

OmniPeek® Product Family

Intelligent 24/7 Network Analysis Solution



Distributed Network Analysis



Unlocking Virtual Data



Enterprise VoIP and Video Analysis

WildPackets' solutions enable businesses to

- Gain unprecedented visibility into networks and applications
- Accelerate find-to-fix times
- Discover and close network security gaps
- Increase end user productivity
- Increase ROI on existing networks and applications
- Increase IT efficiency and responsiveness
- Reduce costs associated with network downtime and service degradation
- Reduce IT labor costs

WildPackets®
Illuminate Your Network™

WildPackets OmniPeek Product Family

The OmniPeek Product Family gives network engineers real-time visibility into every part of the network – simultaneously from a single interface – including Gigabit, 10GbE, Ethernet, 802.11 wireless, VoIP, and WAN links to remote offices. Using OmniPeek's local capture capabilities, centralized console, distributed engines, and expert analysis, engineers can rapidly troubleshoot faults and fix problems, restoring essential services and maximizing network uptime and user satisfaction.

The OmniPeek Product Family comprises OmniPeek network analyzers and consoles, as well as distributed OmniEngines, which analyze data at remote locations on the network. With its open APIs and a growing family of plug-ins, OmniPeek is uniquely designed to meet the ever-changing needs of network engineers responsible for wired and wireless networks and applications such as VoIP, Video over IP and VoWiFi.

OmniPeek

Software, Appliances and Services Address Converged Networks, Application Performance, Virtualization, 802.11n, Voice and Video over IP, and Other Enterprise IT Challenges

OmniPeek is WildPackets' popular solution for network and application assurance. The OmniPeek Product Family offers a broad range of IT solutions designed to meet the requirements of CIOs, data centers, network engineers, field service staff and help desk personnel. OmniPeek features next-generation forensics analysis; packet flow reconstruction of Email, IM, and Web traffic; virtual server analysis; and enhanced support for converged networks including 10 Gigabit, 802.11n, Voice and Video over IP, and application performance monitoring (APM).

Offerings for Data Centers and Network Operations Centers

OmniPeek provides products and features to help data center engineers and network engineers troubleshoot, optimize, and secure networks and applications.

The Application Performance Dashboard provides a high-level view of the quality of service that applications are delivering to end users. Apdex, an industry standard developed by the Apdex Alliance (www.apdex.org), provides a single metric that represents the level of satisfaction users are experiencing with applications. When the dashboard reports a low score, engineers can use OmniPeek to drill down for Expert analysis, graphical reports, and the packets themselves to uncover the root cause of the problem.

Voice and Video Analysis includes support for industry leading VoIP solutions like Cisco and Avaya, new quality and signaling analysis of video over IP, enhanced call quality and signaling analysis of VoIP, new VoIP-specific Expert diagnoses and decodes, enhanced VoIP call playback in stereo providing simultaneous playback of both sides of the call, and new voice over IPv6 support.

Next-Generation Forensics enables engineers to capture, store, and analyze historical network traffic in order to conduct investigations for troubleshooting, security attack analysis, HR and policy compliance, application performance analysis, and business transaction analysis. OmniPeek forensics now features an optimized data-discovery algorithm, along with utilities for reconstructing Email, IM, and Web traffic.

The **Wi-Fi Alliance** has selected OmniPeek Professional for the official interoperability test bed for the new 802.11n draft 2.0 specifications. OmniPeek enables network engineers to analyze and troubleshoot 802.11n networks, using the same features previously available in OmniPeek for 802.11a/b/g networks.



OmiEngine

Distributed 24/7 Network Analyzer and Monitor

Building on WildPackets' award-winning network analysis technology, OmiEngine performs real-time network analysis on traffic from one or more network interfaces, including Ethernet, 802.11 a/b/g/n wireless, Gigabit, 10 Gigabit, and WAN. As part of the OmniPeek Product Family, OmiEngine captures and analyzes data in real-time, provides statistics for real-time monitoring and records data for post-capture analysis. Using WildPackets OmniEngines, network engineers can rapidly troubleshoot faults – even faults occurring at remote locations- without leaving their office.

