Pravail® Network Security Intelligence Appliances

Comprehensive visibility for incident response and forensics

Advanced security attacks are not one size fits all. Whether motivated by profit or politics, today's attackers are organized and efficient. They get to know each enterprise network and create custom attacks designed to take advantage of whatever vulnerabilities are left open, either through business design or human error. The resulting attacks—through advanced denial of service, botnets, malware, etc.—are unrelenting. These targeted attacks are designed to bypass basic perimeter protections like anti-malware, firewalls or intrusion prevention systems.

The Pravail® portfolio 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. Pravail® Network Security Intelligence acts as the central nervous system for security deployments. It sits inside the network and collects information on network traffic patterns and security events that are occurring throughout the network, alerting security teams to those events that indicate an attack or breach is in progress. Pravail Network Security Intelligence aggregates traffic data from multiple Pravail® Availability Protection System deployments with network-wide internal traffic to provide a clearer picture of enterprise risk. This traffic is analyzed using policies and threat countermeasures developed by Arbor's Security Engineering and Response Team (ASERT) to not only detect attacks, but to also prioritize risk and provide salient details that enable fast remediation.

Key Features

Network Wide Visibility

Aggregate IP flow information and network traffic information into a single view for pervasive, cost-effective visibility and performance analysis across the entire network.

Comprehensive Threat Detection and Analysis

Quickly and accurately identify attacks that have bypassed security controls and breached the network.

Enable Faster Incident Response

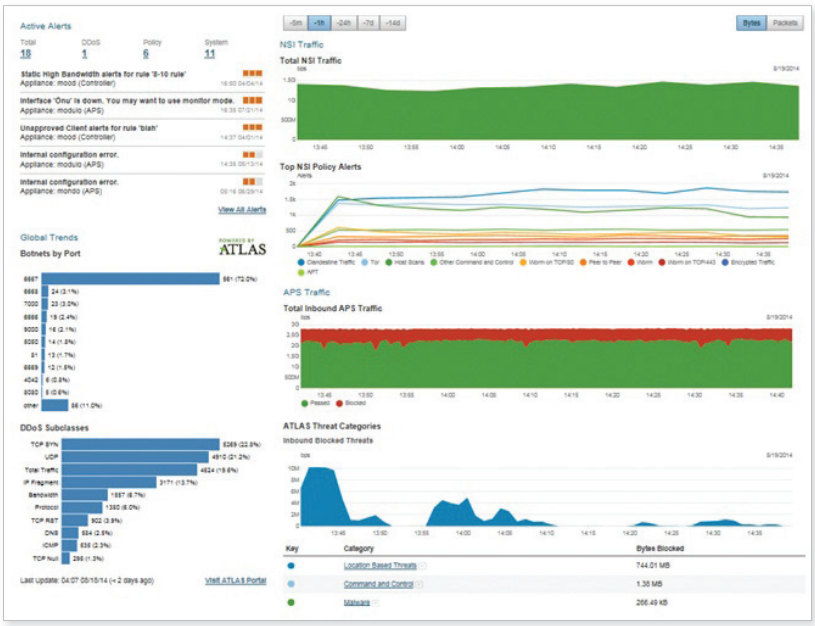
Identify and quickly follow up on security events with in-depth analysis on traffic activity and attack data.

Enhanced Forensic Capabilities

Leverage detailed network traffic reporting and attack analysis for security forensics.

Best-in-Class Security

Take advantage of expert security analysis and attack data derived from real world events for enhanced detection and alerting



Detailed deployment and management from a single dashboard, with the ability to easily click through to a specific device for in-depth investigation and/or adjustments.

ARBOR® NETWORKS

Why Arbor?

Broadest Level of Enterprise Network Information

Pravail Network Security Intelligence uses IP flow information 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 sit outside the network.

Security Fueled by World-Class Research

The ATLAS Intelligence Feed keeps Pravail Network Security Intelligence at the cutting edge of network security. The threat policies in this service are created from data derived from the ATLAS Active Threat Level Analysis System. Using this system, Arbor monitors Internet traffic to detect new threats targeting the enterprise. This data is analyzed by security experts within ASERT and developed into effective detection methodologies.

