

# PacketSentry™ Probe 100/400/1000/2000

**PacketSentry Probes deliver multi-gigabit transaction monitoring, real-time policy enforcement, and identity correlation – with no risk or impact to mission-critical applications.**

The PacketSentry solution employs patented deep-packet analysis technologies and multi-core processing power to convert network traffic into succinct, actionable records of user activity at LAN-speed. The solution leverages identity, directory and application intelligence to facilitate monitoring, search, policy creation, alerting, reporting and controlling user actions with complete business context, enterprise-wide. Simple to use and easy to scale, PacketSentry is the ideal solution to gain immediate control over insider threats without significant operational overhead.

The PacketSentry solution is comprised of hardened, high-speed network appliances that are installed out-of-band for easy, rapid deployment. PacketSentry's two-tier architecture consists of one or more Probes and a single Manager to deliver both scalability and flexibility:

- **Manager: Stores transaction records sent by probes; manages rules; provides single user interface for entire solution**
- **Probes: Monitors network traffic; sends transactions records continuously to Manager; enforces real-time rules**

PacketSentry Probes are deployed in key locations on the network, typically connected to network switch monitor (SPAN) ports in front of data centers. Due to the passive nature of the probe, application availability or performance is never affected. Each Probe processes network traffic and conducts L4-7 decode analysis to identify applications, decode transactions, bind user identities and enforce PacketSentry rules. All communication between the PacketSentry Manager and Probes is authenticated and encrypted. This scalable architecture allows companies to easily expand monitoring and control coverage as needed because the Manager seamlessly combines traffic from all probes into a unified, user-correlated transaction database.

PacketMotion offers a full range of Probes that deliver monitoring and enforcement capabilities and address the complete needs of any size organization:

**Probe 100: Remote Office**  
(Traffic analysis up to 100Mbps)

**Probe 400: Mid-size Locations**  
(Traffic analysis up to 400Mbps)

**Probe 1000 and 2000: Data Centers**  
(Traffic analysis up to 1 or 2Gbps)



## PacketSentry™

A comprehensive insider threat management solution with no impact to application availability or performance

- **Track sensitive data access and movement**
- **Understand and control high-risk user activity**
- **Solve data classification challenges**
- **Automate audit, investigation, and compliance reporting**
- **Track network bandwidth usage by identity**

Ease of deployment, administration, and maintenance drives low cost of ownership

**PacketMotion™**

© 2008 PacketMotion, Inc.

## PacketSentry Solution Features and Benefits

FEATURES	BENEFITS
Passive Monitoring and Application Decode Solution	Complete visibility of user activity, with no risk to applications. Solve data classification challenges by tracking user behavior
Agent-less Monitoring and Control	No agents on servers or PCs, or domain controllers – no application performance impact or integration challenges
Deep Inspection Decode System	Detect and decode over 50 applications, including port-hopping and web-based applications
Application Identification and Monitoring: Use context, protocol information to identify applications on any port. More than 150 application are supported	Enable application monitoring and control based on application profile rather than ports – track and control application usage by identity
Advanced Transaction Analysis: Captures all business-level network transactions down to the database and database table, directory/folder name and filename, e-mail, webmail, chat and P2P sources, destination and attachments	Readily gain granular user, group and information movement insight. Apply policies based on specific actions: read, write, delete, etc.
Active Directory or other LDAP-compliant directory integration	All network activity and transactions correlated with user identity in real time. Build policies based on directory groups, or leverage custom groups for flexibility
File Permissions and Active Directory Change Monitoring	Maintain complete audit and control of file permissions and ownership of critical data. No server agents or use of NAS API that could degrade end-user response time
Failed Access Monitoring	Detect and record failed attempts to access data; identify suspicious activity and vulnerability probing
User Tracking: Full details on IT administrators, contractor and unknown (rogue) user access to data center assets – with assured identity and response	Readily gain comprehensive user action visibility – including high-risk users – even in Citrix thin-client environments.
Rules Engine	Real-time policy enforcement and alerts. Build and deploy virtual policies network-wide in seconds
Policy Enforcement	Optional injection of TCP resets to enforce policy
Centralized Management	Ease of use: Entire solution controlled from single user interface, independent of number of probes deployed.
Intel quad-core CPU architecture – Up to four quad-cores per probe	High performance enables decode of all network traffic. Automatically identify all activity in a dynamic environment
Full redundancy of key components	Highly-available; lower maintenance costs
Dedicated Management Port	Separate out-of-band management traffic: compressed, encrypted management solution for security and bandwidth conservation
Pass-Through/Fail-Open Monitor Port	Share single switch monitor (SPAN) port with multiple devices. Probe bypassed automatically on power failure
Automatic disk caching	No data lost upon WAN link failure to remote probe
SPAN or TAP connectivity options	Flexible deployment methods for any environment or architecture

