USE CASE

BRADFORD NETWORKS

Network Sentry

Easy, One-Step IoT Security

Ponemon Institute research shows IoT devices are the most challenging technology to secure. With a Gartner estimate that 20 billion IoT devices will be connected by 2020, and projections that 25% of identifiable attacks will involve IoT devices, securing these devices is crucial.[1] This is especially concerning since a recent Ponemon Institute study found 75% of organizations are not confident or have no confidence that they know all of the IoT applications in their network.[2]

Why are IoT devices hard to secure?

- IoT devices have no "user"— so most existing authentication protocols don't work
- Most firewalls — the first line of defense — cannot "see" or protect IoT devices because they can't authenticate headless devices
- Most IoT devices have no inherent security 'built-in,' others lack enterprise-grade security
- Even with onboard security, weak IoT authentication and authorization protocols can cause a security gap
- Some IoT devices have hardcoded PINs in the firmware that cannot be patched or updated
- There is no common platform and operating systems for these devices
- Most IoT devices lack the memory and processing power for meaningful security
- IoT devices are designed to automatically send information to manufacturers and/or share information with other devices over the internet — sometimes without owners even realizing these devices are connecting outside the network

KEY BENEFITS

- » Provides a live inventory of every endpoint – including IoT devices
- » Uses existing network infrastructure to save money and time
- » Eliminates common audit failures from "shadow IT" and IoT security gaps
- » Offers simplified IoT onboarding using a sponsor
- » Delivers full device profiling and classification information
- » Isolates rogue devices with "Friend or Foe" functionality to lockdown network security gaps
- » Integrates with MDM solutions and any firewall

IoT and headless devices increase risk

Hackers are constantly scanning networks for vulnerabilities, and IoT devices are an easy target because most firewalls cannot see or protect these endpoints. There are two main use case scenarios:

Unwitting accomplices and shadow IT

Many corporate staff members are unaware that they are compromising network security when they purchase everyday devices such as internet-enabled coffee makers, refrigerators and projectors. When a legitimate attempt to simplify a business challenge results in the addition of a new technology, such as a router or printer, without IT notification, a vulnerable open portal can be created. This is frequently referred to as "shadow IT," a term created to describe how rogue devices can appear on the network without the knowledge of the IT team.

[1] www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

[2] securityintelligence.com/10-key-findings-from-the-ponemon-institutes-mobile-iot-application-security-testing-study/

Unsecured enterprise-approved headless devices

When organizations add security cameras, HVAC sensors, medical equipment and thousands of other similar devices, many are IoT-enabled to deliver better operational efficiency. Unfortunately, such devices have little or no inherent security, and in the absence of a user to authenticate, most existing firewalls and security equipment cannot authenticate and secure them. The same issue exists with other headless devices, such as industrial control systems (ICS) and programmable logic controllers (PLC), which lack a user to authenticate and cannot be secured using a persistent agent. Often the IT team does not even realize devices are IoT-enabled or that the existing firewall and security solutions cannot close the security gap caused by these devices.

Real-time visibility into all connected endpoints is a crucial first step in closing security gaps since it is impossible to secure a device if an organization does not know it exists. All Network Sentry products provide IoT security with real-time visibility into every device connected to the network. The Network Sentry product line ensures that organizations can identify every switch, router, IoT and BYOD device, and provides a live inventory of everything connected to the network. Bradford Networks' **Network Sentry** is an easy-to-use, one-step solution specifically designed to close the IoT security gap left open by firewalls. It provides full visibility into all endpoint devices, enables network lockdown, and simplifies IoT device onboarding and management.

Securing IoT devices by controlling access

Network Sentry enables organizations to fill a gap by controlling devices. It offers:

Endpoint profiling and classification

With the large number of IoT and BYOD devices, organizations need to automate the profiling and classification of endpoint connections. **Network Sentry** automates device discovery and classifies each device as corporate or employee-owned. This product provides the what and where information for devices.

Control for unsecured or headless devices:

Network Sentry can protect unsecured endpoints such as those used in IoT, ICS and PLC solutions. It enables organizations to define policies that immediately shut down individual ports when a device acts suspiciously by using "Friend or Foe" technology.

Simplified deployment of IoT devices

When using IoT or headless devices, organizations are not authenticating a specific user so agent technology does not work with most of these devices. **Network Sentry** simplifies the deployment of IoT devices by automating most of the authentication process using a sponsor. When a new IoT device tries to connect to the network, **Network Sentry** automatically places the device in an isolated network, profiles the device, then sends the information and the suspected type of device to the appropriate department for review and authorization. Once the device is confirmed, **Network Sentry** notifies the firewall of the type of device and where to place it in the correct network segment.

