SOLUTION BRIEF

Bradford Networks and Cyphort

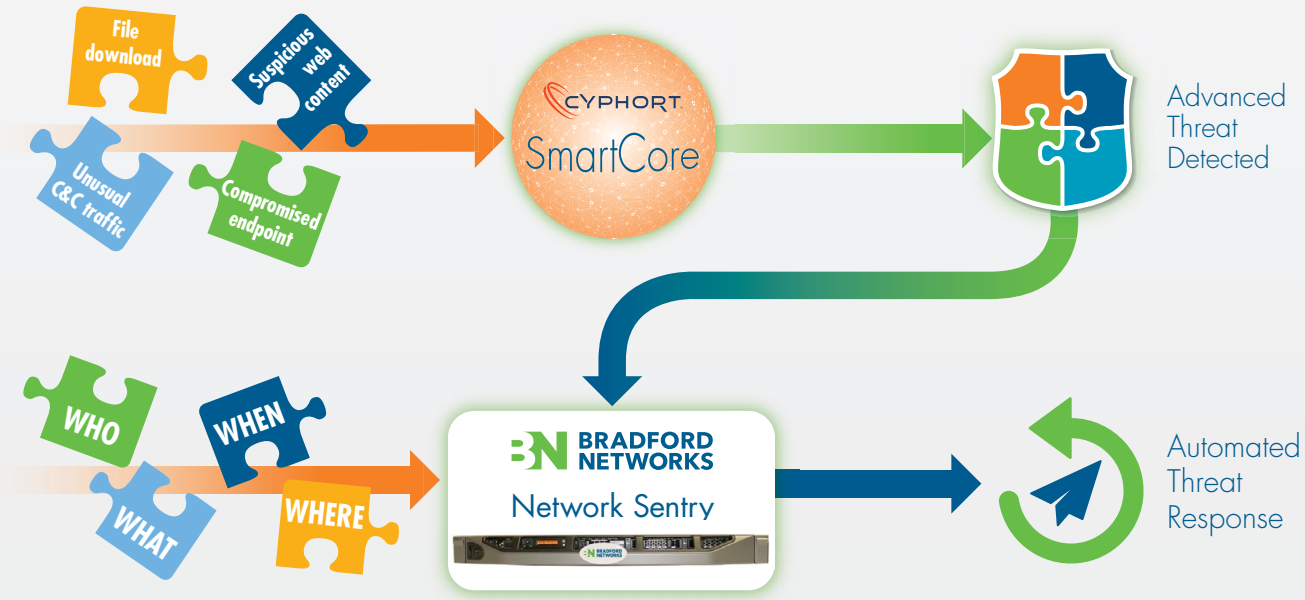
Solution Overview

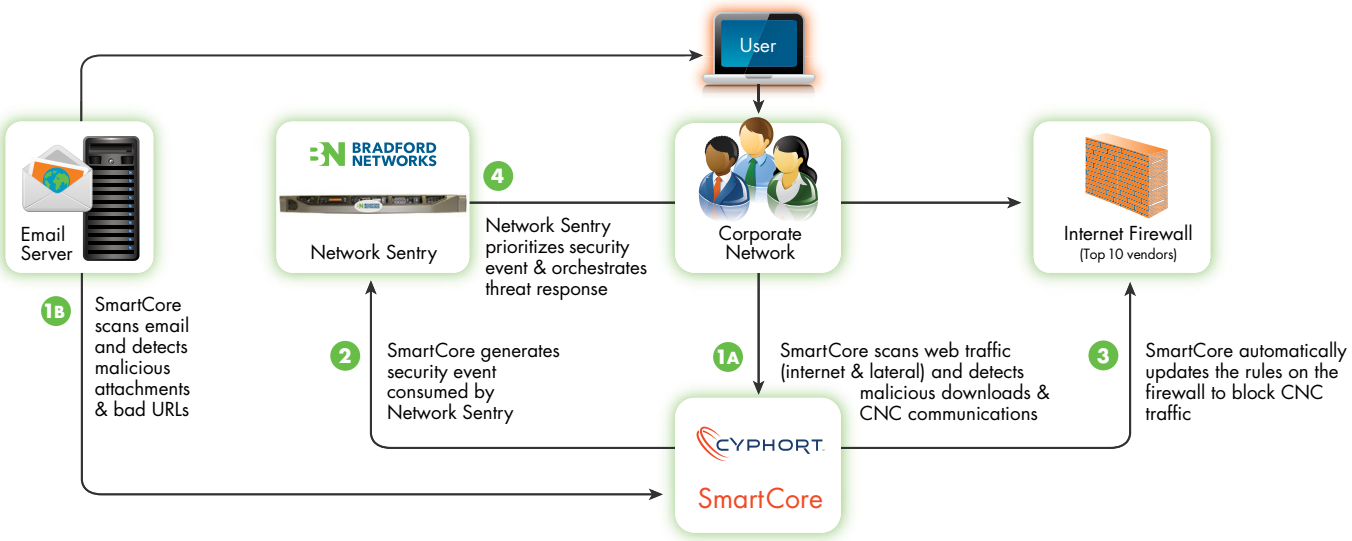
The widespread adoption of disruptive IT trends such as mobility, virtualization and cloud has expanded the attack surface and diminished the network perimeter of an organization. These long-term trends have made it easier for cyber adversaries to design sophisticated malware that can infiltrate corporate networks, engage in reconnaissance activities such as lateral movement and credentials stealing, and exfiltrate sensitive corporate data without getting detected by traditional security solutions.

