

NETWORK SENTRY™ EXTENSION

INTEGRATION SUITE

Allows integration of multiple systems to enhance security & control

Today's networks are secured using a variety of purpose-built solutions that function independently in their own silos. Examples include firewalls, intrusion detection and prevention systems (IDS/IPS), network behavior analysis (NBA), data loss prevention (DLP), security information and event management (SIEM), endpoint security software, and security functions built into network devices such as switches and wireless controllers.

These static solutions each address part of an organization's overall security needs, but no single solution can do all that is needed. This presents unique challenges for IT organizations in terms of managing various security systems, while trying to extract as much value as possible from these technology investments.

What is lacking in the security silos that exist in the network is a way to integrate the functions of different systems in a way that "best of breed" technologies can be brought together to provide even greater security impact. This would not only enhance security and control in the network, but also allow IT organizations to maximize the value of existing technologies.

Bradford Networks' Integration Suite extension allows its Network Sentry family to be integrated with other security systems in the network environment and to leverage the unique capabilities of each system. Standards-based communication with other security systems allows Integration Suite to collect and share information. New information collected can be correlated with what Bradford's Network Sentry already knows about the network, its users, and devices to enable better-informed security policy decisions.

When deployed in combination with other solutions in Bradford's Network Sentry family, Integration Suite greatly enhances the collection and correlation of information that can be used to automate advanced security controls throughout the network.

Standards-based Approach

Utilizes industry standard protocols, including SNMP and Syslog.

Bi-directional Integration

Receives information and shares information with third-party systems.

User-Customizable Functionality

Allows administrative users to create custom integration capabilities.

Automated Security Controls

Enables automated actions to take place in response to third-party information. (e.g., a network port could be disabled in response to a threat alert from an IPS)

Logging and Reporting

Provides detailed data for reporting to satisfy internal and external regulations.

CHALLENGE

Lack of technology integration among various security systems in the network limits overall security and control.

SOLUTION

Customizable integration capabilities allowing multiple technology investments to be leveraged to their fullest potential.

BENEFITS

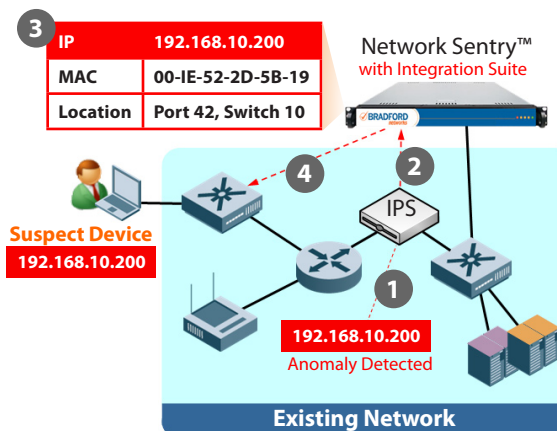
Enhanced network security and control, and greater investment protection.

- Integrate with third-party security systems (IDS, IPS, NBA, etc.)
- Correlate information from different sources
- Create user-customized integrations
- Automate security policy enforcement

HOW IT WORKS

Integration Suite can be utilized in a variety of ways depending on the network environment. As an example, consider a network in which an intrusion prevention system (IPS) is deployed to detect security threats. Network Sentry with Integration Suite enhances the capabilities of the IPS and can stop threats at the network edge where devices connect.

- 1 IPS detects an anomaly on the network and identifies a suspect IP.
- 2 IPS notifies Network Sentry of the event and the suspect IP.
- 3 Network Sentry correlates the suspect IP to its MAC and location on the network (switch port or wireless access point).
- 4 Network Sentry takes action based on pre-defined policies. For example;
 - Send an alert to IT staff with the suspect IP, MAC, and location
 - Automatically disable the network connection of the suspect device



When Integration Suite is deployed in combination with other solutions in Bradford's Network Sentry family, information about an individual endpoint device and its user can be correlated with the threat information collected from the IPS. In this scenario, Network Sentry would be able to identify not only the location on the network where the threat originated, but also the specific endpoint device (identified by type, hostname, etc.) as well as the identity of the user of that device. This information gives network and security staff a much more complete set of data to use in dealing with the threat and preventing future occurrences.

A NETWORK SENTRY™ FAMILY EXTENSION

Integration Suite is one of three feature set Extensions in Bradford's Network Sentry™ family, an Adaptive Network Security platform that greatly enhances security and automates IT operations. The Network Sentry family consists of Foundation appliances, along with software-based Solutions and Extensions which can be deployed in combination to meet the needs of any environment.

OUT-OF-BAND ARCHITECTURE LEVERAGES EXISTING NETWORK

Bradford's Network Sentry family utilizes a unique out-of-band architecture that leverages the network infrastructure—including switches, wireless access points and controllers—and correlates information to enforce security policies at the network edge. No forklift upgrades or major network configuration changes are required. The Network Sentry family integrates with network equipment from all major manufacturers, so there is no technology lock-in.

UNMATCHED VENDOR INTEROPERABILITY

The Network Sentry family integrates with an extensive range of network and security infrastructure equipment, operating systems, and security applications, and leverages unique features and properties of each element to maximize overall network security*.

Network Infrastructure	Switches, Routers, Wireless Controllers and Access Points from dozens of leading vendors
Security Infrastructure	IDS/IPS, NBA, SIEM, DLP, and other 3rd-party security systems
AAA, Directory Services	RADIUS, LDAP-based directory services, and other AAA services
Host Operating Systems	Microsoft Windows, Apple Mac OS X, and Linux
Endpoint Security Suites	Anti-virus, anti-spyware and other host security software suites from dozens of vendors

*Integration capabilities highlighted above may require the purchase of additional Solutions or Extensions from the Network Sentry family.



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

Bradford Networks is a proven leader in securing today's heterogeneous networks. Bradford's adaptive security platform fortifies networks and leverages features from existing infrastructure to dynamically enforce policies across both wired and wireless networks. Bradford solutions uniquely identify and profile every device and every user to provide complete visibility and control. Hundreds of customers and millions of users worldwide rely on Bradford to secure their critical IT assets and automate security operations. Bradford Networks is headquartered in Concord, NH and is privately held.

Copyright © 2010 Bradford Networks. All rights reserved. Printed in USA. Bradford Networks and the logo are registered trademarks of Bradford Networks in the United States and/or other countries. Adaptive Network Security, Network Sentry, Campus Manager and NAC Director are either trademarks or registered trademarks of Bradford Networks or one of its affiliated companies in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Bradford Networks reserves the right to change, without notice.