



# IPS-1

*Robust and accurate intrusion prevention*

## YOUR CHALLENGE

The velocity at which change occurs in today's network environments is staggering. Daily changes in the network environment, delays in providing operating system patches, along with a constant threat of targeted attacks by hackers—and even the unknowing launch of worms by employees from within the organization—all translate into windows of real-time exposure that make enterprises vulnerable. Today's network environments introduce more vulnerabilities than most security teams can track—let alone be able to manage and patch. Simply put, this leaves networks—and your business—open to inevitable attack.

## OUR SOLUTION

Check Point IPS-1™ is a dedicated intrusion prevention system (IPS) solution that delivers mission-critical protection with unmatched management and granular forensic analysis capabilities and flexible deployment. The IPS-1 Hybrid Detection Engine™ delivers active detection and prevention at the network perimeter while the IPS-1 Dynamic Shielding Architecture™ drives preemptive functions to protect the network interior. Additional prevention is enabled through Confidence Indexing™, which delivers unmatched flexibility in deploying prevention across the network. All these IPS-1 functions are controlled by powerful centralized management that readily supports both small- and large-scale deployments.

### ACCURATE AND GRANULAR ATTACK PREVENTION

Designed to provide immediate and reliable blocking of unwanted network traffic, IPS-1 systems not only stop backdoor and hybrid threats (such as Code Red, MS Blaster, Nimda, and SQL Slammer worms), but also attacks including SQL injection, command tampering, and polymorphic buffer overflows—in real time before they can affect your organization. From its core outward, IPS-1 is built to deliver trusted intrusion prevention while minimizing the time, costs, and staff requirements associated with intrusions.

At the heart of IPS-1 is the Hybrid Detection Engine™ which leverages multiple detection and analysis techniques including vulnerability signatures, exploit signatures, anomaly detection, protocol analysis, application awareness, smart IP reassembly, operating system and application fingerprinting, multi-element correlation, and dynamic worm mitigation. This robust detection engine ensures coverage across a broad range of the threat spectrum, ensuring IT assets are protected against known and unknown threats.

In addition to the standard, out-of-the-box configuration, the IPS-1 Hybrid Detection Engine includes a powerful and flexible signature language that allows security managers to write new protocol decoders and signatures as well as customize existing ones to ensure accurate attack detection.

## PRODUCT DESCRIPTION

Check Point IPS-1™ is a dedicated intrusion prevention system (IPS) that delivers mission-critical protection with unmatched management and granular forensic analysis capabilities and flexible deployment.

## PRODUCT FEATURES

- Hybrid Detection Engine™ leverages multiple detection and analysis techniques to prevent network- and application-layer attacks
- Confidence Indexing™ offers the unique ability to direct and calibrate enforcement
- Advanced forensic analysis and reporting
- Centralized management provides real-time, graphical views across all IPS-1 Sensors
- Powerful, flexible signature language enables customized signatures and protocol decoders

## PRODUCT BENEFITS

- Protects IT systems against both known and unknown attacks
- Provides immediate, reliable blocking of unwanted network traffic
- Aids forensic investigations to effectively pinpoint sources of attack and their scope
- Simplifies IPS deployment and administration



IPS-1 includes a unique feature called Confidence Indexing that enables your administrators to direct and calibrate prevention enforcement according to factors such as the threat and asset under attack. In this way, IPS-1 earns your trust that only legitimate traffic can get through and reduces the chances of false-positives.

**AWARE, ADAPTIVE, AND ACTIONABLE SECURITY**

IPS-1 provides security that is aware, adaptive, and actionable. This means it has awareness of the network environment, adapts to changes in the environment, and can take action to protect those changes from exploitation. This makes your network more secure while simplifying network security management, freeing your network security team to focus on more value-added security functions.

The IPS-1 Dynamic Shielding Architecture is a breakthrough in intrusion prevention and is the key to achieving highly aware, adaptive, and actionable security. IPS-1 automatically recognizes threat points and dynamically protects them against inevitable attack. IPS-1 determines critical vulnerabilities and changes in the network, alerts security managers to these threat points, and automatically deploys the proper signature sets to protect threat points before they are attacked.

