Dramatically Reduce Your Time To Know Critical Threats Already Inside Your Organization

With Arbor Networks Spectrum and the NETSCOUT ISNG Platform

Today's threat landscape requires us to move beyond tackling visible known threats and defensive processes. Attackers are slipping under the surface to penetrate your traditional security controls. They are evading detection – and there's no straightforward way to quickly identify and contain these breaches with conventional technologies and processes.

Security teams are already overwhelmed investigating visible, surface-level activity - the known threats detected by modern layered security architectures. They confront billions of events per day. It takes too much time just to detect anything significant, making it impossible to find the needle in the haystack that represents significant business risk. In fact, 140+ days is the average mean time to detect (MTTD) the presence of an attacker within an environment in many sectors.

Solutions to the security problem, under these circumstances, can seem elusive. Approaches to threat detection and investigation tend to fail because they focus on providing network and threat data rather than true visibility. Security professionals monitor screens awaiting signals and responding to alarms. But they lack visibility into the full range of network activity as it pertains to users, applications and systems. And even when a potential threat is detected, the investigation is laborious and time-consuming, putting tremendous demands on the teams involved.

Arbor Spectrum addresses these challenges by serving as a force multiplier for the security team, regardless of their size and expertise levels. Not only does it provide unprecedented visibility into network activity and quickly surface high-priority issues, it enables security teams to detect and investigate incidents in a far more efficient and complete fashion. By automating and orchestrating key incident response and security operations workflows, security teams can scale up – accomplishing far more with existing staff and resources.

Augmenting Today's Network Security Solutions

Today, most organizations use SIEM (Security Information and Event Management) solutions as their primary window into network security concerns. The SIEM collates and correlates data from deployed security controls, enabling an organization to passively monitor security infrastructure and observe activity and identify threats. However, SIEM technologies only identify what's known and visible, serving as a dashboard for correlating endpoints, firewalls, and sandbox events, which are abstracted from underlying network and user activity. Further, SIEM technologies tend to focus analysts on individual events – forcing analysts and responders to process each high priority alert in isolation, rather than allowing the alert to be quickly put in relevant context, and either quickly escalated or ignored.

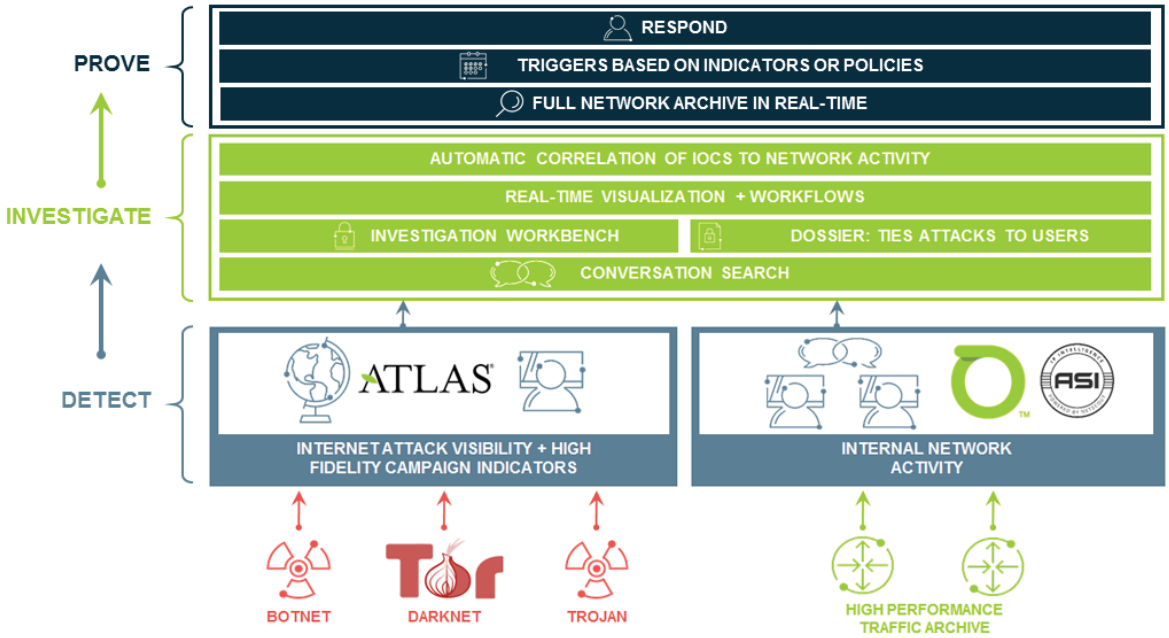

Figure 1: How Arbor Spectrum works.

