SOLUTION BRIEF

FireEye and Bradford Networks

Threat Analytics Platform and Network Sentry/RTR

SECURITY REIMAGINED

INTEGRATED SOLUTION AT A GLANCE

- **Accurate Threat Detection:** Threats are detected based on Rules, Intelligence and Analytics
- **Correlation with Business Context:** Enhances security alerts by adding business context details to security alerts
- **Applied Threat Intelligence:** Applies FireEye threat intelligence, including threat actors, to all customer generated data sent to TAP
- **Risk Prioritization:** Security alerts are prioritized and made visible based on risk to highlight important alerts
- **Shortened Threat Response Time:** Access and analyze all data relevant to a security alert to qualify that alert in minutes
- **Immediate Time to Value:** Cloud-based solution can be deployed rapidly with minimal resources

Provide additional context around security events by importing Live Inventory of Network Connections (LINC) from Network Sentry/RTR.

OVERVIEW

The FireEye Threat Analytics Platform (TAP) is a cloud-based solution that enables security teams to identify and effectively respond to cyber threats by layering enterprise generated event data with real-time threat intelligence from FireEye. The FireEye Threat Analytics Platform delivers prioritized alerts to help accelerate and enhance incident response. The platform quickly determines the scope of a suspected incident so that the security teams can respond appropriately. It provides the ability to pivot into any field within a security alert to identify related users, endpoints, and attacker profile.

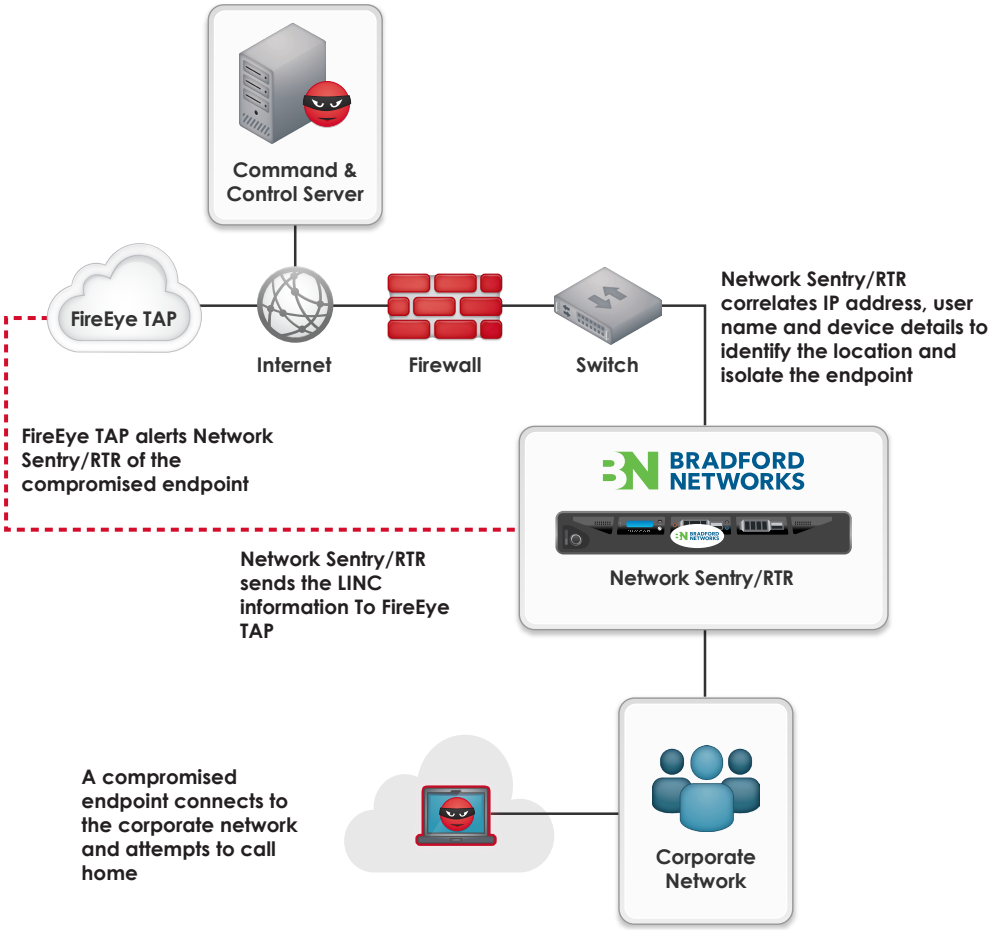
Network Sentry/RTR limits cyber threat's impact by minimizing the response time once a compromised host is identified. Network Sentry/RTR leverages its unique Live Inventory of Network Connections (LINC) to automatically correlate high fidelity security alerts from FireEye Threat Detection Platform (NX Series) and FireEye Threat Analytics Platform, with detailed contextual information on compromised hosts, users and applications. Once identified, Network Sentry/RTR triggers an automated response, based on the severity and business criticality of the incident, to contain compromised hosts in real-time.

HOW THE JOINT SOLUTION WORKS

TAP seamlessly correlates security alert against the network connections data forwarded by the Network Sentry/RTR, and pinpoints compromised host – thereby enabling rapid threat response triage and bridging organizational and informational silos.

The joint solution enhances security alerts by adding business context details such as user name, functional group, device type, operating system and additional devices owned by the same user, installed applications, specific wireless access point or wired switched port, connection duration and location of the network connectivity request.

When FireEye TAP triggers a security alert, Network Sentry/RTR automatically takes a response action on the compromised host, such as blocking or restricting network access, isolating the host in a different VLAN, or sending an informational message to instantly contain the threat in real-time and minimize its impact. Network Sentry/RTR does not require a persistent agent and can contain all leading desktop platform and mobile devices by leveraging the existing networking infrastructure.



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 2,500 customers across 65 countries, including over 150 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. Bradford Networks' network security solutions are used by more than 900 enterprise customers worldwide in markets such as healthcare, financial services, retail, government, education and more.

For more information, please visit www.bradfordnetworks.com

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**

FireEye