**ADVANCED FORENSIC ANALYSIS AND REPORTING**

IPS-1 features impressive analysis capabilities to quickly help administrators dissect attack data and compile reports on attack and event trends. Through the IPS-1 Management Dashboard, administrators get real-time, high-level graphical views across all sensors as well as the ability to drill-down and group event and alert data to effectively pinpoint attack sources and their scope. Administrators can customize attack graphs and attack-vector timelines, forming their own window to monitor real-time attack and prevention activity. Alert data can be easily sorted into common groups, which are customizable based on user-configurable criteria. Alerts can be grouped by any field such as source IP, attack type, and target vulnerability.



An intuitive Timeline View makes it easy for administrators to analyze alerts that appeared within a particular time period.

Ad hoc reports can also be easily generated using Crystal Reports. Administrators can choose from an assortment of predefined reports and can easily modify them to suit their needs.

**INTUITIVE CENTRALIZED MANAGEMENT**

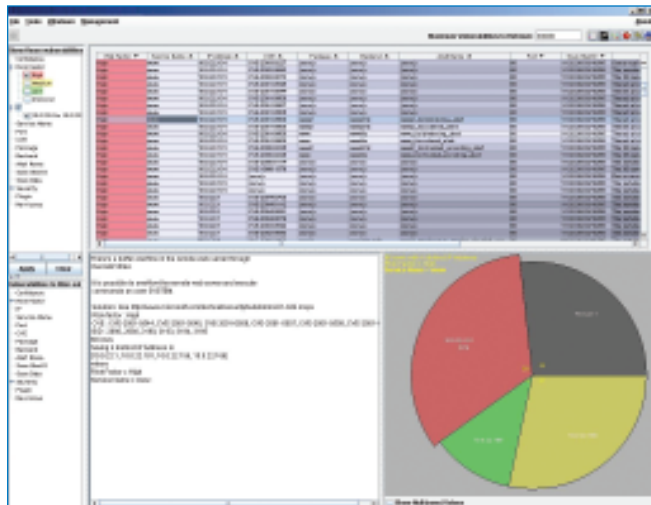
IPS-1 centralized management delivers simplicity with small deployments and intuitive, powerful centralized control and scalability for large enterprise deployments.

Using graphics, automation, and wizard-driven features, IPS-1 saves your network security staff time by making management of network security more intuitive and more efficient. Wizard-driven approaches to configuring key features include real-time monitoring and policy management. Also, there is the Consolidate Alerts capability for aggregating event data on any field including compound fields.

**IPS-1 ARCHITECTURE**

IPS-1 systems are based on a three-tier architecture, providing efficient management and a small footprint for small deployments while easily scaling to support large-scale deployments of hundreds of sensors. Each IPS-1 system is composed of the following components:

- IPS-1 Sensors — IPS-1 Sensors leverage multiple detection and analysis techniques to deliver proven network protection against a wide variety of threats. Each sensor is capable of operating in passive intrusion-detection or inline passive or inline active IPS modes. IPS-1 Sensors come preconfigured in a variety of models, depending on organization needs and network location (see models and specifications section for more information)
- IPS-1 Management Server — the IPS-1 Management Server receives, processes, and manages alert and event data generated by IPS-1 Sensors and provides a centralized facility for IPS-1 Sensor management

