

## Multi Layer Intrusion Prevention and DoS Protection



### APbsolute Immunity: Your Business' Clear Choice for Proactive Network Security

Protecting the network perimeter alone is no longer sufficient in a world where boundaries are increasingly erasing and threat sources are rapidly multiplying. DefensePro®, Radware's comprehensive intrusion prevention and denial of service (DoS) protection solution, provides enterprises and carriers with complete immunity against known, emerging and zero-minute threats across the network.

DefensePro combines vulnerability-based signature protections with automatic, real-time signatures so you can proactively protect your business from what you know, and more importantly, what you don't know. DefensePro provides full protection against known threats through signature updates, which safeguard against vulnerability-based attacks including worms, Trojans, Bots, SSL-based attacks and VoIP threats. In addition, DefensePro provides unique behavioral-based and automatically generated, real-time signatures that further prevent unknown non-vulnerability threats and zero-minute attacks such as application misuse attacks, server brute force attacks, and application and network flooding. And, DefensePro accomplishes this all, without blocking legitimate user traffic and without the need for human intervention.

And, if you're worried about user experience, DefensePro's integrated bandwidth management module enables dynamic traffic shaping to guarantee bandwidth and service levels for critical applications while restricting bandwidth consumed by non-critical applications such as peer-to-peer.

*With DefensePro APbsolute Immunity, worry-free security is only a few seconds away.*

### Key Business Values

- Maintains business continuity even when the network is under attack
  - Ensures servers' survivability and critical application (web, mail, FTP, DNS and more) availability even under network attack, server and application attack
  - Wide coverage against current and emerging, known and zero-minute threats including non-vulnerability attacks, application misuse, application and network flooding, pre-attack probes, worms Trojans, Bots, and more
  - Blocks attacks without blocking legitimate users' traffic, so infected hosts can continue to work uninterrupted
- Reduces total cost of ownership (TCO) of security management
  - Reduce CAPEX through "pay-as-you-grow" licensing for maximum investment protection by scaling solution costs to needs
  - Reduce OPEX through automatic signature generation and activation for the duration of the attack without human intervention
  - Adapts to changing network conditions - requires minimal configuration without the overhead of system tuning and ongoing maintenance
  - Seamless integration into the network environment
- Reduces link capacity costs for carriers
  - Removes high volume worm propagation and DoS/DDoS flood attacks
  - Immediate response to known and zero-minute attacks without blocking legitimate user traffic during attack
- Ensures Service Level Agreement (SLA) for service providers
  - Service Level guarantee using BWM rules

## Comprehensive Application Vulnerability Protection

### Full Application Security for the Enterprise and Data Centers

Securing the enterprise and data centers DefensePro signature engine includes web protection against IIS and Apache vulnerabilities, SQL injection and cross-site scripting; mail server protection against POP3, IMAP and SMTP vulnerabilities; SQL servers and DNS service protection against SQL and DNS vulnerabilities; remote access protection against Telnet and FTP server vulnerabilities; SIP servers, proxies and IP phones against SIP protocol violations preventing shut downs, denial of service and malicious takeovers; and malware protection against worms, Trojan Horses, Spyware, Phishing and backdoor attacks.

### Protection Against Encrypted, SSL-Based Attacks

In conjunction with Radware's AppXcel™ application accelerator appliance, DefensePro provides a powerful and scalable solution for protection against encrypted SSL-based attacks that would otherwise evade regular security inspection. While the original SSL tunnel is maintained between the client and the server, DefensePro copies the SSL traffic to an AppXcel device, which decrypts the traffic and forwards it for inspection to DefensePro. When an attack is detected in the decrypted SSL traffic, DefensePro reports and terminates the malicious session in real-time.

### Security Updates

With Security Update Service, Radware's 24x7 Security Operations Center (SOC) provides subscribers with automated, weekly delivery of new attack signatures as well as emergency and custom delivery of signatures. This helps ensure networks and applications are fully protected from current and emerging vulnerabilities.