Proven Effectiveness in the World's Toughest Environments

Pravail Network Security Intelligence utilizes the same flow intelligence and tracking engine that powers Arbor's renowned Peakflow SP solution, which is used to help stop DDoS and botnets in hundreds of global Internet and Cloud service providers. The engine is built into a platform designed to address the unique demands of the enterprise.

Pravail Network Security Intelligence offers threat detection and network visibility that is critical for enterprise incident response and forensics. The attack details provided by this platform can be used to adjust and enhance enforcement policies in other network security products, including the Pravail Availability Protection System.

Using Pravail Network Security Intelligence, organizations have the ability to:

- View and prioritize advanced threat risks with the Pravail Threat Console.
- Defend the network against in-bound malware, botnets and targeted attacks while stopping infected hosts on the network from leaking data.
- Decrease risks from malware and botnet infection by blocking access to malware infected sites or known command and control servers.
- Conduct detailed incident response and/or network forensics on attacks post-breach.

Advanced Threat Detection with the ATLAS Intelligence Feed

Arbor Networks' ATLAS® Intelligence Feed is Arbor's research-based security intelligence service. These policies are developed by ASERT 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 ASERT's expert research team and turned into security policies that are used by Pravail Network Security Intelligence for threat detection.

Centralized Configuration and Management with the Pravail Console

The Pravail Threat Console is sold with the Pravail Network Security Intelligence appliance. The threat console offers users comprehensive visibility of the network and detection of activities indicative of security threats such as DDoS, malware, botnets or Trojans. The Console aggregates traffic and alerts from Pravail Availability Protection System deployments with the internal activity monitoring of Pravail Network Security Intelligence to give organizations a clearer picture of their security risk.

Advanced Security Powered by Flow Intelligence

The Pravail Network Security Intelligence platform leverages Arbor's flow intelligence and tracking engine. This powerful engine is used to gather and analyze IP flow information to track malware activity, detect botnet communication and/or other activity that could cause harm to the corporate network.

Key features of the flow engine include:

Stateful Flow Reassembly

Account and correct for multiple traffic flows generated by multiple appliances on a network; address real-world challenges that make raw IP flow monitors unreliable, including:

- De-duplication of redundant flows.
- Proper handling of data—channel connections from multiple protocols such as VoIP, FTP and RPC.

Compensation for Asymmetric Routing and Route Updates

Gain an accurate view of the traffic at a high or granular level through a specific router.

Activity-Based Detection

Protect internal networks from employee misuse or worms; track the behavior of individual hosts or users and identify anomalous behavior.

Real-Time Risk Assessment

Quickly pinpoint the biggest threats on your network by calculating a risk index that identifies which hosts or users are involved in multiple activities.

Application Intelligence

Network security intelligence demands application awareness for enterprises to understand what they need to do to protect and identify application-specific threats. Pravail Network Security Intelligence extends visibility to layer 7, providing a single, integrated solution for detecting and thwarting advanced attacks that can lead to fraud or leakage of confidential or proprietary information.

Identity Tracking

Identity tracking technology adds valuable context to data being monitored by Pravail Network Security Intelligence. Using directory service information (i.e., Active Directory), the product can associate user identity with traffic flowing throughout the network. This information allows organizations to see who has access to what applications and how they are using them. It also allows organizations to set usage policies that align with compliance requirements.

Comprehensive Reporting for Effective Incident Response

Pravail Network Security Intelligence features a wide range of standard and customizable graphical reports containing the actionable information required to identify and escalate incidents. The reports provide insight into which users are accessing which applications, the information leaving the confines of the network, and which types of devices are accessing corporate resources.

