FireEye Fuel Technology Alliances

FireEye and Bradford Networks

Enabling Visibility and Protection across all Devices on the Network

Key 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

Integrated Solution

- 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

The FireEye platform and Bradford Networks integration enables the rapid isolation of infected systems in the event of an advanced cyber-attack. The solutions work together to enforce advanced isolation policies to reduce the scope of an attack.

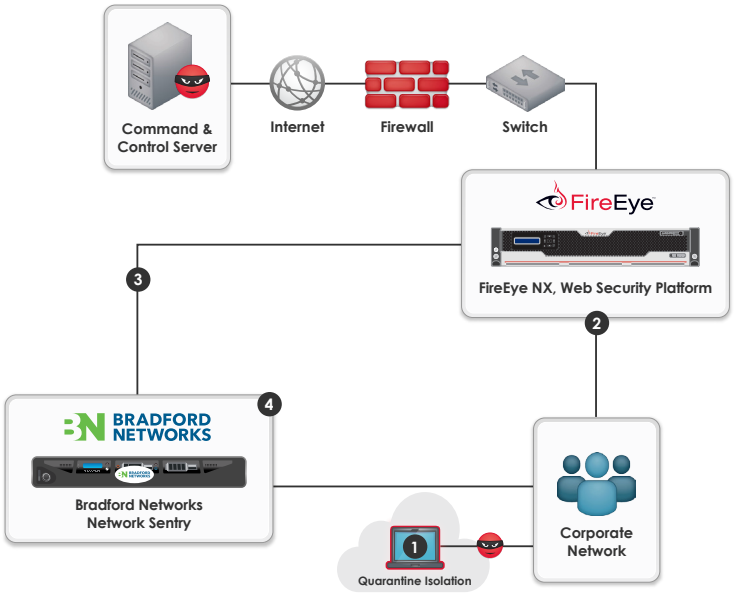
The challenge of BYOD

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, 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. Solutions must be able to automate detection, validate advanced malware, as well as intelligently identify registered users, guests, and 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.

How the joint solution works

Network Sentry automatically identifies and profiles all devices and all users on a network—providing visibility into who, what, where, and when someone connects to the network—and then provisions network access based on pre-defined security policies. The FireEye platform is designed to ensure the devices are not infected with today's new breed of cyber-attacks, such as zero-day threats and APT attacks. If a device becomes infected on the network, the FireEye MPS automatically detects and blocks the infected device then sends the compromised IP address via



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

For more information, contact Alliances@FireEye.com

Syslog to Network Sentry. Network Sentry correlates the IP address with its endpoint inventory of every connected device, which includes details such as user name, location (switch and port connection point) and time of connection, to accurately locate the infected device.

About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,500 customers across more than 40 countries, including over 100 of the Fortune 500.

About Bradford Networks

Bradford Networks offers the best solution to enable secure network access for corporate issued and personal mobile devices. The company's flexible Network Sentry solution 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.

www.bradfordnetworks.com