The Arbor Networks Spectrum Platform for Network Threat Traffic Analytics

Complete Network Visibility. Arbor Spectrum augments these capabilities – offering a window on the internal network into host and user behavior across your organization. By observing all network traffic, Arbor Spectrum identifies unusual activity that would otherwise go undetected. It surfaces the most critical threats so that analysts can focus their time and energy where there is the most business risk, and provides workflows that allow analysts to quickly triage and investigate any detection. You'll be able to see not only surface-level activity, but the full range of network traffic activity including access to historical data from weeks or months before. It's a level of visibility that until now hasn't been possible because the necessary instrumentation hasn't been accessible from either a cost or performance perspective.

Detection of Irregular or Malicious Activity. Integrated with Arbor Spectrum is Arbor's Active Threat Level Analysis System (ATLAS®) – a unique threat analysis research infrastructure – and the ATLAS Intelligence Feed (AIF). AIF provides Arbor Spectrum with a unique set of data derived from Arbor's research activities and visibility into one-third of all Internet traffic. Arbor Spectrum quickly identifies any communication with known suspicious or malicious hosts, wherever it occurs across a network. With advanced policies and learning algorithms to assess network behavior, teams will be able to detect even subtle signs of post-exploit activity. Detecting and containing threats before a costly event occurs becomes a reality.

High Performance Traffic Archive. Typical indicators show a singular activity or, in some cases, a set of them. What they don't establish is when, where or how these events occurred, and what assets and users are implicated. Now, a timeline can be easily established. Network data is at the fingertips of each member of the team – enabling them to detect lateral movement or to clarify precisely which hosts were involved in the incident. Having both real-time traffic information as well as historic traffic information gives the full picture needed to distinguish benign activity from active threats. Leveraging NETSCOUT's industry leading network and application meta data collection and analysis technology from the ISNG Platform gives unprecedented pervasive visibility into, and analysis of, protocol, application and network data, resulting in the smart data needed so teams can see and understand what the risks are to their organization more comprehensively.

Operational Task Automation. 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. But this productivity barrier can now be surmounted. With smart workflows and automated detections, junior analysts can now work at the level of senior analysts. By automating and orchestrating key incident response and security operations workflows, security teams can scale up – accomplishing far more with existing staff and resources.

Context Driven Investigations. With context-driven workflows, teams can orchestrate and automate much of their operational activity. They will have an Indicator Dashboard, allowing them to quickly see the indicators, assets, and users that need to be observed. The Connections Module allows one to quickly assess all the different network connections so they are able to move from conversation to conversation over time. And then, finally, there's an Investigation Workbench capability that makes all work visible. This enables shift-working, response teams to collaborate so investigations can continue around the clock.

Benefits of the Arbor Spectrum Platform with NETSCOUT ISNG:

- **Force multiply the security team.** With automated detections and context-driven workflows, you orchestrate and accelerate manual and resource-intensive activities. Whatever the skill-level of team members, they can accomplish 10X what is accomplished now with existing staff.
- **Enable teams at all expertise levels to attain high performance at detecting and investigating sophisticated threat activity.** Accelerate the mean time to detect and the mean time to contain.
- **Bring what's hidden to the surface.** With complete internal network visibility for security, track subtle indicators and otherwise undetectable threats. Instead of just seeing North-South activity, see East-West – isolating users, assets, and locations.
- **Quickly identify high priority threats.** Distinguish active threats from false signals – and deploy team's resources appropriately.
- **Hunt with purpose.** Instead of waiting for threats to reach a critical stage, go on the offensive and proactively assess users, locations, and assets that may reveal a threat.
- **Instant access to the relevant historic network data.** With historical data at the team's fingertips, more complete investigations can be conducted, risk reduced, and the performance of your security operations or Incident response functions increased.
- **Rapidly deploy Network Threat Traffic Analytics.** Breaking through the deployment barrier that's thwarted other efforts to take on these problems, Arbor Spectrum with ISNG offers an intuitive and easily deployable solution – getting a team up and running in less than a day.

The integration of Arbor Networks Spectrum with NETSCOUT's ISNG platform delivers a solution that leverages common network infrastructure to give security teams pervasive visibility across users, applications, protocols, and network data. The combined solution uses smart data to expose and extract the key potential threat activity across the network, reducing mean time to resolution of critical security threats.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
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/

© 2017 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, and the NETSCOUT logo are registered trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. All other brands and product names and registered and unregistered trademarks are the sole property of their respective owners.

SQL_001-1700 07/2017