Pravail® Security Analytics Cloud

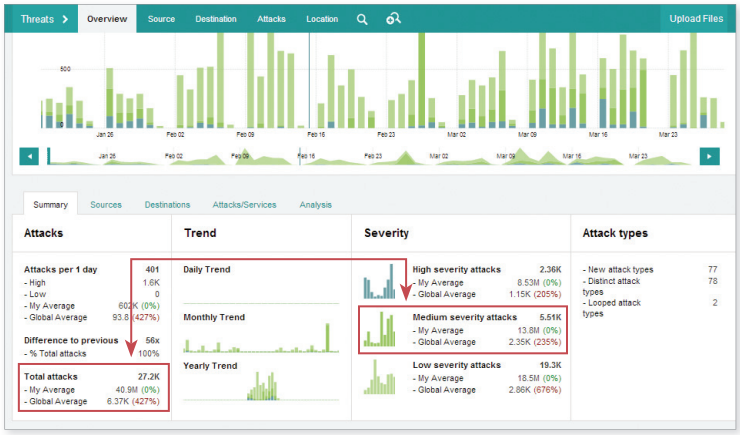
Instantly begin the hunt for advanced attacks

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.

The Pravail Security Analytics Cloud solution gives organizations immediate access to critical details about attacks that may exist within the network. The platform allows security analysts to easily upload and begin analysis on suspected attack activity, displaying data from multiple perspectives (attacker, target, location or attack type). The main visualization shows a summary of attack information that enables analysts to quickly identify malicious behavior. Detailed information about the attack—including the IP address of the attacker, the source location and targeted host—give the analyst critical data to help with remediation. In addition, Pravail Security Analytics re-evaluates older data with new information to uncover previously undiscovered attacks.

Using Pravail Security Analytics Cloud, organizations have the ability to:

- Begin investigation immediately upon alert of compromise.
- Explore and better understand attacks across any captured network traffic.
- 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 Cloud customers can measure their attack information against other users.

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

Pravail Security Analytics Cloud Specifications

Pravail Security Analytics Cloud is 100 percent Software as a Service delivered in the cloud. An organization can securely upload and store packet captures within minutes of a threat being identified. The cloud-only delivery, offers organizations an easy-to-use approach for investigating activities and events occurring inside the network.

Visit pravail.com to create an account and get started.

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*	*Included*
	• 100 GB • 250 GB • 500 GB • 1 TB • 2.5 TB • 5 TB *Note: This amount of storage covers both uploaded packet capture files and the cumulative security analytics data for each capture point. Customers may manage the retention of data and delete PCAP files as they require.*	• 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	Combine with Pravail Security Analytics Collectors to maintain captures on customer network	

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/PRAVAILSACLOUD/EN/0914-LETTER

About Arbor Networks

Arbor Networks, Inc. helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor's advanced threat solutions deliver comprehensive network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market-leading analytics for dynamic incident response, historical analysis, visualization and forensics. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context—so customers can solve problems faster and help reduce the risk to their business.