Pravail® Security Analytics

Revealing attacks in real time within your global network

Understanding attacks that have bypassed defenses and gained a foothold in the network has become a priority for IT security teams. These teams are dealing with a constant, escalating barrage of attacks on the network—as well as a steady stream of information alerting them to other potential threats. Attackers are counting on this chaos to remain undetected, for as long as possible. Motivated by profit or other political gains, these attackers will look to exploit any vulnerability in a network, often using methods that will see them bypassing traditional security systems designed to actively prevent such an attack. Once embedded in a network, these attackers may stay inactive for months before using compromised hosts to attack other parts of the organization or to systematically exfiltrate data from the target environment.

The Pravail® portfolio of solutions from Arbor Networks tackles these advanced threats head-on by giving organizations an enterprise-wide view of all network activities, critical attack details for fast remediation and expert-level blocking, all backed by world-class security research.

The Pravail Security Analytics platform enables organizations to deal with advanced threats by offering an unprecedented and detailed view of the attacks in any captured network traffic. It allows security analysts to assess an organization's security posture at a glance, displaying attack trends and severity across long periods of time. Powerful visualizations display the data from multiple perspectives (attacker, target, location or attack type) enabling the analyst to quickly compare attack statistics from different periods or locations, over years or terabytes of traffic. Once an indicator of compromise has been identified, Pravail Security Analytics provides the analyst with actionable intelligence, allowing confirmation of the exact 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, organizations have the ability to:

- Explore and better understand attacks across any captured network traffic, either historically or in real time
- Identify and isolate single attack threads in billions of packets
- Establish attack time lines for long running threats
- Perform frame by frame analysis using Deep Packet Inspection of attacks to determine extent of compromise
- Establish attacker location (by country or city) or ISP (by Autonomous System Number)
- Pivot on a targeted host to see what the compromised host did next
- Compare baseline averages of your data to all other organizations using Pravail Security Analytics to determine if you are overly targeted

Pravail Security Analytics provides a level of visibility and fine-grained ability to analyze suspicious traffic activity that can be used in conjunction with other network security products such as Pravail® Network Security Intelligence to perform the detailed attack analysis required to confirm the validity of a threat.

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.

ARBOR® NETWORKS

Why Arbor?

Deepest Level of Network Traffic Information

Pravail Security Analytics uses full packet captures to give enterprise organizations the richest set of data regarding the activities happening on the network. This level of activity awareness is unmatched by products that simply sit at the perimeter logging events.

Security Based on Real Attack Data

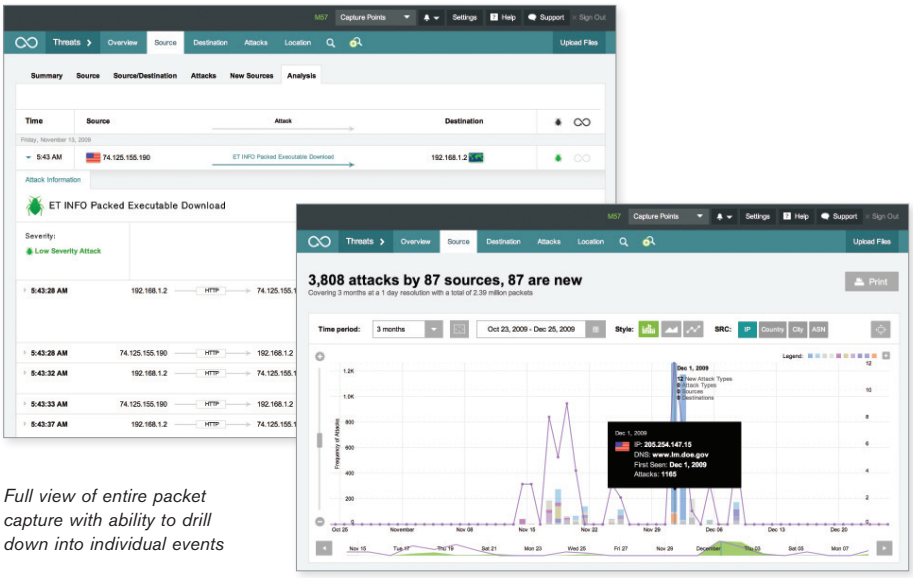
Threat intelligence at the cutting edge of network security comes from multiple sources, including real attack data derived from the ATLAS® Active Threat Level Analysis System. Using this system, Arbor monitors Internet traffic to detect new threats that are targeting the enterprise. This data is analyzed by security experts within ASERT and developed into effective analytics or detection methodologies.

