network Security (ANS) platform delivers integration, correlation, and automation, as well as visibility and control, across the entire network.

- **Integrate** with desktop security software, directories, network infrastructure and third-party security systems to provide unparalleled visibility and control across the network environment.
- **Correlate** data including identity of users and devices, security posture of endpoint devices, time of day, physical location, and other information to produce a comprehensive view of the entire network.
- **Automate** security and IT operations duties — such as identifying and classifying everything on the network, validating compliance of users and devices with pre-defined security policies, and enforcing network access policies — to ensure network-wide security, while alleviating IT staff from having to perform many manual tasks. Automated logging of historical network activity provides a wealth of data for security management and reporting.

The combination of these powerful functions enables Bradford's ANS Platform to orchestrate multiple security functions and dynamically manage security policy across the entire network.

PRODUCT FAMILY

The Network Sentry product family leverages Bradford's Adaptive Network Security architecture to deliver a highly-flexible security platform. The Network Sentry family consists of Foundation appliances and software-based Solutions and Extensions which can be deployed in any combination to meet the needs of a particular environment.

Foundation

The Network Sentry Foundation consists of a hardware appliance or set of appliances with built-in software capabilities. It is the intelligent base upon which additional functionality is added via Solutions and Extensions. Built in functionality includes:

- Visibility of all network connections (MAC, IP, location)
- Network management and control
- Automated actions triggered by network events
- Directory integration for administrative user accounts
- Management console using web-based admin interface
- Historical connection logs (time, location, MAC, IP)
- Logical grouping of network devices, ports, administrators

Solutions

Solutions are feature sets that are licensed on a per-user or per-device basis to address specific needs. One or multiple types of solution licenses can be added onto the Network Sentry Foundation. Available solutions include Access Manager, Guest Manager, Shared Access Tracker, and Device Tracker.

ACCESS MANAGER provides visibility and control of all users and their endpoint devices.

- Manage and monitor all access activity
- Associate all endpoint devices to users
- Authenticate all network users
- Enforce role-based network access policies
- Prevent unauthorized network access
- Generate reports on users and/or their devices

GUEST MANAGER ensures secure network access for guest users and simplifies the administration of guest accounts.

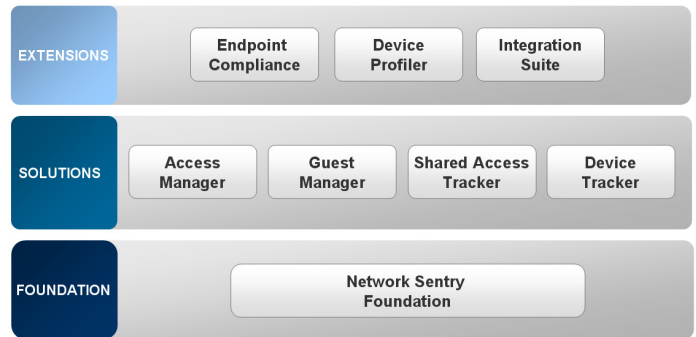
- Easily register and manage guests and their devices
- Prevent unauthorized network access
- Enforce role-based network access policies
- Simplify administration of guest accounts
 - » Delegate guest management to non-IT staff
 - » Provide self-service registration for guests
 - » Easily manage access for groups / conferences
- Generate reports on guest activity

SHARED ACCESS TRACKER allows secure, role-based access for users of shared workstations, along with tracking usage and activity.

- Monitor use of shared-access systems
- Authenticate users to ensure secure access
- Enforce role-based access policies
- Prevent access by unauthorized users
- Generate reports on user activity

DEVICE TRACKER locks down the network to allow only known networked devices, and tracks activity of all known devices.

- Secure the network and monitor all access activity
- Prevent access by rogue devices
- Locate and track all identified devices on network
- Enforce access policy by device type
- Generate reports on network activity



NETWORK SENTRY PRODUCT FAMILY

Extensions

Extensions are additional feature sets that are enabled with a one-time activation key. One or multiple types of extensions can be added to further enhance Solutions. Available extensions include Endpoint Compliance, Device Profiler, and Integration Suite.

ENDPOINT COMPLIANCE enables validation of security posture of endpoint devices.

- Create device security policies
- Validate security policies by OS type (Windows, Mac, or Linux)
- Deploy dissolvable or persistent agents
- Send broadcast alerts, emergency notifications
- Generate endpoint compliance reports

DEVICE PROFILER provides dynamic profiling/classification of what's on the network.

- Automatically discover devices and classify them by type
- Delegate device management to non-IT staff (by device type)
- Generate logs and reports on all device connections

INTEGRATION SUITE allows integration of multiple systems to enhance security & control.

- Integrate with third-party security systems (IDS, IPS, NBA, etc.)
- Correlate device information (IP address, MAC address, location)
- Automate policy enforcement
- Create user-customized integrations
- Detailed logs and reporting

A PROVEN LEADER IN SECURING TODAY'S HETEROGENEOUS NETWORKS

Bradford's powerful and innovative security solutions are based on years of expertise in network security. Since the company's founding in 1999, hundreds of customers and millions of users have come to rely on our technology to secure critical IT assets and automate IT security operations. With solutions that dynamically adapt to changing network conditions and continually combat network threats, Bradford addresses the security needs of a wide variety of organizations in markets including education, financial services, state and local government, healthcare, energy, retail and many others.

Bradford sells its solutions worldwide through a network of authorized Channel Partners. Our Certified Delivery Partners and Bradford's own highly-skilled Services and Support organization provide the information, tools, expertise and resources needed to ensure successful implementation and integration of Bradford solutions in your environment. 7x24x365 support capabilities and an extensive set of professional services are available to meet your organization's needs.

Bradford's innovative, award-winning products and solutions are widely recognized by industry analysts including Forrester and Gartner, as well as leading publications including SC Magazine, CRN, and others.

Learn more by visiting us at www.bradfordnetworks.com



CAROLINA ADVANCED DIGITAL, INC
IT INFRASTRUCTURE | SECURITY | MANAGEMENT

www.cadinc.com | 800.435.2212



Address	162 Pembroke Road, Concord, New Hampshire 03301, USA
Toll Free	+1 866.990.3799
Phone	+1 603.228.5300
Fax	+1 603.228.6420
Email	info@bradfordnetworks.com