OmiEngine runs as a service on standard Windows platforms as well as on WildPackets' network recorder, Omnicpliance, which is available in both Windows and Linux configurations. By installing an OmiEngine in each business location, a network engineering team gains real-time visibility into all its remote networks. Enterprises that cannot afford to staff each office with a network engineer can use OmiEngine to ensure that every business location receives the network support it needs.

OmiEngine provides comprehensive network service analytics, including:

- Application-layer Expert diagnoses, Apdex user satisfaction scores, and application response time (ART) analysis
- Expert Systems Diagnoses, including flow-based packet analysis and correlations between events and conversations

- Statistical Analysis, including packet flows and details about nodes, protocols, and sub-protocols
- Packet Analysis, including extensive protocol decodes and detailed descriptions of physical errors
- VoIP call signalling and call quality analysis, including MOS and R-Factor scores, as well as Expert analysis for leading VoIP solutions such as Avaya, Cisco, and Megaco
- Infrastructure monitoring, including 24x7 monitoring and analysis of network traffic; when network problems occur, OmiEngine executes SNMP traps, notifying SNMP monitoring systems such as HP OpenView of potential problems; because it captures the traffic that generated the error, OmiEngine provides engineers the detailed information they need to investigate and resolve problems.

While other packet analysis products offer only simplistic threshold-based alarms, OmiEngine offers a wealth of information and features that engineers can use to rapidly troubleshoot faults.

When running on an Omnicpliance, OmiEngine can capture and store hours, days or weeks of network traffic for post capture forensics analysis.

Critical Traffic May Never Leave the Rack

The migration to blade chassis-based virtual servers has created a new blind spot in the enterprise: the traffic between virtual servers in the same blade chassis. This "invisible traffic" never crosses any network segment where it can be easily captured. As a result, engineers have little or no visibility

into the traffic among virtual servers.

OmiVirtual

A Small Service that Shows the Big Picture

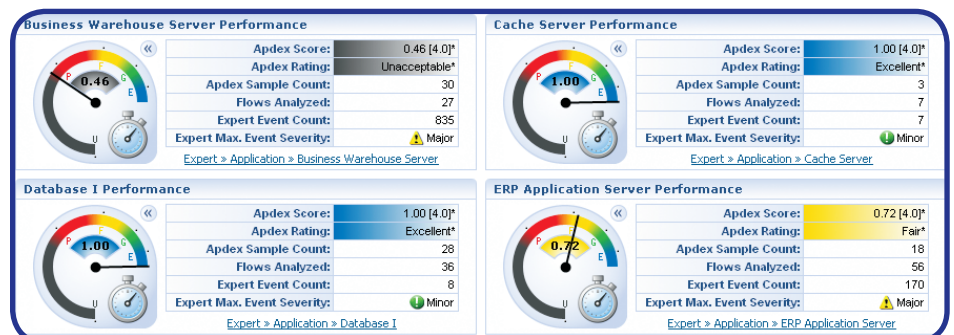
OmiVirtual is a small, lightweight service that runs on any Windows XP or Windows 2003 virtual server. It consumes minimal RAM and CPU resources, so you can troubleshoot, optimize, and secure virtual applications without compromising server performance.

When other virtual management tools report problems, get to the root cause by capturing traffic with OmiVirtual. Take advantage of the full capabilities of OmiVirtual by using OmniPeek Enterprise network analyzer's full suite of post-capture analysis tools, including Peer Map, Expert event reporting, Apdex application performance measurements, and more.

OmiPeek®

Portable Network Analyzer and OmiEngine Console

Serving a dual role as both a portable network analysis solution and as the software console for OmiEngines, OmiPeek offers an intuitive, easy-to-use graphical interface that engineers can use to rapidly analyze and troubleshoot enterprise networks. OmiPeek provides centralized expert analysis for all networks being managed by any components of the OmniPeek Product Family. With OmiPeek, enterprise IT professionals can analyze local segments on a portable basis, and monitor