Fueled by World-Class Research

Unlike many creators of security point products, Arbor maintains a dedicated team of security professionals to continuously analyze the threat landscape to ensure the Pravail Security Analytics product family is up-to-date against the latest advanced threats. ASERT is a renowned group of researchers and engineers that monitors data from ATLAS, and other sources, to create "fingerprints" that identify threats and malicious activity occurring within the enterprise.

Highly Scalable Solution to Accommodate Growth or Change in the Data Center

The Pravail Security Analytics solution can be easily scaled to accommodate the changing needs in the enterprise. As networks grow and more information flows through the systems, the platform can adjust by adding Collectors to increase processing capability or storage for data retention.



Full view of entire packet capture with ability to drill down into individual events

Security Beyond the SIEM

Many organizations rely on a security information and event management solution to log data and events for analysis and reporting. While a SIEM is ideal for aggregating events from numerous security devices such as firewalls, IDS/IPS and load balancers, if these devices do not detect targeted attacks then a SIEM is not going to see them either. Further, if security devices are updated to find newly detected targeted attacks and inform the SIEM of subsequent attacks, there is still no way to determine if the traffic they had previous processed included that zero day attack.

Pravail Security Analytics stores the network traffic while it is being processed and is able to reprocess this traffic with the latest threat intelligence to assist an analyst to determine the following:

- If and when the attack did occur previously within an environment;
- If it did occur what hosts were compromised;
- If these compromised hosts were then used as a foothold to compromise other hosts within an environment;
- If the attacker is still in the environment

Data Looping for Enhanced Forensics

Whenever the Pravail Security Analytics detection capability is updated, stored packet captures are automatically looped through the system to uncover additional threats. This provides an in-depth look at data to uncover previously unknown attacks for greater security and enhanced forensics.

Maximum Data Control for Custom Visibility

Interact with your data like never before. Zoom from years to minutes, move forward and backward in time to follow threats. View data from different perspectives such as Attacking Source, Target, Attack Type or Location of the Attack.

Comparison to Global Averages

Pravail Security Analytics Cloud customers are able to compare their attack experience against the global average of other customers. This allows an analyst to answer questions such as:

- In a given period if they are being overly targeted
- Have other networks seen this attack
- Have other networks seen this attacker

Comprehensive Availability and Threat Detection

Arbor Networks' ATLAS Intelligence Feed is Arbor's research-based security intelligence service. These policies are developed using a combination of real attack data pulled from multiple sources including ATLAS, the Red Sky Alliance and other partners. This attack data is analyzed by Arbor's expert research team and turned into security policies that are used by Pravail Security Analytics for both DDoS and advanced threat detection.

The ATLAS Intelligence Feed works in tandem with other threat intelligence feeds to provide the most comprehensive detection available for the enterprise. In addition, Pravail Security Analytics includes a custom signature engine that enables organizations to upload their own unique policies.

Pravail Security Analytics Cloud Specifications

An organization can securely upload packet captures and be analyzing data within minutes of a threat being identified.