## Network-Based Adaptive Behavioral-Based Protection

### Advanced, Multi-Layer DoS/DDoS Flood Protection

Protection is provided against both known attacks and unknown zero-day attacks. DefensePro protects against DoS attacks caused by a single packet or several packets, such as buffer overflows, Ping of Death, and Land attacks. In addition, adaptive behavior-based DoS protection mitigates zero-day DoS/DDoS flood attacks (see figure 1). Known and unknown flood attacks that are blocked include:

- TCP SYN Floods
- UDP and DNS Floods
- TCP Push, Fin and reset floods
- ICMP and IGMP Floods

### Zero-Day Worm Propagation Prevention

DefensePro detects and prevents malicious activity created by advanced self-propagating network worms that use random or pseudo-random spreading techniques. The detection technique is based on adaptive behavioral analysis of user traffic and utilizes the fuzzy logic engine for decision making (see figure 2). Using a closed-feedback technology, the countermeasures employed against a worm adapt dynamically in real-time, to the worm's ever-changing behavior, thus insuring that even "smart" mutating worms are handled quickly and persistently.

### Proactive Prevention of Network Scanning and Pre-Attack Probes

Prior to launching an attack, hackers often look for open application ports on network servers or available machines on a service port. DefensePro detects and mitigates scanning activity that threatens to compromise your mission-critical systems. Reconnaissance protection capabilities include mitigation of known and unknown scanning tools and all types of port scanning, including horizontal scans, vertical scans, stealth scans and ICMP sweeps.

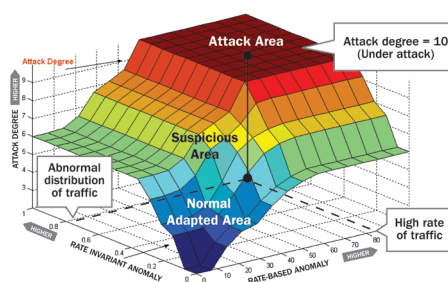
## Server-Based Adaptive Behavioral-Based Protection

### HTTP Page Flood Protection

The HTTP Mitigator feature deploys the behavioral security technology to prevent HTTP page flood attacks that are often generated by malicious tools such as HTTP BOTs and HTTP page flooders. These tools are used directly by hackers or are installed unwittingly on victim computers. They systematically download web pages from a web site attempting to exhaust its resources and create service denial.

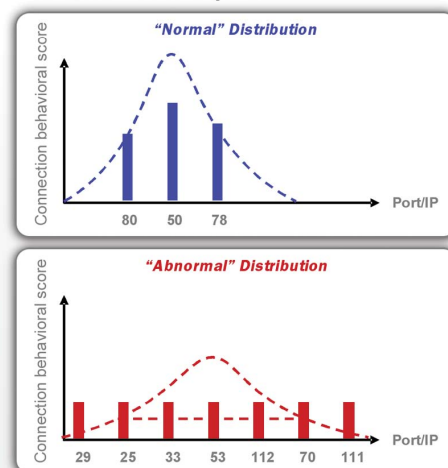
### Server-Crack Protections

DefensePro also extends adaptive behavioral technology to the detection of application level pre-attack probes, misuse of authorization and denial-of-service attacks. The Server-Crack Protections include HTTP, FTP, POP3, IMAP, SIP, MS-SQL server-based adaptive behavioral protections. Threats that are detected and prevented include: brute-force attempts, dictionary attacks, HTTP vulnerability scanning, SIP spoofed Invite floods, SIP spoofed register floods and more.



**Figure 1: Adaptive Decision Engine**  
DefensePro is unique in its ability to rapidly and accurately distinguish between three broad categories of behavior: legitimate normal traffic, attack traffic and unusual patterns created by legitimate activity.

### User Distribution Space



**Figure 2: Worm Activity Prevention**  
DefensePro Worm detection is based on an analysis of a host payload distribution across its connections in the network. Worm filtering is performed on user-infected traffic while allowing legitimate traffic to flow uninterrupted.

## Bandwidth Management and Access Control for End-to-End Traffic Shaping and Optimization

DefensePro's Bandwidth Management and Access Control modules enable dynamic control of bandwidth from end-to-end. Bandwidth can be guaranteed or limited per client, per session or per application. Access control of traffic, per application ports, hosts and networks, allows only predefined application traffic. For example, controlling the bandwidth usage of peer-to-peer (P2P) applications ensures adequate bandwidth for legitimate application traffic.

