

## Bradford Networks and Tenable

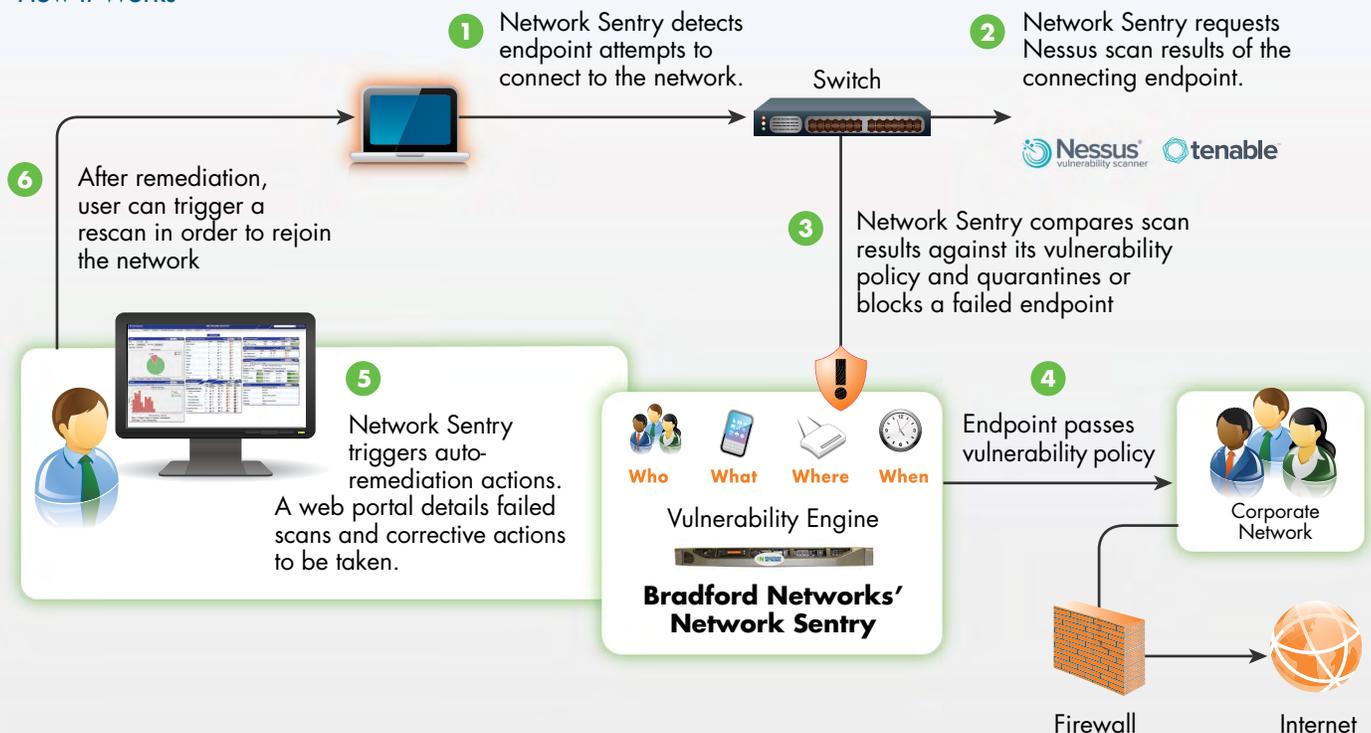
### Solution Overview

As the Internet of Things (IoT) explodes with an ever-increasing mobile user population, it is critical to understand every device and user connecting to a corporate network. IT departments struggle to ensure that mission-critical network resources are both operational and secure, while allowing network access for an exhaustive number of endpoint devices — tablets, smart phones, biomedical devices, security cameras — the list is endless.

Continuously assessing vulnerabilities in real time is the foundation of a successful security program. Tenable™, a leader in providing next-generation vulnerability assessment, and Bradford Networks™, an expert in the security and automation space, have partnered to provide the ability to quickly profile endpoints during onboarding and scan each device for vulnerabilities. Available globally, this integrated offering can be deployed on premise or via the cloud. Requirements include Nessus Manager v6 and above, Tenable Cloud, or Tenable.IO., and Network Sentry v8.1 and above.

This solution provides complete visibility, profiling and scanning for every endpoint, and enforces policies that help ensure regulatory compliance. Organizations leveraging this solution benefit from continuous network monitoring that identifies vulnerabilities, automatically quarantines suspect endpoints, then prioritizes and delivers alerts along with contextual information to system analysts. This partnership results in reduced impact, time and costs of containing cyber threats.

### How it Works



## How it Works

When a device connects to the network, Bradford Networks' Network Sentry queries Tenable's Nessus Manager for scan results. The scan information is fed back to Network Sentry which determines the who, what, where and when of endpoints. If the scan results are acceptable, Network Sentry uses policies to determine the appropriate level of access.

If an endpoint is found vulnerable, the security event is fed into Network Sentry's correlation engine to enhance its fidelity, assign priority and enforce policy-based threat containment actions. Network Sentry's Live Inventory of Network Connections (LINC) provides real time tracking of user, device, application and network-related metadata and utilizes this information to triage security events into actionable security alerts.

## Highlights

- Pre-connection scan, without requiring an agent
- Assess risk of every endpoint on the network
- Identify vulnerable devices and take decisive action to contain the compromised endpoint
- Isolate, restrict, or block compromised endpoints from the network in real-time
- Reduce containment time from days to seconds



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



7021 Columbia Gateway Drive, Suite 500  
Columbia, MD 21046  
North America +1 (410) 872-0555  
Latin America +1 (443) 545-2278

**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](http://www.bradfordnetworks.com).

**TENABLE** transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring. For more information, please visit [www.tenable.com](http://www.tenable.com).