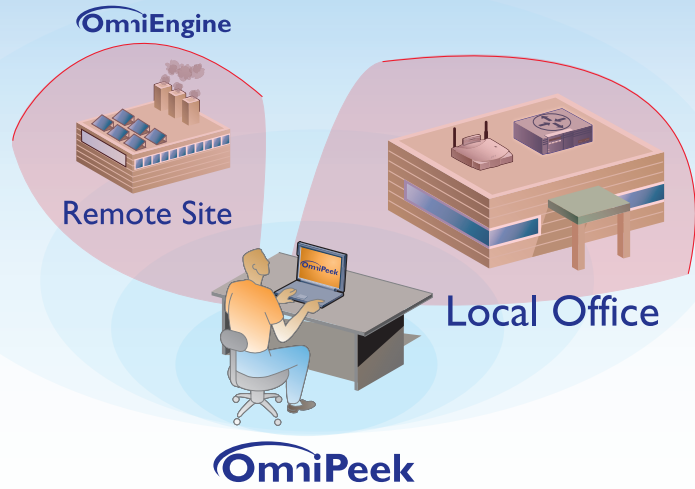


The Apdex dashboard displays user satisfaction scores for the applications on your network.

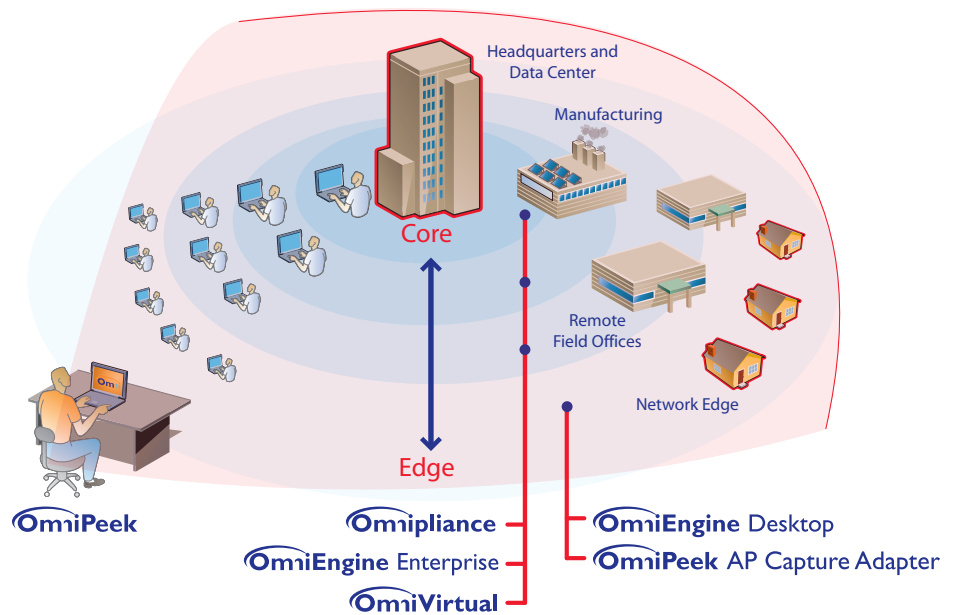
remote locations simultaneously. Using OmniPeek's intuitive user interface and "top-down" approach to visualizing network conditions, network engineers can quickly analyze faults from multiple network segments, drill down through multiple layers of analysis, and pinpoint problems that need correction.

Using OmniPeek engineers can:

