

# ISNG for Security Assurance

## ISNG Platform for Business Assurance

As a real-time information platform, NETSCOUT® ISNG, with patented Adaptive Service Intelligence™ (ASI) technology, is ideal data source for several business assurance applications including service assurance, big data initiatives and cyber security projects. Satisfying pressure from customers and competitors alike, enterprises are undertaking high profile digital transformation ventures to improve efficiencies, costs, and customer experience. Business interruptions before, during or after migration to these initiatives is unacceptable. With visibility into wire data, the ISNG platform delivers timely, accurate, and actionable business assurance information wherever an application is deployed – data center, cloud, or hybrid infrastructure environments.

### Business Assurance Challenges

As application and network disruptions are an unfortunate fact of life for most enterprises, quickly triaging and restoring the services to optimal operations is essential. There have been a variety of obstacles when it comes to visibility for resolving these problems with varying degrees of success.

The challenges can be broken down into the following categories:

**Lack of Common Visibility** – Operating several tools for service assurance and cyber security assurance, that use different data sources for visibility, including packet-based and NetFlow, has been the norm, but can be costly, time consuming, and inconclusive. For the vast majority of organizations, having visibility and fast access into the data they need, across their applications, protocols and network, without the performance and deployment challenges, has remained elusive.

**Conflict vs Collaboration** – Collaboration challenges have also been created by the use of different visibility data sources. When degradations and outages have occurred in the past, pinpointing the root cause has been delayed and time lost as Security, NetOps and AppOps teams wrestle over where the actual source of the problem lies.

**Tool and Vendor Clutter** – Too many devices connected to the network is a very real concern. Tool clutter abounds as organizations implement a different box for every monitoring and analysis task, each of which requires regular maintenance and upkeep by the IT staff and annual service charges and vendor management costs

through finance. Adding insult to injury is the lack of visibility and access to the “right” insight from wire data across the entire network for the purpose of security or service assurance.

## Automate and orchestrate key network and security workflows with Smart Data from NETSCOUT solutions

Built on a disruptive combination of NETSCOUT ASI, which provides unprecedented internal network visibility, and Arbor Networks ATLAS, which provides unprecedented Internet traffic visibility, throughout the entire network, only NETSCOUT provides complete traffic visibility to extract the smart data vital to resolving security threats.

## Security Assurance with ISNG and Arbor Networks Spectrum

In real time, ISNG delivers accurate and actionable information across service assurance, cybersecurity and business intelligence applications on a single platform for the first time in the industry. It provides real-time, complete network visibility into monitored traffic flows, across all environment types regardless of network, server or application architecture. Based on wire data, NETSCOUT’s extended ASI technology provides smart data as the foundation for the most robust data sources available to monitor and analyze the modern IT landscape, offering unprecedented scalability and flexibility in multiple form factors and deployment options: virtual, software and hardware appliances.

The nGeniusONE® service assurance platform leverages ISNG smart data to reduce the time necessary to resolve network and application performance and availability issues in enterprise environments. The same ISNG platform provides smart data to Arbor Spectrum, an internal network threat analytics platform. Engineered from the ground up with the security user in mind, Arbor Spectrum delivers unmatched network visibility combined with scale and speed of analysis for security threats.

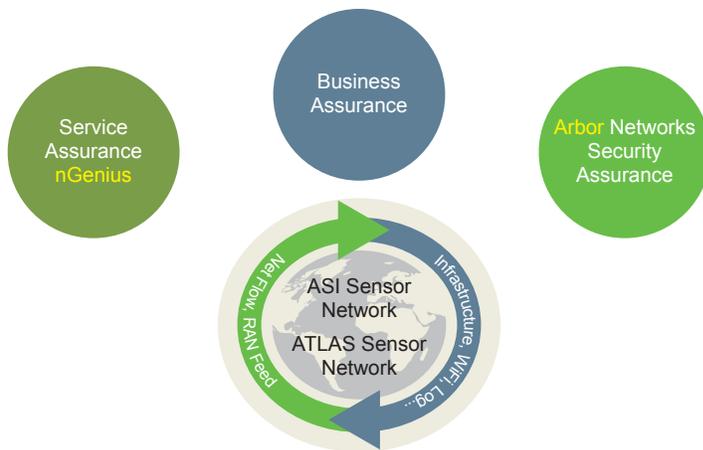


Figure 1: Accelerate Business Assurance with nGenius and Arbor Networks.

