BRADFORD NETWORKS
the smart edge

HealthCheck Service

Computing devices employed across today's organizations change and grow at a dramatic rate while IT resources and staffing budgets often remain constant. Bradford Networks' HealthCheck Service enables you to realize the full value of your Network Sentry solution, while continuing to meet your changing business requirements.

Bradford Networks' HealthCheck Service deliverables include:

- Statement of Work
- Two (2) days service time with remote assessment and tuning of the following:
  - Server and agent configuration
  - Communications
  - Device and user profiling
  - Auditing and reporting
  - Alerting
  - Network provisioning
  - Endpoint remediation
  - Integrations

Statement of Work (SOW): To plan the project, Bradford Networks' Project Manager works with the customer to create an SOW that documents the stakeholders, requirements, process, deliverables and schedule for the HealthCheck session. The SOW forms the basis for the service.

Server and Agent Configuration: To ensure that Network Sentry is configured for maximum performance and the best user experience, the Service Engineer reviews current configurations and determines what needs to be tuned.

Communications: Because communication between Network Sentry and the network infrastructure and endpoint devices is crucial for maintaining an up-to-date view of the network, the Service Engineer will validate this functionality.

Device and User Profiling: The key to providing flexible yet secure network access to devices and users is to ensure the Network Sentry's profiling rules are configured properly for your environment. The Service Engineer will review and modify these rules as appropriate.

Auditing and Reporting: Collecting historical network access data is critical to providing the audit trail and perspective often needed to resolve a security incident. The Service Engineer will verify that Network Sentry's report generation and distribution is configured properly for monitoring and logging users and devices connecting to the network.

8-STEP SERVICE DELIVERY

1. **Server & Client Configuration**
   - » Configuration parameters
   - » Availability
   - » Performance
2. **Communications**
   - » Network infrastructure
   - » Endpoint clients
   - » Device library
3. **Device & User Profiling**
   - » Device inventory
   - » Device identification
   - » User identification
4. **Auditing & Reporting**
   - » Historical data collection
   - » Reporting parameters
   - » Reporting distribution
5. **Alerting**
   - » Security violations
   - » Security anomalies
   - » Configuration thresholds
6. **Network Provisioning**
   - » Guest networks
   - » Restricted access
   - » Full access
7. **Endpoint Remediation**
   - » User notification best practices
   - » Guided instructions for self-service
   - » Warnings vs. enforcement
8. **Integrations**
   - » Syslog events
   - » Active directory
   - » RADIUS

Alerting: Based on your notification requirements, the Service Engineer will verify events and alarms are configured for detecting and notifying security anomalies and violations that require investigation, as well as disabling those that are not of concern.

Network Provisioning: The risk profile for a device attempting to connect to a network can determine the level of access that is provided. The Service Engineer will adjust the corresponding provisioning rules for full, guest, or restricted access.

Remediation: The Service Engineer can provide assistance in improving the user experience for the self-remediation process when a device is identified as at risk and isolated.

Integrations: If you have integrated the Network Sentry with third-party solutions such as an Intrusion Detection System (IDS), the Service Engineer can verify that it is communicating correctly with Network Sentry.

CHALLENGES

- Adapting Network Sentry for a changing network environment
- Keeping up with consumerization of IT – Bring Your Own Device
- Modifying device profiling rules to provide access while limiting risk
- Providing knowledge transfer during staff turnover
- Leveraging new features

BENEFITS

- Faster identification of new devices and users
- Knowledge transfer of best practices
- Continued value of Network Sentry
- Improved security posture and reduce risk
- Safer introduction of new devices
- Maximum console performance
- Maximum endpoint performance
- Seamless integration with existing NOC/SOC solutions

DELIVERABLES

- Key functionality assessment
- Tuning of server and agent parameters
- Validation of reliable communication across all network components
- Impactful network access reports and alerts
- Event integration with core security and operations platforms
- Instructions for designated staff to gain experience in best practices
- Duration: 2 days of remote assessment and tuning

BRADFORD NETWORKS
the smart edge

One Broadway, 4th Floor, Cambridge, MA 02142, USA
Toll Free +1 866.990.3799
Phone +1 617.401.2515
Email info@bradfordnetworks.com
Web www.bradfordnetworks.com

Bradford Networks offers the best solution to enable secure network access for corporate issued and personal mobile devices. The company's flexible Bradford Networks platform is the first network security offering that can automatically identify and profile all devices and all users on a network, providing complete visibility and control. Unlike vendor-specific network security products, Bradford Networks provides a view across all brands of network equipment and connecting devices eliminating the network blind spots that can introduce risk.