Features	Description	
Cloud Package Options	• Available via annual subscription and priced based on total volume of storage required per month • No setup fee • No additional maintenance and support fees • Multi-year pricing available	
Flexible Service Packages	Monthly Storage Options • 100GB • 250GB • 500GB • 1TB • 2.5TB • 5TB	Included • Automatic looping of stored captures • Web UI using HTTPS • Secure upload via HTTPS or S3 Bucket copy • Comparison to Global Averages • Instant access to all new features
Additional Options	• Downloadable Amazon Machine Instance (AMI)–used as a Virtual Collector in the cloud, for customers who need to perform security analytics and already have infrastructure deployed in AWS • Combine with Pravail Security Analytics Collectors to maintain captures on customer network	

Pravail Security Analytics On-Premise Specifications

For organizations that cannot upload their packet captures to the Cloud due to compliance or regulatory reasons, Pravail Security Analytics can also be deployed as an on-premise solution 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.

Flexible Deployment for Always Available, Infinite Scalability

The platform can be deployed in a range of scenarios:

- **Cloud Only:** Upload captures to the Cloud for storage, processing and analysis.
- **On-Premise:** All captures, storage and processing contained within the on-premise Collector. No data leaves your organization. All analysis and visualization is performed in the Pravail Security Analytics Controller.
- **Cloud/On-Premise:** A hybrid model where Pravail Security Analytics Collectors are deployed in an organization's network for capture, storage and processing, and the analytics data is sent to the Cloud solution for analysis and visualization.

FREE TRIAL

See what you've been missing.

Try Pravail Security Analytics Cloud Free!

Today's attacks are designed to bypass your security controls and remain stealthy as they exfiltrate your confidential data. Pravail Security Analytics allows you to inspect suspicious traffic on your network to identify and understand where your real risks are. Don't remain in the dark—give Pravail Security Analytics a try today.

Just sign up using the link below and upload up to 1GB of data to the Pravail Security Analytics cloud to get started. See what attacks may be lurking in your network. See what you've been missing.

Start a free trial today »

Pravail Security Analytics Controller

Features	6115
Maximum Collectors	Unlimited
Security Analytics Data Storage (Usable)	9TB
Cluster Interface Options	• 4 x 10/100/1000 Copper • 4 x GE SX/LX • 2 x 10GE SR/LR
Management Interfaces	2 x 10/100/1000 Copper
Processor	2 x XEON ES-2658 2.1GHz/20MB 8Core Processors
Hard Drives	5 x 3TB SATA 7200 RPM
Memory	64GB
Power Supplies	Dual AC or DC Power
Size	2 RU

Pravail Security Analytics Collectors

Features	6015	6032	6064
Maximum Capture Points	1	1	1
Packet Capture Storage (Usable)	15TB	32TB	64TB
Capture Interface Options	• 4 x 10/100/1000 Copper • 4 x GE SX/LX • 2 x 10GE SR/LR	• 4 x 10/100/1000 Copper • 4 x GE SX/LX • 2 x 10GE SR/LR	• 4 x 10/100/1000 Copper • 4 x GE SX/LX • 2 x 10GE SR/LR
Cluster Interface Options	• 4 x 10/100/1000 Copper • 4 x GE SX/LX • 2 x 10GE SR/LR	• 4 x 10/100/1000 Copper • 4 x GE SX/LX • 2 x 10GE SR/LR	• 4 x 10/100/1000 Copper • 4 x GE SX/LX • 2 x 10GE SR/LR
Management Interfaces	2 x 10/100/1000 Copper	2 x 10/100/1000 Copper	2 x 10/100/1000 Copper
Processor	2 x XEON ES-2658 2.1GHz/20MB 8Core Processors	2 x XEON ES-2658 2.1GHz/20MB 8Core Processors	2 x XEON ES-2658 2.1GHz/20MB 8Core Processors
Hard Drives	5 x 3TB SATA 7200 RPM	8 x 4TB SATA 7200 RPM	16 x 4TB SATA 7200 RPM
Memory	64GB	64GB	64GB
Power Supplies	Dual AC or DC Power	Dual AC or DC Power	Dual AC or DC Power
Size	2 RU	3 RU	3 RU

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/PRAVAILSA/EN/0314-LETTER