FireEye Mobile Threat Prevention (MTP) and Bradford Networks

Application Visibility and Rapid Threat Response for Mobile Devices to Mitigate Cyber Threats

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

- **Application Visibility:** Gain full visibility of all apps running on mobile devices.
- **Threat assessment for Mobile Apps:** Identify malicious apps on Android and iOS devices with next-generation threat detection technologies.
- **Rapid Threat Response for Mobile Devices:** Contain and isolate mobile devices that exceed the established threshold value for mobile apps.

OVERVIEW

As mobile devices increasingly become the de facto productivity platform for organizations, they have become the prime target for cyber criminals to steal private and sensitive information via malicious apps. Though gaining visibility into the apps running on a mobile device is the first necessary step towards mitigating the impact of these attacks, a comprehensive solution also requires detection and prevention of mobile threats along with rapid threat response to contain the compromised device.

FireEye Mobile Threat Prevention (MTP)™ identifies and stops mobile threats by executing apps within the FireEye Multi-Vector Virtual Execution (MVX)™ engine to protect mobile devices against compromise. FireEye Mobile Threat Prevention (MTP) offers real-time visibility of threats on mobile devices, displays play-by-play analysis of suspicious apps, provides an index of pre-analyzed apps, and generates threat assessments for custom apps.

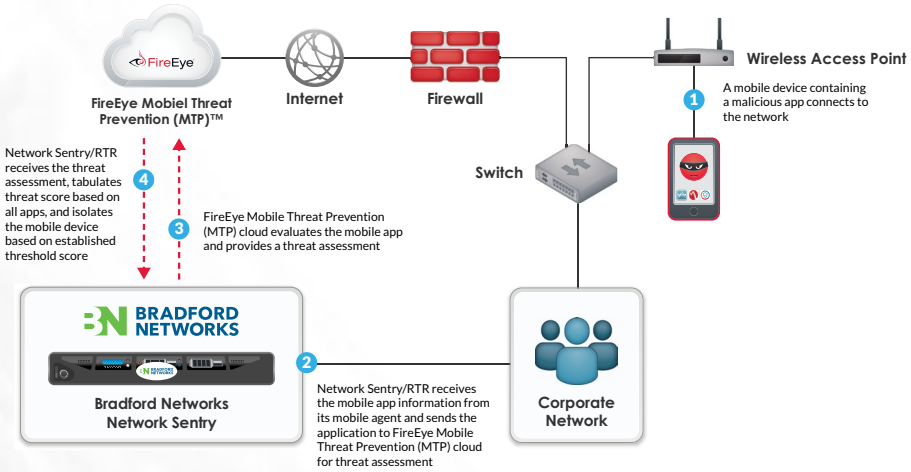
Network Sentry/RTR™ from Bradford Networks limits the impact of malicious apps by compiling the threat score of a mobile device, and dramatically reducing the containment time of the impacted device.

THE CHALLENGE

Traditional incident response is a manual process that can take days of traversing disparate security tools, IT domains, and endpoints. The challenge for IT security professionals is to identify and deploy complementary solutions that can work together effectively to automate the incident response process for cybersecurity teams, eliminate the barriers that delay investigations, and reduce the impact and remediation costs of an advanced targeted attack.

THE INTEGRATED SOLUTION

Bradford Network Sentry/RTR leverages its unique Live Inventory of Network Connections (LINC) to correlate high fidelity security alerts automatically from FireEye Mobile Threat Prevention (MTP) with detailed contextual information on compromised endpoints, 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 devices in real time. Network Sentry/RTR also provides detailed historical information on all network connections, giving security experts unprecedented forensics to help fully understand and investigate the threat's methodology, lifecycle, and scope.



FIREEYE PRODUCT AND VERSION

FireEye Mobile Threat Prevention (MTP)™

BRADFORD NETWORKS PRODUCT

Bradford Network Sentry/RTR™

HOW THE JOINT SOLUTION WORKS TOGETHER

Bradford Network Sentry/RTR's mobile agent builds an inventory of mobile apps on the mobile device and communicates that information to Network Sentry/RTR. Network Sentry/ RTR queries FireEye Mobile Threat Prevention (MTP) cloud for assessment of mobile app threats. FireEye Mobile Threat Prevention (MTP) evaluates the application, conducts dynamic analysis (including various malware parameters and contextual correlation), and returns threat score to Network Sentry/RTR.

The Network Sentry/RTR tabulates the cumulative threat score for mobile apps, and if the score exceeds the threshold value, the impacted mobile device is contained or isolated in real-time by sending appropriate commands to the networking gear like a switch or a router. Bradford Networks' support for a broad range of networking infrastructure equipment enables rapid containment of mobile devices, laptops, and desktops connected to the corporate network.

The granularity of containment can be customized to fit the business needs. For example, a compromised mobile device of a company employee can trigger a VLAN re-assignment and redirection to a customized portal for remediation. On the other hand, a compromised mobile device of a contractor can trigger termination of network connection to the corporate network.

THE VALUE OF THIS PARTNERSHIP

The integration between the FireEye Mobile Threat Management (MTP) and Bradford Networks' Network Sentry/ RTR solution enables complete visibility into applications running on a mobile device. Based on the verdict of one or more mobile apps from the FireEye Mobile Threat Management (MTP) cloud, the integrated offering allows mutual customers to contain and isolate a mobile device that exceeds a set threat score.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

ABOUT BRADFORD NETWORKS

Bradford Network's Network Sentry solution enables cyber security teams to assess the risk of every user and endpoint on the network continuously 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.

For more information contact CSC@fireeye.com.

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