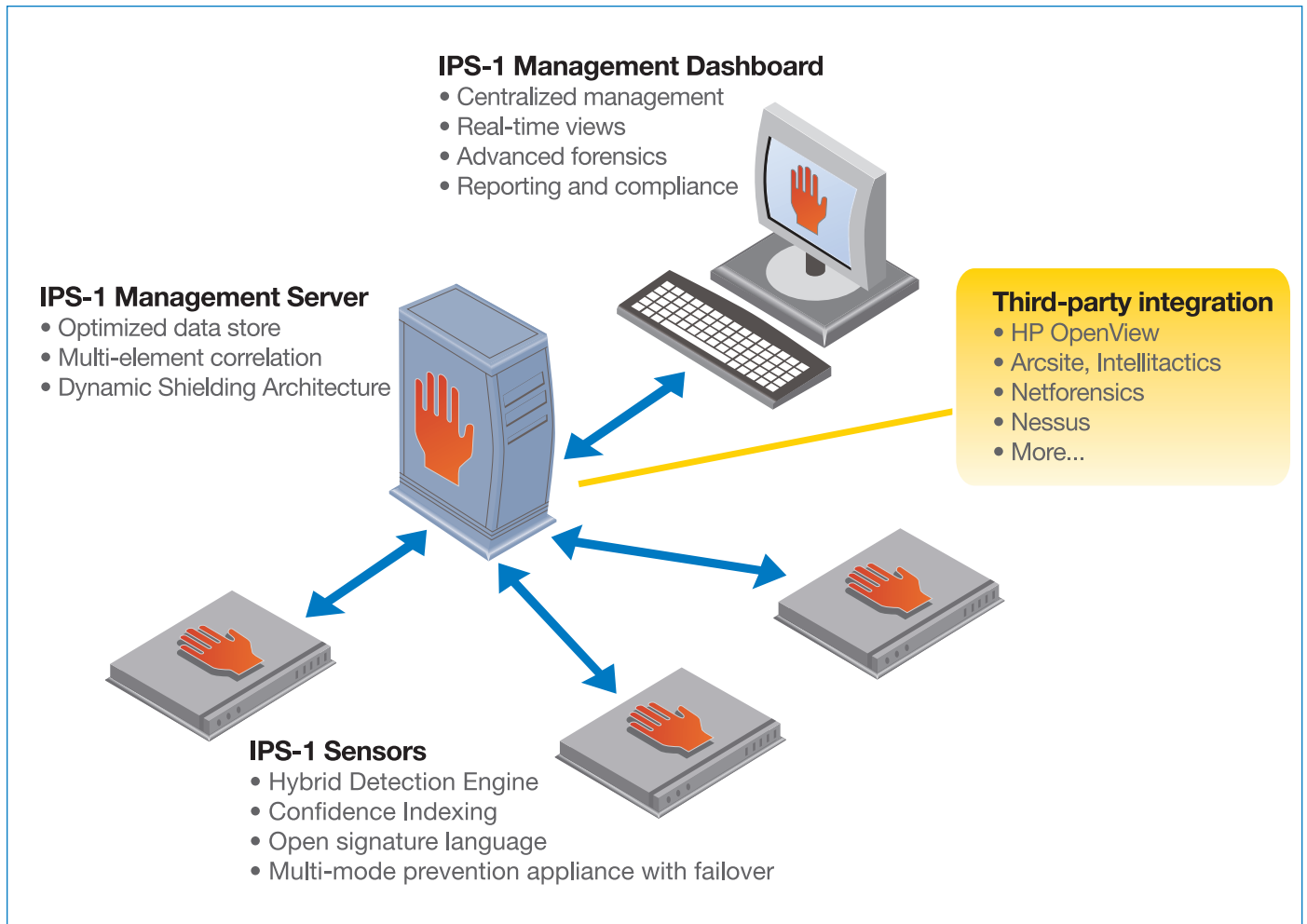


The IPS-1 Vulnerability Browser enables vulnerability scanning, viewing, and management from a single dashboard.

- **IPS-1 Management Dashboard**—the IPS-1 Management Dashboard is the management component of IPS-1. Through the IPS-1 Management Dashboard, administrators can monitor alerts generated throughout the system and perform high-level analysis

**ONGOING SECURITY UPDATES VIA SMARTDEFENSE SERVICES**

IPS-1 systems, like other Check Point security solutions, are backed by Check Point SmartDefense™ Services, which provide ongoing and real-time updates and security advisories, helping ensure that Check Point security solutions are continuously updated to stay ahead of today’s constantly evolving threats. Security experts at the Check Point SmartDefense Research Center continuously monitor the Internet for new exploits and vulnerabilities and rapidly develop and deliver new defenses and signatures to help ensure that you are protected from the latest threats.



The IPS-1 intrusion prevention system is based on a three-tier architecture, providing reliability and scalability.