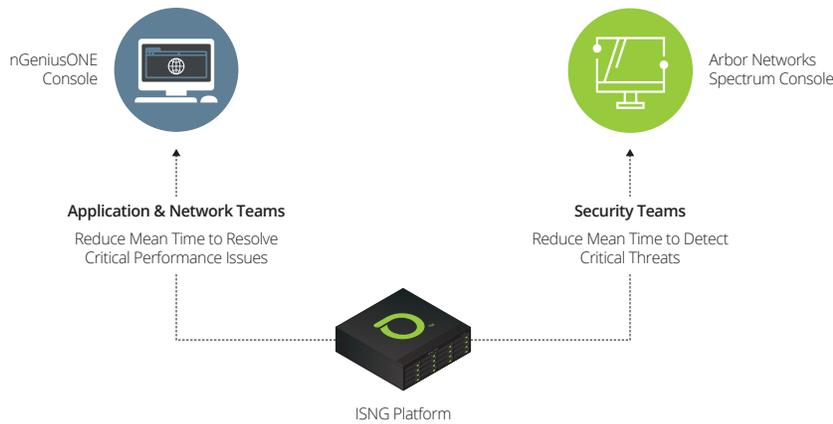


Figure 2: Security and Network teams can leverage common ISNG infrastructure.

### Security Team Force Multiplier

The new threat landscape requires security teams to become more like detectives of their internal network and user activity, rather than acting as fences, blocking or stopping unwanted or known threats. This comes at a time when hiring and retaining cyber security staff is a huge challenge, and most teams do not have enough staff or expertise to manage the “known” threat activity. Detection, investigation, and timeline building are immensely labor-intensive and time-consuming tasks. Senior-level responders are often deployed to meet these objectives because junior-level staff lack the requisite expertise.

Arbor Spectrum addresses these challenges by serving as a force multiplier for your security team. Not only does it provide deep visibility into network activity and quickly surface high-priority issues, by automating and orchestrating key incident response and security operations workflows, security teams can scale up – accomplishing far more with existing staff and resources.

Integrated with Arbor Spectrum, ISNG provides IP traffic “mining” intelligence, pervasively and passively, across the network to track the multiple stages of attack campaigns while maintaining the context needed to take quick and deliberate action. Arbor Spectrum empowers security analysts to use the smart data from ISNG to detect, investigate, prove and ultimately contain hidden threats in a faster and more efficient manner. Enterprises will reduce risk to the business and scale their security teams by using Arbor Spectrum to detect and confirm security incidents across the entire network, up to 10x faster than traditional forensics or security information and event management (SIEM) tools.

Benefits of this disruptive combination of NETSCOUT ISNG and Spectrum:

- **Removes the greatest complexity, performance and deployment barriers** for security teams requiring access to high resolution wire data, past and present, to detect and distinguish irregular activity from active security threats.
- **Orchestrates and automates the key network and security workflows** to detect and investigate network threat activity up to 10x faster than traditional solutions, enabling security teams to scale up – accomplishing far more with existing staff and resources.
- **Optimizes investment in the ISNG platform, with common network infrastructure** used for both service assurance with nGeniusONE platform and for security assurance with Arbor Spectrum.

**NETSCOUT**

**Corporate Headquarters**  
 NETSCOUT Systems, Inc.  
 Westford, MA 01886-4105  
 Phone: +1 978-614-4000  
[www.netscout.com](http://www.netscout.com)

**Sales Information**  
 Toll Free US: 800-309-4804  
 (International numbers below)

**Product Support**  
 Toll Free US: 888-357-7667  
 (International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: [www.netscout.com/company/contact-us-2/](http://www.netscout.com/company/contact-us-2/)