

NETWORK SENTRY™ SOLUTION

DEVICE TRACKER

Enables network “lockdown” by allowing only known devices on the network, while providing network-wide visibility and tracking all connection activity

IT organizations have made great strides in providing “anywhere, anytime” access to network resources, and as a result today’s networks are easier to access and easier to use than ever. However, this can also mean that unknown, unauthorized devices can quickly and easily connect to the network – introducing significant security risks. So how can networks be “locked down” for security, while still providing easy connectivity for known devices? And how can network connections be monitored and managed effectively?

With Device Tracker from Bradford Networks, only known and authorized endpoint devices are allowed access to the network, and access policies can be customized for each type of device. By automatically enforcing those policies, Device Tracker ensures that each device gets access only to the designated resources assigned to it.

Unknown, unauthorized devices can be blocked automatically to secure the network, while alerting IT and/or Security staff of attempted intrusions. Device Tracker monitors and tracks devices that connect to the network, providing complete visibility of all access activity. This enables real-time detection of “rogue” devices with the ability to dynamically block them from the network, essentially “locking down” the network from unauthorized use.

Additionally, Device Tracker stores records of all activity, maintaining detailed audit trails and logs, and enabling customized reports to be generated for internal use, as well as for external reporting for regulatory compliance.

Device Registration

Registration of all known devices that are authorized to connect to the network.

Isolation of Unknown/Unauthorized Devices

Keeps unknown/unauthorized devices off the network.

Access Policy Enforcement

Enforces access policies by device type for all authorized devices.

Detailed Historical Reporting

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

CHALLENGE

Ability to identify, manage and monitor all known endpoint devices connecting to the network.

SOLUTION

Automated discovery and authorization of endpoint devices connecting to the network, along with provisioning of network access based on device type.

BENEFITS

Enhanced security and control with complete visibility of every device connecting to the network.

- Locate and track all devices on network
- Enforce role-based access for all known devices
- Prevent unauthorized network access
- Isolate and block rogue devices
- Manage and monitor network access activity
- Log all connection history and generate reports

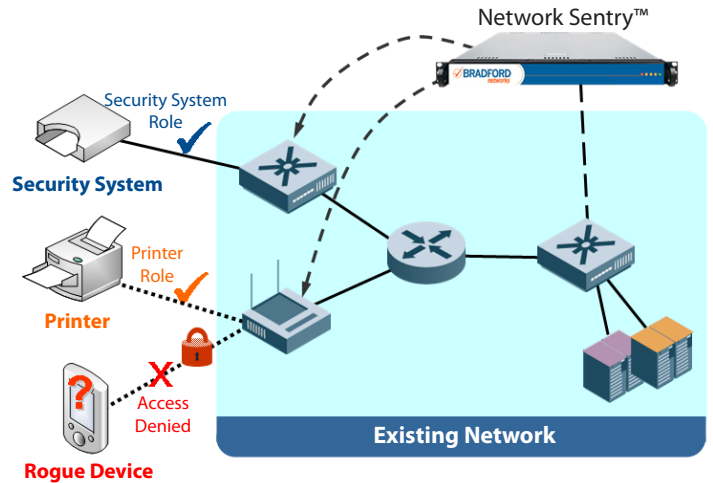
HOW IT WORKS

When a device attempts to connect to the network via a wired port or wireless access point, the Bradford system ensures the device is known and authorized to connect, and determines if there are particular access restrictions associated with the type of device.

If the device is known and authorized, the Bradford system instructs the switch or wireless controller to allow network access with the ability to set access privileges based on the type of device.

If a device is physically disconnected from the network and a new connection is attempted in its place, the authorization process will be initiated again for the new connection attempt. This ensures that an unauthorized device cannot gain access by simply being connected in place of an authorized device.

If an unknown (“rogue”) device is detected, the Bradford system prevents network access by instructing the switch or wireless controller to isolate or disable the physical connection. An alert can also be sent to let IT know that an unauthorized device has attempted to access the network.



A NETWORK SENTRY™ FAMILY SOLUTION

Device Tracker is one of four core Solutions 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.