FireEye Fuel Technology Alliances

FireEye and Bradford Networks

Enabling Visibility and Protection Across All Devices on The Network

FireEye Confidential

Bradford Networks information

- **Solution Category:** Mitigation—Network Access Control (NAC)
- **Product Name:** Network Sentry
- **Product Alignment:** FireEye NX Series, Web Security Platform

Product information

- **Target Market:** Enterprise
- **Vertical Market:** Education, Healthcare, Financial services, Energy, Retail , Government
- **Geo Territory:** Global

Key competition

- ForeScout: Control Fabric (Global)
- Cisco: Cisco SNS NAC (Global)
- Juniper: Unified Access Control (UAC) (Global)
- Aruba: ClearPass (Global)

BRADFORD NETWORKS

Customer needs

In today's organizations, users increasingly use a wide range of mobile consumer devices including smartphones, tablets, and laptops to access the company network. While many companies are embracing bring your own device (BYOD) strategies to increase productivity, reduce costs, and drive employee satisfaction, IT departments have little visibility and control over such users and BYOD devices, complicating network security and introducing significant risk.

Gaining visibility into all the users and devices on the network is the first step to enabling secure access. BYOD solutions must be able to automate detection, validate advanced malware, as well as intelligently identify registered users, guests, and devices. BYOD solutions must then be able to consistently and automatically respond to infections by applying role-based security policies across both wired and wireless segments, and take the necessary action to prevent and remediate security breaches.

- Protection across corporate devices and the BYOD domain
- Secure network access without hampering productivity
- Automate detection and apply role-based security policies

FireEye and Bradford Networks

Bradford Networks™ and FireEye® offer an integrated BYOD security solution that provides organizations with visibility and protection from stealthy Web and email threats that attempt to access the network via corporate-issued and personal BYOD mobile devices.

Bradford Networks' Network Sentry solution enables IT staff to effectively manage network access for many different types of personal and corporate owned mobile devices and categories of users with a minimal investment of time and effort. Depending on the device type, user, location, and other parameters, Network Sentry provides dynamic network access to the appropriate network resources and applications while protecting intellectual property and critical infrastructure from unauthorized use. Employees, consultants, contractors, and guests can use their preferred devices to become more mobile and productive without putting the organization at risk.

- Automated Security Solution
- Ability to use preferred devices to enhance productivity
- Advanced quarantining of compromised endpoints
- Network Access management with minimal time investment
- Dynamic network access to resources

Customer benefits

Automated, rapid response: Automatically correlates user, device, and location information with newly or previously compromised device's IP address for immediate detection and remediation

Auto-quarantine: Upon detection automatically removes or isolates non-compliant or compromised devices from the production network

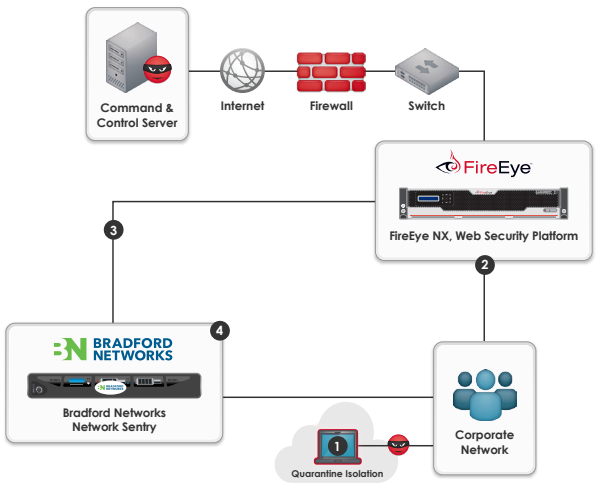
Reduced Total Cost of Ownership (TCO): Increases security by automatically processing FireEye-scanned endpoints

Enforces access policies based on user and device profiles to cut IT management overhead

Integration advantage

- Rapid detection of systems and users
- FireEye detects and blocks outbound malware transmission
- Network Sentry applies pre- defined policy to remediate problem
- Supports all brand of network equipment
- Eliminates network blind spot

Network Diagram



1. A compromised system connects to the corporate network and attempts to call home
2. FireEye blocks callback
3. FireEye alerts Bradford Networks' Network Sentry of the infected system
4. Bradford Networks' Network Sentry correlates IP address user name and device details to identify location and then isolate the device

Use cases

Network Access Control (NAC) support

- Monitor and notify scenario—no automatic enforcement
- Automatic remediation by taking the device off the network completely

Customer win example

Vertical Industry: Oil/Energy

Location: North America

Reason for Integration: Pre connect posture assessment, associating users to devices, building complete network and endpoint inventory.

The FireEye technology identifies post-connect anomalies, notifies and configures Bradford Networks to move the compromised device to quarantine.

Contacts and more information

FireEye partner external email alias:
Alliances@FireEye.com

FireEye website partner link:
www.FireEye.com/partners/index.html