## Hardware Architecture

### The industry's first software-scalable throughput licensing

DefensePro allows users to increase throughput without a hardware upgrade, providing unparalleled investment protection. The DefensePro-x02 series offers software throughput upgrades from 100 to 200, and 500 Mbps. The DefensePro-x20 allows software throughput upgrades from 600 Mbps to 1 Gbps and 3 Gbps.

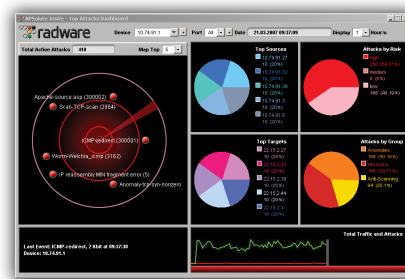
### Redundancy and high availability

DefensePro's built-in internal bypass feature ensures high network availability in the event of hardware (i.e., power) and software malfunctions. A dual power supply provides automatic failover if the primary power supply fails<sup>1</sup>. The Advanced Overload mechanism optimizes security coverage under extreme traffic load, maintaining maximum security without dropping packets.

## Security Management, Monitoring and Reporting

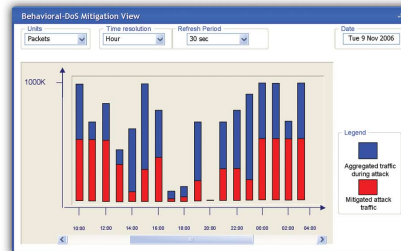
With features that enable centralized device configuration, monitoring and reporting, Radware's Insite management solution<sup>2</sup> increases visibility and control of network security. Insite offers:

- The ability to customize security policies for each network segment using the Connect & Protect policy configuration table
- Real-time dashboards that enables administrators to monitor top attacks, top attack sources and destinations and worm propagation activity in your network (see Figure 3)
- Real-time traffic monitoring allowing the Admin to observe the normal traffic behavior and attacks volume that were mitigated by DefensePro (see figure 4 and 5)
- Real-time security event monitoring and advanced forensics for examining historic network activity down to the packet level.
- Pre-defined and customized executive reporting capabilities to support security decision-making and investments.



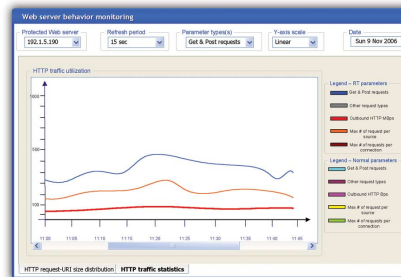
**Figure 3: Real-Time Dashboard**

A real-time dashboard provides security managers with immediate awareness of the top attacks on their networks and affected systems.



**Figure 4: Real-Time Traffic Monitoring and Mitigation View**

Real-time traffic monitoring views expose DefensePro attack mitigation capabilities to the managerial level showing normal traffic vs. attack traffic that was filtered out to provide immediate ROI visualization.



**Figure 5: Real-Time Web server behavior Monitoring**

Real-time Web server traffic monitoring enables the Admin to view normal vs. real-time HTTP request distribution rates.

## Radware APSolute™ Product Suite

Radware, the global leader in integrated application delivery solutions, assures the complete availability, performance and security of business-critical applications for more than 5,000 enterprises and carriers worldwide. With Radware's comprehensive and award-winning APSolute suite of application front end, access, and security products, companies can drive business productivity, improve profitability, and reduce IT operating and infrastructure costs by making their networks "business-smart."

## Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements - phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

## Learn More

To learn more about how Radware's integrated application delivery solutions can enable you to get the most of your business and IT investments, email us at [info@radware.com](mailto:info@radware.com) or go to [www.radware.com](http://www.radware.com).

