



OmniEngine™ Software Probe

Building on WildPackets' award-winning network analysis technology, OmniEngine™ performs real-time network analysis on traffic from one or more network interfaces, including Ethernet, Gigabit, 10 Gigabit, 802.11 a/b/g/n wireless, and WAN. OmniEngine captures and analyzes data in real-time, and records data for post-capture analysis. With WildPackets OmniEngine, network engineers can rapidly troubleshoot faults—even faults occurring at remote locations—without leaving their office.

Designed for data centers, network operations centers and large application servers, OmniEngine software extends network analysis capabilities through distribution to any network segment or function, even to remote locations. OmniEngine software can perform data capture and network analysis on multiple network interfaces, and over all network topologies, as well as providing advanced Voice and Video over IP analysis. OmniEngine software is best deployed in large scale, distributed networks that include remote locations, providing continuous network monitoring and analysis without the need for local network engineering support. To completely cover your network analysis needs, one or more OmniEngine software probes should be deployed at each remote location, with every server farm, and within the network operations core.

OmniEngine software runs as a service on standard Windows platforms as well as on WildPackets' Omnipliance® Network Recorder, which is available in both Windows and Linux configurations. By installing OmniEngine software 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 OmniEngine software to ensure that every business location receives the network engineering support it needs.

OmniEngine software provides comprehensive network service analytics, including:

- Monitor networks, application performance and multi-media in separate high-level views, or "Dashboards," and instantly drill down to see which traffic characteristics are affecting network performance
- Application-layer expert diagnoses, application performance, and application response time (ART) analysis
- Complete Voice and Video over IP media and signaling analysis, including MOS and R-Factor scores, detailed packet flow visualization of each call, and call playback
- Complete analysis for leading solutions such as Avaya, Cisco, and MGCP
- Complete visibility into MPLS and VLAN networks by monitoring, gathering statistics, and making graphs and alarms on packet-switched and virtual environment
- Expert Systems Diagnoses, including streams-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 protocol decodes and descriptions of physical errors
- Detailed reporting of all statistical network analysis in a range of output formats, including real-time graphs, HTML, PDF and CSV



Total Network Visibility



Edge to Core Network Analysis

WildPackets' solutions enable businesses to

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

- Flexible Capture Settings tuned to meet every need, from detailed, real time analysis to high-speed capture-to-disk for post-capture analysis
- Forensic search tools to quickly isolate and process data from multiple capture files
- Infrastructure Monitoring, including 24x7 monitoring and analysis of network traffic; when network problems occur, OmniEngine executes SNMP traps, notifying SNMP monitoring systems such as HP OpenView of potential problems; because it captures the traffic that generated the error, OmniEngine software provides network engineers the detailed information they need in order to investigate and resolve problems.

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

OmniEngine Enterprise

OmniEngine Enterprise performs real-time network analysis on traffic from one or more network interfaces, including full-duplex 10 Gigabit and Gigabit, Ethernet, 802.11 a/b/g/n wireless, and WAN. OmniEngine captures and analyzes data and multimedia in real time, and records data for post-capture analysis. OmniEngine Enterprise software provides advanced Voice and Video over

IP functionality including signaling and media analyses, voice and video Expert Analysis, and monitoring of the entire multi-media network. OmniEngine Enterprise is also ideal for IT organizations responsible for application performance and network service level agreements (SLAs) for the entire organization.

When running on an Omnipliance Network Recorder, OmniEngine Enterprise software can capture and store hours or even days of network traffic for forensic analysis.

OmniEngine Desktop

WildPackets' OmniEngine Desktop is a Windows service that runs on desktop computers and captures packets for analysis. OmniEngine Desktop software provides network engineers with the visibility into end user computers they need in order to accelerate troubleshooting and to maximize productivity. Packet captures can be initiated by network engineers or Help Desk representatives running the OmniPeek network analyzer; alternatively, captures can be initiated automatically when specific trigger conditions are met. Once a capture is complete, network engineers can transfer the packets into OmniPeek for analysis.

Omnipliance Network Recorder

The WildPackets Omnipliance Network Recorder is a turnkey, continuous capture solution that gives network engineers unprecedented, real-time and post-capture

visibility into remote network segments. Each Omnipliance Network Recorder runs WildPackets' OmniEngine Enterprise software and sends real-time analytics and monitoring results to a central OmniPeek console. The Omnipliance is an ideal data recorder for network forensics applications, such as incident response operations and policy compliance investigations.

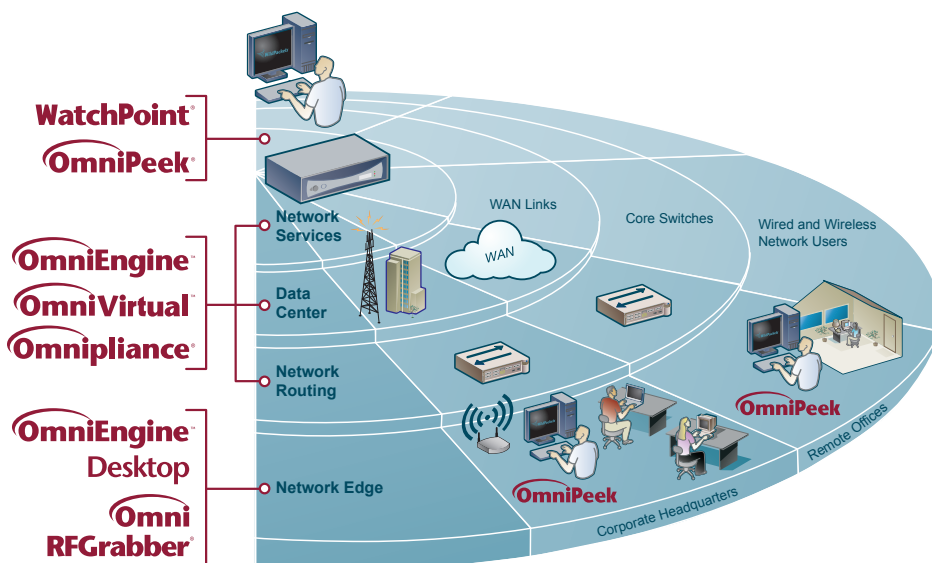
WildPackets OmniPeek Distributed Analysis Suite

The OmniPeek Distributed Analysis Suite gives network engineers real-time visibility into every part of the network simultaneously from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, Video, and WAN links to remote offices. Using the OmniPeek Distributed Analysis Suite, network engineers can rapidly troubleshoot faults and fix problems to maximize network uptime and user satisfaction.

The OmniPeek Distributed Analysis Suite comprises OmniPeek network analyzers and consoles, as well as distributed OmniEngine software probes, Omnipliance Network Recorders, and OmniAdapter Analysis Cards, which continuously capture, analyze and store data at remote locations on the network.

About WildPackets, Inc.

WildPackets develops hardware and software solutions that drive network performance, enabling organizations of all sizes to analyze, troubleshoot, optimize, and secure their wired and wireless networks. WildPackets products are sold in over 60 countries and deployed in all industrial sectors. Customers include Boeing, Chrysler, Fidelity, Motorola, Nationwide, and over 80 percent of the Fortune 1000. WildPackets is a Cisco Technical Development Partner (CTDP). For more information, visit www.wildpackets.com.



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