Sophisticated malware tends to traverse different domains of IT management – security, networking, and endpoints – making it a cross-functional challenge to correlate the silos of information, and rapidly contain a compromised endpoint in the event of a cyber breach. The traditional threat response process requires significant manual intervention and expertise to trace and contain the threat's electronic foothold. Cyphort™ and Bradford Networks™ have partnered to automate the complex threat triage and response process to reduce threat containment time following a cyber breach. Cyphort's network-based Adaptive Detection Fabric (ADF) leverages machine learning and behavioral analysis to provide best protection from advanced, otherwise undetectable threats. Bradford Networks' Network Sentry leverages its unique Live Inventory of Network Connections (LINC) to enhance fidelity of security events from Cyphort by correlating device, user, application and connections information to the compromised endpoint.

With this integrated offering, organizations can minimize the risk associated with exposure of digital assets and intellectual property, protect brand equity, and limit the cost of cyber breaches.

Security Event Correlation, Triage and Response





How it Works

Cyphort's SmartCore analytics engine continuously collects web, email, and lateral spread traffic, then employs a comprehensive, multi-stage data analysis using machine learning, behavioral analysis, and other techniques to correlate data from multiple sources and accurately identify previously undiscovered malicious content. Information is prioritized based on the severity of risk, areas targeted within the network, and the threat's progress in executing its mission. Network Sentry ingests security event information from Cyphort's SmartCore, and applies contextual awareness: device profile, ownership, installed applications and attempted network connections. Based on the severity and business criticality of an event, Network Sentry then triggers an automated workflow and threat response which can include termination of connection, adjustment of access control, SMS and email notifications or quarantine of the endpoint in a specific VLAN for remediation.

Highlights

- Enable rapid triage of security events and automated threat response to reduce containment time from days to seconds
- Bridge the gap between the SOC and NOC with automated workflows
- Gauge severity and business criticality of security events to determine appropriate threat response
- Isolate, restrict, or block compromised endpoints from the network in real-time
- Dynamically control network access for every user and device based on its security posture
- Leverage live and historical inventory of network connections to trace additional points of compromise

BRADFORD NETWORKS
374 Congress Street, Suite 502
Boston, MA 02210, USA
Toll Free +1 866.990.3799
Phone +1 603.228.5300

BRADFORD NETWORKS is leading the transformation of network security by providing visibility, control and response to minimize the risk and impact of cyber threats. The company's patented Network Sentry solution continuously assesses the risk of every user and endpoint, and automatically contains compromised devices that act as backdoors for cyber criminals. The company's award-winning Network Sentry is used by more than 1000 organizations worldwide across many market sectors, including financial institutions, government and defense, healthcare, education, logistics and transportation, media and entertainment, retail and hospitality, technology, utilities and many others. For more information, please visit **www.bradfordnetworks.com**.

CYPHORT
5451 Great America Pkwy, Suite 225
Santa Clara, CA 95054, USA
Toll Free +1 855.862.5927
Phone +1 408.841.4665

CYPHORT, INC. is a network security company providing mid- and large-size enterprise customers with the innovative Adaptive Detection Fabric, a scalable software solution designed to integrate with existing security tools to discover and contain the advanced threats that bypass the first line of security defense in an organization. Based in Santa Clara, California, the company was founded in 2011 and distributes its software through direct sales and channel partners across North America and international markets. Learn more at **www.cyphort.com**