



FireEye and Bradford Networks

NX Threat Prevention Platform and Network Sentry/RTR

SECURITY
REIMAGINED

INTEGRATED SOLUTION AT A GLANCE

- Network Visibility:**
Identify every endpoint and networking device, user and its connection to the network, thereby eliminating network blindspots
- Contextual Information for Security Events:** Correlate user, device, and applications with newly or previously compromised endpoint to provide a broader perspective of the business risk and impact
- Rapid Threat Response:**
Apply policies to isolate, restrict, or block compromised endpoints from the network in real-time
- Bridge the gap between SOC and NOC:** Automate workflows between the SOC and NOC to eliminate dependency, complexity, and latency associated with human interaction
- Accelerate Forensic Investigations:** Provides long-term system audit logs for analysis to simplify and accelerate cyber threat investigations.

Comprehensive Visibility and Rapid Threat Response across all Endpoints to reduce threat containment time from days to seconds

OVERVIEW

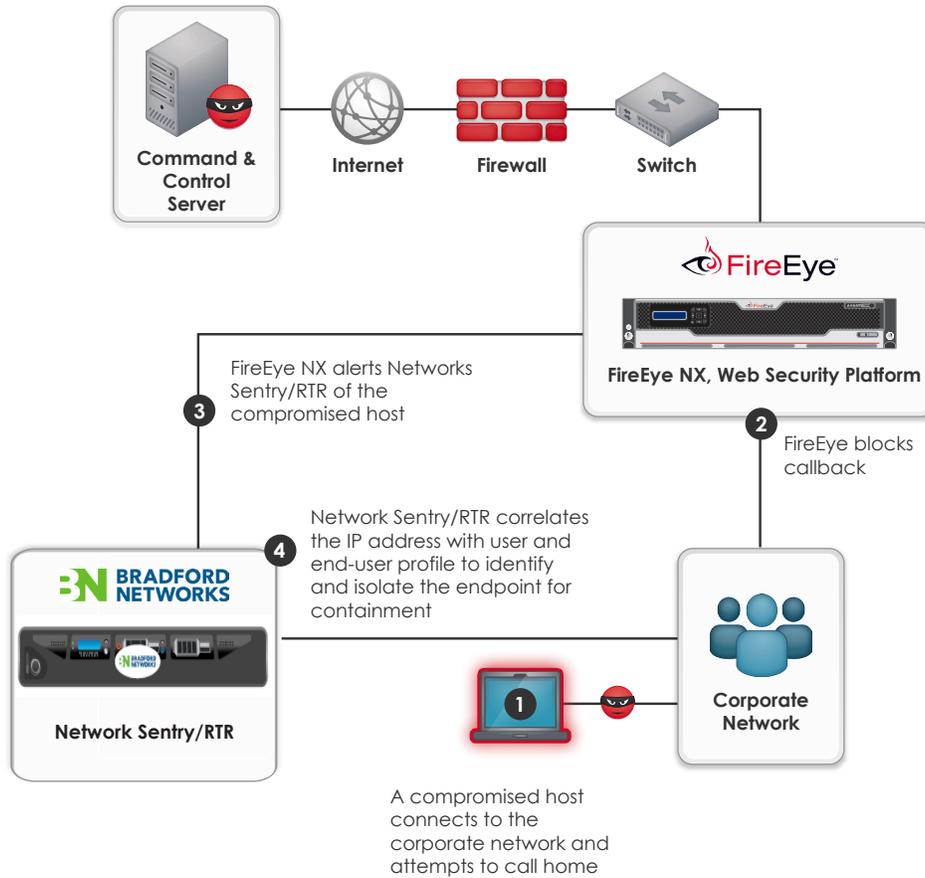
In recent years, organizations have moved away from being solely dependent upon traditional signature based security solutions to a more holistic approach towards security that also includes rapid containment and remediation of compromised endpoints. Amid an explosion of bring-your-own-device (BYOD), Internet of Things (IoT), and increasingly advanced cyber-attacks, the average breach lasts for 229 days before being detected. Going beyond simply preventing and detecting threats, companies need a proactive plan to contain and resolve them.

The integration between the FireEye NX Threat Prevention Platform and Bradford Networks' Network Sentry/RTR solution enables detection and containment of compromised endpoints in the event of a cyber-attack. The combined solution leverages the Multi-Vector Virtual Execution (MVX) technology from FireEye and flexible endpoint containment policies from Bradford Networks to mitigate adverse impact of cyber threats.

HOW THE JOINT SOLUTION WORKS

Bradford Networks' Network Sentry/RTR leverages its unique Live Inventory of Network Connections (LINC) to automatically correlate FireEye detected security events with detailed user, application, and network connection information to identify critical threats. Armed with this information, Network Sentry/RTR for FireEye triggers an automated workflow and response based on the severity and business criticality of the identified threat.

Network Sentry/RTR bridges the gap between the Security and Networking teams by automating the workflow to contain and remediate compromised or vulnerable endpoints – thereby minimizing threat response times from days to seconds. The granularity of rapid threat response can be customized to fit the business needs. For example, a high-fidelity security event tied to an endpoint of a company employee can trigger a VLAN re-assignment and redirect the compromised endpoint to a customized portal for remediation. The same security event tied to a contractor's endpoint can trigger the termination of the network connection. Bradford Networks' support for a wide variety of networking infrastructure equipment enables rapid containment of desktops, laptops and mobile devices connected to the corporate network.



ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise – reinforced with the most aggressive incident response team – helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 2,700 customers across 67 countries, including over 157 of the Fortune 500.

ABOUT BRADFORD NETWORKS

Bradford Networks is the leading provider of rapid threat response solutions that minimize the risk and impact of cyber threats. The company's patented Network Sentry solution enables Cyber Security Teams to continuously assess the risk of every user and endpoint on the network, and automatically remove vulnerable and compromised devices that act as backdoors for cyber criminals. Through its SmartEdge Platform, Network Sentry seamlessly integrates with the leading Advanced Threat Detection solutions to correlate high-fidelity security alerts with a threat's foothold. This unique correlation bridges the silos of security, network, and endpoint information to enable confident, automated threat containment before it has an adverse impact on the business. Visit www.bradfordnetworks.com for more information.