Easy to upgrade and scale

As the entry-level product of the Network Sentry security line, **Network Sentry Secure Enterprise Basic (SEB)** is designed specifically to close the IoT and headless device security gaps in firewalls, eliminate common audit failures from "shadow IT" and enable network lockdown. **Network Sentry SEB** works best for organizations that need to close network security gaps caused by IoT and headless devices, but do not require more advanced user/network controls, persistent agents or automated threat response. For organizations requiring IoT security as well as additional features, such as persistent agents, advanced network access control, event triage and automated threat response, Bradford Networks offers a family of solutions to meet these needs.

Network Sentry Secure Enterprise Advanced (SEA) provides the functionality of **Network Sentry SEB**, but adds more advanced network access controls as well as automated provisioning and controls for users, guests and devices. This solution adds the "who" information, with additional automation and granular network control. With automated guest and user provisioning, users automatically receive only the required amount of access based on their role or device. **Network Sentry SEA** also offers pre-connect and post-connect scans to ensure all devices meet the minimum network security requirements before enabling access, it can even direct users to self-remediate certain issues. **Network Sentry SEA** also provides policy-driven automated quarantine for non-compliant devices or if a device falls out of compliance while connected to the network. This solution is best for organizations that want complete endpoint visibility and an advanced NAC solution with granular control, but do not require event triage, event correlation or full automated threat response.

Network Sentry Secure Enterprise Response (SER) offers complete network endpoint visibility and an automated threat response solution that delivers contextual information with triaged alerts. **Network Sentry SER** provides a live inventory of all network connections, offers immediate, automated threat containment and dramatically reduces the amount of time spent to triage and research security events. Ideal for the SOC or for organizations that have existing NAC, SIEM or firewall solutions that do not provide event triage or automated threat response, **Network Sentry SER** provides endpoint visibility, event triage, and real-time automated threat response.

Network Sentry Secure Enterprise Premier (SEP) is the ultimate in visibility, control and response. As the premium product in the Network Sentry family, **Network Sentry SEP** incorporates the complete functionality of the other products into one solution. It provides real-time endpoint visibility, comprehensive NAC, and automated threat response while delivering contextual information with triaged alerts. It integrates with other security devices on the network to ingest additional security logs and data, then uses a correlation engine to triage alerts by severity, improve the accuracy of event triage, and present the alert, along with all contextual data, to an analyst. By presenting all the information in one comprehensive alert, **Network Sentry SEP** automates much of the manual security review process, dramatically reducing the time IT analysts spend sifting through alerts and researching event information. **Network Sentry SEP** is the solution for organizations that seek the combined functionality of all Network Sentry products.

The Network Sentry family of products provides various combinations of endpoint visibility, network access control and automated threat response, to suit the needs of any organization. With features that work with all firewalls and integrate seamlessly with other security solutions, the Network Sentry product line enables organizations to leverage existing security investments to build a strong security posture, as well as automate numerous processes that simplify endpoint management and dramatically speed threat response.

Bradford Networks' Network Sentry Solutions

PRODUCT	USE CASE	VISIBILITY	CONTROL	RESPONSE
NETWORK SENTRY SECURE ENTERPRISE BASIC (SEB) Easy, one-step IoT security solution to close endpoint security gaps by seeing all endpoint devices on the network, automating authorization, and enabling network lockdown.	Organizations that need to secure IoT and headless devices, and enable network lockdown without more advanced user/ network controls or automated threat response.	◔	◑	○
NETWORK SENTRY SECURE ENTERPRISE ADVANCED (SEA) All the functionality of Network Sentry plus more advanced Network Access Controls and automated provisioning for users, guests, and devices.	Organizations that want complete endpoint visibility and a flexible NAC solution with granular control, but do not require automated threat response.	●	●	○
NETWORK SENTRY SECURE ENTERPRISE RESPONSE (SER) Provides complete visibility and an automated threat response solution that also delivers contextual information along with triaged event alerts.	Ideal for the SOC or for organizations with existing security solutions like SIEM or firewall. Provides endpoint visibility, event triage, and real-time automated threat response.	●	○	●
NETWORK SENTRY SECURE ENTERPRISE PREMIER (SEP) The ultimate in visibility, control and response, Network Sentry SEP offers real-time endpoint visibility, comprehensive NAC, and automated threat response and delivers contextual information with triaged alerts.	Organizations that want complete endpoint visibility, a flexible NAC solution with granular controls, as well as accurate event triage and real-time automated threat response.	●	●	●

BRADFORD NETWORKS

374 Congress Street, Suite 502, Boston, MA 02210, USA
Toll Free +1 866.990.3799 | Phone +1 603.228.5300
Email info@bradfordnetworks.com
Web vwww.bradfordnetworks.com

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 1,000 enterprise companies worldwide across many market sectors, including finance, 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.