## Specifications

	Probe 100	Probe 400	Probe 1000	Probe 2000
<b>PERFORMANCE</b>				
Capacity (Monitoring Throughput)	100Mbps	400Mbps	1Gbps	2Gbps
<b>PORTS</b>				
Traffic Monitoring	1 RJ-45 Ethernet 10/100/1000	3 RJ-45 Ethernet 10/100/1000	3 RJ-45 Ethernet 10/100/1000	3 RJ-45 Ethernet 10/100/1000
Management	1 RJ-45 Ethernet 10/100/1000	1 RJ-45 Ethernet 10/100/1000	1 RJ-45 Ethernet 10/100/1000	1 RJ-45 Ethernet 10/100/1000
Enforcement	1 RJ-45 Ethernet (Shared with Management)	1 RJ-45 Ethernet 10/100/1000	1 RJ-45 Ethernet 10/100/1000	1 RJ-45 Ethernet 10/100/1000
Pass-Through	None	1	1	1
Console	1 x Serial (RS232 DB-9 Male)	1 x Serial (RS232 DB-9 Male)	1 x Serial (RS232 DB-9 Male)	1 x Serial (RS232 DB-9 Male)
Future Expansion	1 RJ-45 Ethernet 10/100/1000	No	No	No
<b>REDUNDANCY</b>				
Redundant Power	Yes	Yes	Yes	Yes
Redundant Fan	Yes	Yes	Yes	Yes
Fail-Open or Bypass	No	Yes	Yes	Yes
Redundant Hard Disks (RAID-1)	Yes	Yes	Yes	Yes
<b>DATA STORAGE</b>				
Disk Drives (SATA)	2 x 250GB	2 x 320GB	2 x 320GB	2 x 320GB
Effective Storage Capacity	250GB	320 GB	320 GB	320 GB
<b>DIMENSIONS AND POWER</b>				
Dimension(HxWxD)	1.7"x17.2"x25.6" (4.3cm x 43.7cm x 65.0cm)	5.25"x17"x27.25" (13.3cm x 43.2cm x 69.2cm)	5.25"x17"x27.25" (13.3cm x 43.2cm x 69.2cm)	5.25"x17"x27.25" (13.3cm x 43.2cm x 69.2cm)
Rack Space Required	1RU	3RU	3RU	3RU
Weight	32 lbs (14.5kg)	70 lbs (31.75kg)	70 lbs (31.75kg)	70 lbs (31.75kg)
Power Supply	650W (1 + 1) Redundant AC power supply w/ PFC  AC Voltage : 100 - 240V, 60-50Hz, 3.5A/1.75A	550W (2+1) Redundant AC power  AC Voltage: 100-240VAC, 50-60Hz, 4.6A/2.3A (1.5A/0.75A per input)	550W (2+1) Redundant AC power  AC Voltage: 100-240VAC, 50-60Hz, 4.6A/2.3A (1.5A/0.75A per input)	550W (2+1) Redundant AC power  AC Voltage: 100-240VAC, 50-60Hz, 4.6A/2.3A (1.5A/0.75A per input)
<b>ENVIRONMENT</b>				
Operating Temperature	10°to 35°C (50°to 95°F)	10°to 35°C (50°to 95°F)	10°to 35°C (50°to 95°F)	10°to 35°C (50°to 95°F)
Non-operating Temperature	-40°to 70°C (-40°to 158°F)	-40°to 70°C (-40°to 158°F)	-40°to 70°C (-40°to 158°F)	-40°to 70°C (-40°to 158°F)
Operating Relative Humidity	8% to 90% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)
Non-operating Relative Humidity	5 to 95% (non-condensing)	5 to 95% (non-condensing)	5 to 95% (non-condensing)	5 to 95% (non-condensing)
Altitude	Up to 3000m, (10,000 ft.)	Up to 3000m (10,000 ft.)	Up to 3000m (10,000 ft.)	Up to 3000m (10,000 ft.)
<b>CERTIFICATION</b>				
	EN 60950/IEC 60950-Compliant, TUV Certified, CE Marking (Europe)	FCC Part 15/Subpart B/ Class A, TUV/CSA-60950, CE	FCC Part 15/Subpart B/ Class A, TUV/CSA-60950, CE	FCC Part 15/Subpart B/ Class A, TUV/CSA-60950, CE

## Ordering Information

PRODUCT	PART NUMBER
PacketSentry Probe 100	PS-PRB-100-0300
PacketSentry Probe 400	PS-PRB-400-0300
PacketSentry Probe 1000	PS-PRB-1000-0300
PacketSentry Probe 2000	PS-PRB-2000-0300

## About PacketMotion

PacketMotion is the developer of the industry's first security solution that gives businesses the ability to see user activity inside their networks as it happens, allowing them to identify improper actions in real time and to instantly respond. PacketSentry works with an organization's existing infrastructure and processes to cost-effectively safeguard assets, automate compliance and governance practices, and reduce business risk. For more information:

**Visit** [www.packetmotion.com](http://www.packetmotion.com)  
**Call** 408.449.4300  
**Email** [info@packetmotion.com](mailto:info@packetmotion.com)

**PacketMotion**<sup>™</sup>

110 Baytech Drive, Suite 200, San Jose, CA 95134

Phone 408.449.4300 Fax 408.945.4301

©2008 PacketMotion, Inc. All rights reserved.