## IPS-1 MODELS AND SPECIFICATIONS

	IPS-1 Sensor 50	IPS-1 Sensor 200	IPS-1 Sensor 500	IPS-1 Power Sensor 1000	IPS-1 Power Sensor 2000
Network location	Remote office/network perimeter	Remote office/network perimeter	Network perimeter (multi-segment)	Network core (multi-segment)	Network core (multi-segment)
<b>Performance</b>					
Throughput (IPS/IDS)	50/75 Mbps	200/250 Mbps	500Mbps/1Gbps	1/2Gbps	2/4Gbps
Concurrent sessions (rated max.)	100,000	200,000	500,000	1.2 million	2.8 million
<b>Physical characteristics</b>					
Form factor	1-RU	1-RU	1-RU	2-RU	2 @ 2-RU
Dimensions, H x W x D in. (cm)	1.703 x 16.8 x 13.4 (4.325 x 42.6 x 37.98)	1.703 x 16.93 x 26.457 (4.325 x 43.0 x 67.2)	1.703 x 16.930 x 26.457 (4.325 x 43.0 x 69.8)	3.5 x 17 x 22.5 (8.9 x 43.2 x 57.1)	2 @ 3.5 x 17 x 22.5 (8.9 x 43.2 x 57.1)
Weight, lbs (kg)	15 (6.8)	31 (14.1)	35 (15.8)	40 (18)	2 @ 40 (18)
Monitoring interfaces	2 x 10/100/1000 Mbps copper	2 x 10/100/1000 Mbps copper or 2 x 1000 Mbps fiber	4 x 10/100/1000 Mbps copper or 4 x 1000 Mbps fiber	8 x 10/100/1000 Mbps copper or 8 x 1000 Mbps fiber	8 x 10/100/1000 Mbps copper or 8 x 1000 Mbps fiber
Management interfaces	1 x 10/100/1000 Mbps copper	1 x 10/100/1000 Mbps copper	1 x 10/100/1000 Mbps copper	10/100 Mbps copper	10/100 Mbps copper
Lockable front bezel	No	Yes	Yes	No	No
Redundant power supplies	No	Yes	Yes	Yes	Yes
Redundant storage	No	No	No	Yes	Yes
Hardware-level bypass	Yes	Yes	Yes	Yes (copper only)	Yes (copper only)
Hot-swappable main components	No	No	No	Yes	Yes
Scalable to higher data rates	No	No	No	Yes	Yes
<b>Power</b>					
Amps	6/3	6.5/3.2	6.7	5	10 (5 per box)
Voltage (AC)	110/220	100/127	100/127	110/220	100/240
Input range (AC)	100-240	100-127/200-240	100-127/200-240	-	-
<b>Environmental range</b>					
Operating temp.	0°C to 40°C	10°C to 35°C	10°C to 35°C	0°C to 40°C (ambient)	0°C to 40°C (ambient)
Nonoperating temp.	-20°C to 80°C	-40°C to 70°C	-40°C to 70°C	-	-
Relative humidity (nonoperating)	10% to 90% (noncondensing)	10% to 90% (noncondensing)	10% to 90% (noncondensing)	10% to 90% (noncondensing)	10% to 90% (noncondensing)
RF emissions	FCC Class A Device	FCC Class A Device	FCC Class A Device	FCC Part 15 Class A Subpart B (U.S./Canada)	FCC Part 15 Class A Subpart B (U.S./Canada)

\*NSS-approved certification achieved on Sentivist™ Smart Sensor 100C v1.3.



©2003–2007 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, ConfidenceIndexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMSecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988, and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

February 13, 2007 P/N 502334

### Worldwide Headquarters

3A Jabotinsky Street, 24th Floor  
Ramat Gan 52520, Israel  
Tel: 972-3-753-4555  
Fax: 972-3-575-9256  
Email: info@checkpoint.com

### U.S. Headquarters

800 Bridge Parkway  
Redwood City, CA 94065  
Tel: 800-429-4391; 650-628-2000  
Fax: 650-654-4233  
www.checkpoint.com



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.