Pravail® Security Analytics Appliances

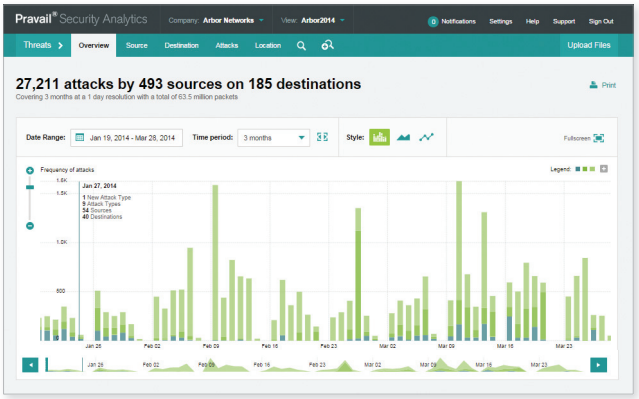
Hunt advanced attacks in real-time

The most devastating advanced attacks are those that operate "under the radar" and do a lot of damage before they are detected. In order to effectively—and quickly—identify these attacks, organizations must get familiar with the traffic patterns in their network and be able to investigate anomalies as soon as they are discovered.

The Pravail Security Analytics On-Premise solution gives organizations an unprecedented and detailed view of the attacks in any captured network traffic. It allows security analysts to analyze data in real time. Powerful visualizations display data from multiple perspectives (attacker, target, location or attack type)—enabling security analysts to quickly assess the security posture of the organization. Once an indicator of compromise has been identified, Pravail Security Analytics provides the analyst with actionable intelligence, allowing confirmation of the details and extent of the attack. Further, Pravail Security Analytics provides a look back in time, re-evaluating existing data with new attack information to ensure a complete picture of compromise.

Using Pravail Security Analytics On-Premise, organizations have the ability to:

- Identify anomalies in network traffic patterns in real time.
- Investigate and explore attacks without having any data leave the network.
- Analyze and process data faster and with more accuracy.
- Create attack timelines for threats that may have compromised the system months before discovery.
- Pinpoint attacker location by country or city or ISP (ASN).
- Scrutinize target hosts to uncover where infections may have spread.



Main visualization of analyzed packet captures

Key Features and Benefits

Explore and Understand Attacks Across the Entire Network

Upload network packet captures from anywhere in the network, not just where you have a security enforcement point, to get an unprecedented view of attack risk across your entire global network.

Simple Setup, Immediate Analysis

Because Pravail Security Analytics deals with uploaded full packet captures, there is no need to integrate with other security systems or logs, and no need to configure complex parsers. Analysis occurs the moment Pravail Security Analytics starts receiving data.

Interactive Visualization and Fine-Grained Control

Analyze packet captures whenever or however the organization requires. This allows for real-time analysis or post compromise research. Organizations can also evaluate captures in scales of minutes or days, as well as view attacks in older data.

Reveal Undetected Attacks

Whenever updated Threat Intelligence is available, Pravail Security Analytics searches your historical traffic to find previously undetected zero day attacks.

Enhanced IR and Forensics

Understand network events and attack indicators. View packet captures and data at custom intervals to determine attack infection and propagation.

Pravail Security Analytics On-Premise Specifications

Pravail Security Analytics On-Premise solution is deployed using a Controller appliance and distributed Collectors. The Collectors are available as appliances enabling organizations to scale out storage or processing capabilities for high speed capture points, or for deployment into multiple locations to provide distributed coverage. The Controller is used to store and analyze the security analytics data as well as manage the Collectors.

ARBOR® NETWORKS

Pravail Security Analytics Controller

All deployments of the Pravail Security Analytics On-Premise solution must include at least one Controller, as it's the primary device for security analysts to interact with. The Controller is responsible for:

- Running the Web Interface and User Interface of the application.
- Receive PCAP uploads and assign them to a collector for storage and processing.
- Storage of the security analytics metadata including:
  - Metrics and counters.
  - Deep Packet Inspection (DPI) results for all packets relating to an attack.
  - Queries against the meta data.
  - Management of the threat intelligence feeds and custom feeds.
  - Issuing the command to Loop stored data on the Collectors (automatic and customer initiated).
  - Management of key pairs between Controller and all Collectors (encryption and authentication of the session between Controller and Collectors).

Features	6115
Security Analytics Data Storage (Raw)	9TB
Hard Drives	5 x 3TB SATA 7200 RPM
Size	2 RU
Cluster Interface Options	4 port SFP options for 10/100/1000 Copper and GE SX/LX Fiber
Management Interfaces	2 x 10/100/1000 Copper
Processor	2 x XEON ES-2658; 2.1 Ghz/20 MB; 8 Core Processors
Memory	64 GB
Power Supplies	Dual AC or DC Power

Pravail Security Analytics Collectors

The Collector appliance processes network streams (Live Capture Points) or Packet Capture files (Non-Live Capture Points), sending metrics and metadata to the Controller for storage, visualization and querying. It uses a mirrored copy of the traffic taken from either a network tap or via a mirror port on a network appliance (switch or load balancer) and adds no latency to the network flow. The Collector is responsible for the following functions in Pravail Security Analytics:

- Writing PCAP files to disk (for uploaded PCAPs).
- Writing real time streams to disk in the form of PCAPs.
- Analyze real time streams for matches against enabled attack signatures. For discovered attacks, perform analysis of PCAP data and extraction of security analytics metadata including:
  - Metrics.
  - Counters.
  - Deep packet inspection information.
  - Encapsulation and sending of security analytics metadata to the Controller.
  - Looping existing stored data against delta changes to rules (feeds and custom signatures) to find previously undetected attacks.

Features	6015	6032	6064
Maximum Capture Points	1	1	1
Packet Capture Storage (Raw)	15 TB	32 TB	64 TB
Hard Drives	5 x 3 TB SATA 7200 RPM	8 x 4 TB SATA 7200 RPM	16 x 4 TB SATA 7200 RPM
Size	2 RU	3 RU	3 RU
Capture Interface Options	4 port SFP options for 10/100/1000 Copper and GE SX/LX Fiber		
Management Interfaces	2 x 10/100/1000 Copper		
Processor	2 x XEON ES-2658; 2.1 Ghz/20 MB; 8 Core Processors		
Power Supplies	Dual AC or DC Power		

ARBOR NETWORKS

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales

Toll Free +1 855 773 9200

Europe

T +44 207 127 8147

Asia Pacific

T +65 68096226

www.arbornetworks.com

DS/PRAVAILSAAPPLIANCES/EN/0914-LETTER