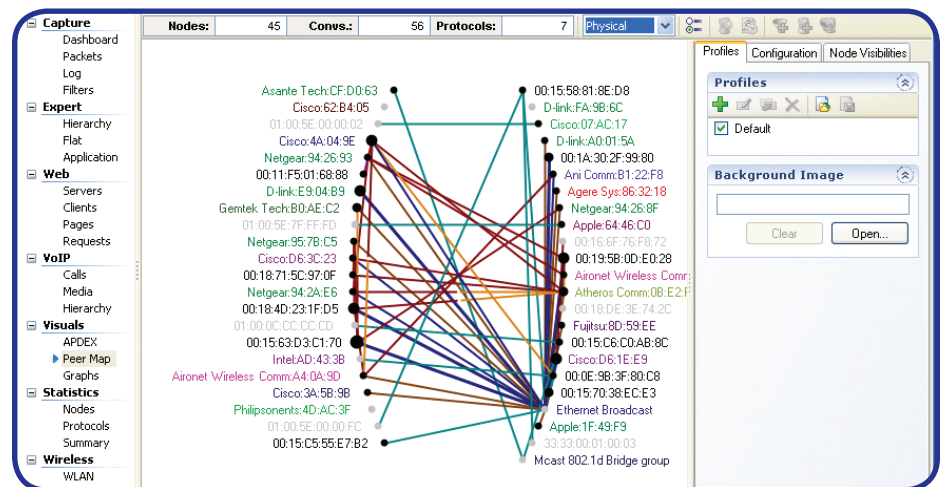
- Analyze traffic from any local network segment, including 10GbE, Gigabit and WAN segments, as well as any network segment configured with an OmniEngine
- Analyze and troubleshoot both data and media traffic using one single product
- Visualize your network from all perspectives—packets, nodes, protocols, conversations and applications.
- Monitor your network with high-level network views, or dashboards, and instantly drill down to see which nodes are communicating, which protocols and sub-protocols are being transmitted, and which traffic characteristics are affecting network performance
- Capture and analyze data from multiple local network adapters, multiple distributed OmniEngines, or any combination of local and remote data
- Leverage your existing wireless network infrastructure by turning managed access points from Cisco or Aruba, and IDS/IPS wireless sensors from AirTight Networks into packet capture devices and collect data from multiple channels simultaneously
- Add reports of wireless interference sources into OmniPeek Summary Statistics, and set triggers on reported interference to troubleshoot interference problems as they occur
- Rely on real-time Expert analysis to do the heavy-lifting, performing aggregated analysis of all network traffic and reporting Expert events as they occur
- Quickly relate Expert events to the offending network traffic flows
- Receive alerts when specific Expert events occur, or when configured Network Policies are violated
- Change filters on the fly without having to stop and restart packet captures



Capturing both locally and at remote sites, OmniPeek provides powerful tools for troubleshooting and performance analysis, eliminating the need for local presence at remote locations.



Distributed analysis allows visibility into the entire network including Virtual Hosted Services and remote locations.



The Peer Map in OmniPeek provides a unique visual summary of communicating nodes, including the volume and traffic type for each node and node pair.

- View packet-stream based analytics by conversation pair, instantly locating network events
- View network traffic in its intended form like PDF, HTML pages, Email, IM, etc.

Ompliance



The Ompliance 2t and Ompliance 6t are 3U appliances built specifically for distributed capture, analysis and recording.

Distributed Network Recorder

The WildPackets Ompliance is a turn-key solution that gives network engineers unprecedented, real-time and post-capture visibility into remote network segments. Each Ompliance network recorder runs WildPackets' OmniEngine Enterprise and sends real-time analytics and monitoring results to OmniPeek consoles. The Ompliance is an ideal data recorder for network forensics applications, such as incident response operations, policy compliance investigations, and transaction analysis. The Ompliance is designed for rapid, convenient deployment. The system can be installed, configured, and online in under an hour. An LCD and keypad on the front panel enable network engineers to enter configuration information such as IP addresses without the use of a keyboard or monitor.

WildPackets' Training and Professional Services

WildPackets' core competency is network analysis. That's what our products do, that's what our instructors teach and that's what our professional services deliver. Our education methodology is centered on practical applications of network and protocol analysis techniques, across a spectrum of network topologies. We focus on what you need to know, not just how to use our products, delivering content that

makes you more productive throughout your day and not just when using OmniPeek. Our professional services team brings decades of experience, as well as objectivity, to any network analysis challenge. Our team is up for any challenge, including application performance analysis; base lining and capacity planning; network troubleshooting; and wireless site survey and security analysis.

About WildPackets, Inc.

WildPackets, Inc., founded in 1990, develops network and application analysis solutions that enable organizations of all sizes to analyze, troubleshoot, optimize, and secure their wired and wireless networks. WildPackets has amassed more than 6,000 customers and its products are sold in over 60 countries in all industrial sectors. Customers include Safeway, Boeing, Siemens, AT&T, Motorola and over 80% of the Fortune 1000. For further information, please visit www.wildpackets.com.

Leading Edge Network Technology

- 10 Gig Support
- 802.11n
- Virtualization support
- Video and Audio Media Analysis
- Application Performance Management



1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
(925)937-3200
fax (925)937-3211

www.wildpackets.com