Pravail Network Security Intelligence Specifications and Features

Systems and Software

Features	Description	
ATLAS Intelligence Feeds	• Hourly updates • Detailed threat analysis • Delivery via RSS feed	
ATLAS Integration	In-depth intelligence on threat activity on a global and local perspective	
Identity Tracking	Identities Tracked • Hundreds of thousands	Other Features • Monitor and record all services • Real-time traffic visibility • Custom and standard report creation • Schedule report creation
Stateful Flow Reassembly	• Asymmetric routing • De-duplication of data • Ephemeral port mapping	
Deployability	Supported Protocols • Cisco Netflow (v5, 7, 9) • Juniper cflowd • Extreme and Foundry Networks sFlow (v2, 4, 5) • IPFIX for UDP	Also Includes • Flow redirection support • Gigabit packet capture • NTP support
Alert Management	Supported Protocols and Logging Standards • SEM • SNMP • SNMP v2c	 • SNMP v3 • SMTP • Syslog
Device Management	Key Features • Multiple users • Web UI using HTTPs • CLI using SSHv1, SSHv2, Telnet and Serial Console • Radius Support	 • Communications channels 2048bit RSA encrypted SSL • TACACS+ support • SNMP poll system and alert status
Operating System	ArbOS®, our proprietary, embedded operating system, is based on open-source operation system technology such as Linux and OpenBSD.	
Device Security	• Hardened OS and network stack • Fully encrypted communications channels • Software packages are cryptographically signed, preventing Trojan code • Built-in firewalling support, rejecting all packets by default (transparent to pings and port scans)	

Security Intelligence that Scales for Every Enterprise

Pravail Network Security Intelligence provides scalable deployment options that start with a central management and intelligence appliance with optional collectors that add scalability for geographically distributed networks. The product family includes:

Pravail Network Security Intelligence Controller

A central platform for receiving IP flow and providing intelligent analysis of all network-wide activity. It can be used to collect IP flow directly or as an aggregation point for IP flow that comes from the Pravail Network Security Intelligence Collectors.

Pravail Network Security Intelligence Controller XL

A 3U platform for receiving IP flow and analyzing network activity. The Controller XL offers the same functions as the regular Controller—but with additional flow storage for more in-depth forensics.

Pravail Network Security Intelligence Collector

Distributed appliances that gather IP flow data and transfer it to the Pravail Network Security Intelligence Controller for analysis. Collector licenses can be purchased according to specific needs.

The Pravail Network Security Intelligence solution is available in multiple platform options to meet the unique needs of each organization. Each platform is designed to offer the highest performance for the amount of traffic volume monitored.

Pravail Network Security Intelligence Controllers

Features	5220XL	5230XL
Flows Per Second Direct flow received from routers	25,000	80,000
Max Flows Per Second Direct + Collectors	250,000	
Monitored Routers	500	
Max Collectors	50	
Optional Deep History Module (DHM)	No	
Flow Storage	8 TB	
Monitoring Interface Options	• 2 x 10 GE SPF+ • 4 x 1 G SPF	
Management Port Interfaces	2 x 10/100/1000 Copper	
Processor	Dual Intel Xeon ES-2658 2.1 GHz/20 MB 8 Core Processors	
Hard Drives	5 x 3 TB SATA 7200 RPM	
Packet Processing	200 Mbps	
Memory	64 GB	
PSU	Dual AC or DC Power	

Pravail Network Security Intelligence Collectors

Features	5003AI	5005XL	5006XL	5007XL
Flows Per Second	Not applicable	16,000	35,000	80,000
Monitoring Interface Options	• 4 x 10/100/1000 Copper • 4 x GE SX/LX • 2 x 10 GE SR/LR	4 port SFP options for 10/100/1000 Copper and GE SX/LX Fiber		
Management Port Interfaces	2 x 10/100/1000 Copper			
Packet Processing	2 Gbps	1 Gbps		
Processor	Single Intel QuadCore Xeon CPU 2.40 GHz	2 x XEON ES-2658; 2.1 Ghz/20 MB; 8 Core Processors		
Hard Drives	2 SSD in RAID 1 (1/2n); 2 x 120 GB drives	8 x 2 TB SATA 7200 RPM		
Memory	24 GB	64 GB		
PSU	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/PRAVAILNSI/EN/0914-LETTER