Arbor Threat Analytics

HIGHLIGHTS

- Innovative platform for rapid network threat detection and incident response
- Patented and scalable ASI technology based on packet data increases the integrity, fidelity, and quality of analysis
- Provides security analytics and logical workflows to detect, identify, validate, investigate, and respond to potential threats and cyber risks
- Available as a standalone or deployed alongside nGeniusONE® Service Assurance platform
- Intuitive workflows with drilldowns from high level risk visualizations to focused monitors for network investigation, and host investigation
- Single pane of glass analysis approach as a result of seamless integration with popular SIEM
- Leverages ASI metrics from world-class InfiniStreamNG™ and vSTREAM™ packet-based data sources
- Operates with Atlas Intelligence Feed

Product Overview

Arbor Threat Analytics is an enterprise-wide network threat and risk investigation solution that helps reduce the impact of cyber threats on your business. It serves as an early warning system with the ability to promptly and efficiently detect, validate, investigate, and respond to cyber threats. Organizations will benefit from having this cost-effective and highly scalable cyber threat analytics solution at their fingertips which can also easily integrate with popular SIEM platforms used by many corporations.

ASI Technology

Arbor Threat Analytics is built on NETSCOUT's patented Adaptive Service Intelligence™ (ASI) technology which leverages packet data for fast, context-based, vendor independent analysis. The access to rich, meaningful, security analytics data, combined with high-quality detection, improves the speed of investigations, and simplifies the evaluation of threatening incidents in an efficient manner.

Anywhere, Everywhere Visibility

ASI technology is the foundation of NETSCOUT's broad data source technologies including InfiniStreamNG (ISNG) software and hardware appliances as well as vSTREAM virtual appliances. Pervasive, continuous visibility for anywhere, everywhere cyber security monitoring is made possible through the innovative deployment choices of ISNG and vSTREAM across the variety of private, public, conventional infrastructure and virtualized environments that require visibility for threat detection and troubleshooting when used in combination with Arbor Threat Analytics.

Scalable Architecture

Arbor Threat Analytics has a highly scalable, redundant system architecture that supports data collection and analysis in very large, distributed networks. The Arbor Threat Analytics Dedicated Global Manager and the Arbor Threat Analytics Standby Server are optional licenses which can be used to expand your Arbor Threat Analytics deployment for even more scalability or high availability.

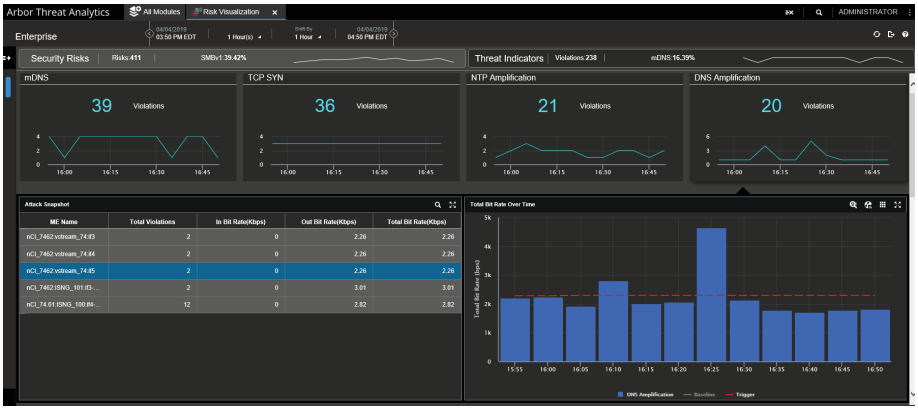

Figure 1: Arbor Threat Analytics: Analysis of rich, meaningful data provides views of risk visualizations (shown above), metrics, and session information.

Product SKU	Description*
51D41L	Arbor Threat Analytics – Workgroup (10 Pack) – Standard Appliance
51DH1L	Arbor Threat Analytics – Intermediate (25 Pack) – Standard Appliance
51D51L	Arbor Threat Analytics – Full (50 Pack) – Standard Appliance
51D21L	Arbor Threat Analytics – Full (50 Pack) – Standby Appliance
51DD1L	Arbor Threat Analytics Dedicated Global Manager – Software (Linux)
91D41L	Arbor Threat Analytics – Workgroup (10 Pack) – Software (Linux)
91DH1L	Arbor Threat Analytics – Intermediate (25 Pack) – Software (Linux)
91D700	Arbor Threat Analytics – Incremental (50 Pack) – Software (Linux)
91D50L	Arbor Threat Analytics – Full (50 Pack) – Software (Linux)
91D20L	Arbor Threat Analytics – Full (50 Pack) – Standby Software (Linux)
91DD0L	Arbor Threat Analytics Dedicated Global Manager – Software (Linux)

* Please consult with your NETSCOUT Sales Professional to determine system requirements suited for deployment in your environment.

Intelligent Threat Detection and Incident Investigation

Arbor Threat Analytics operates deep inside the data centers and enterprise environments, between the edge and the endpoints, where other tools have failed to provide cyber threat visibility. Security analysts can use ATA to address a wide selection of risk and threat indicators in today's large, complex environments which might otherwise be missed.

From a threat detection perspective, security events are triggered in ATA for internal attacks, protocol related risks and anomalous behaviors. Specific protocol risk assessments include detection of certificate expirations, weak SSL versions or ciphers or the use of unencrypted protocols.

Through the use of flexible workflows, the intuitive user interface of Arbor Threat Analytics is both powerful and easy to operate by intermediate and advanced security analysts alike for event-driven investigations.

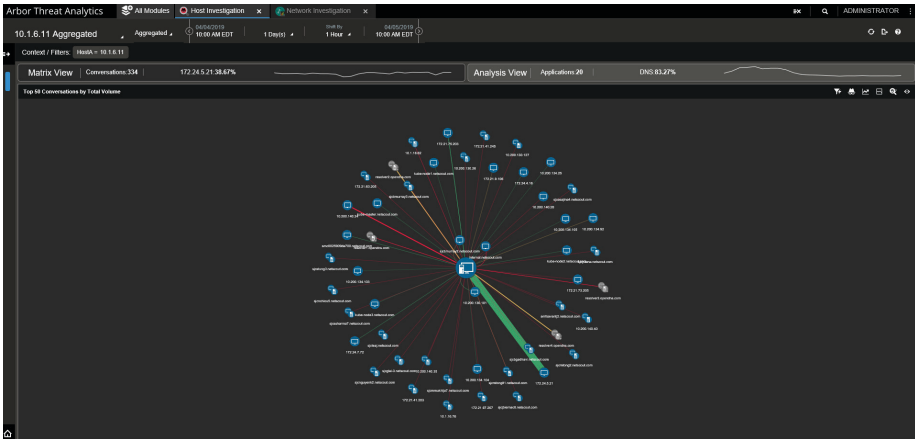

Figure 2: Arbor Threat Analytics Host Investigation module shows interactions of a suspicious host.

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

© 2019 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.

EPDS_031_EN-1901 04/2019