1. The dual power supply is only available for the DefensePro-x20 series  
2. Available as a DefensePro Option



## Technical Specifications



DefensePro Model	DP-3020	DP-1020	DP-620	DP-502	DP-202	DP-102
ASIC-based Hardware Platform	Application Switch 4 (DP-x20 Series)			Security Platform 1 (DP-x02 Series)		
<b>Performance<sup>4</sup></b>						
Max. Throughput	3 Gbps	1 Gbps	600 Mbps	500 Mbps	200 Mbps	100 Mbps
Maximum Concurrent Sessions	1,600,000 <sup>2</sup>	1,600,000 <sup>2</sup>	1,600,000 <sup>2</sup>	500,000	500,000	500,000
Maximum SYN Flood Attack Rate (SYNs per second)	4,000,000 <sup>4</sup>	4,000,000 <sup>4</sup>	4,000,000 <sup>4</sup>	70,000	70,000	70,000
Latency (micro-seconds)	< 200					
<b>Ports</b>						
GE (GBIC)	8	8	8	-	-	-
10/100/1000 Copper	12	12	12	3	3	3
Console RS-232C	1	1	1	1	1	1
<b>Scanning Ports</b>						
Maximum Segments	9	9	9	1	1	1
Network Operation	Transparent L2 Forwarding					
Deployment Operation Modes	In-line, SPAN Port Monitoring and Copy Port					
Operation Modes	Block & Report, Report Only					
<b>Management Ports</b>	Includes GE, FE and RS-232					
<b>Tunneling Protocols Support</b>	L2TP, MPLS, GRE, GTP, VLAN Tagging					
<b>Signature Protections</b>	Web Protection, Mail Servers Protection, FTP Servers Protection, DNS Vulnerabilities, Cross-Site Scripting, SNMP Vulnerabilities, Worms and Viruses, Brute Force Protection, SQL Injections, Backdoors and Trojans, Spyware, Custom Attack Signatures, LAN Protocol and Services Protection (RPC, NetBIOS, Telnet etc.), Generic Payloads (Remote Execution, Shellcodes), SIP Protection, user-defined signatures, Security updates service					
<b>Server-Crack Protection</b>	Brute force attacks, cracks and scans of web sites, mail servers (SMTP, POP3, IMAP), FTP servers, SIP servers, MS-SQL, MYSQL					
<b>Reconnaissance Detection</b>	Horizontal and Vertical TCP and UDP Scanning, Stealth Scanning, Ping Sweeps, Worm Propagation Prevention					
<b>Stateful Operation</b>	TCP Stream Reassembly, IP Defragmentation					
<b>Stateful Inspection</b>	RFC Compliance verification for TCP, ICMP, DNS, HTTP, HTTPS, SMTP, IMAP, POP3, FTP, SSH					
<b>Network DoS/DDoS Protection<sup>3</sup></b>	Adaptive Behavior-based, Zero Day protection. Flood Protection for SYN, TCP, UDP, UDP (with ICMP Back Scattering), DNS Query, ICMP, IGMP, IP Fragment Floods. Blocking is done through "Automatic Real Time Signatures". TCP Connection Flood Protection.					
<b>HTTP Flood Protection<sup>3</sup></b>	Adaptive behavior based web server traffic monitoring detecting and preventing known and zero-day HTTP Page Flood attacks. Blocking is done through "Automatic Real Time Signatures".					
<b>Automatic Real Time Signatures (Packet Filter Criteria)</b>	Source IP, Destination IP, Source Port, Destination Port, Packet ID, Packet size, TTL (Time to Live), ToS (Type of Service), IP Checksum, TCP Sequence Number, TCP Checksum, TCP Flags, ICMP Checksum, UDP Checksum, ICMP Message Type, DNS Query, DNS Query ID, HTTP request URI.					
<b>Bandwidth Management</b>	Guarantee bandwidth per application (granular, per user or session basis). Limit bandwidth per application. Limit P2P protocol traffic per session.					
<b>SSL Attack Prevention</b>	Available for DP-3020, DP-1020 and DP-620 in conjunction with AppXcel.					
<b>IPv6</b>	Support IPv6 networks and block IPv6 attacks.					
<b>Access Control</b>	Access Lists, Black/White Lists					
<b>Alerting</b>	SNMP, Log File, Syslog, E-mail					
<b>Forensics</b>	Attack Packet Logging, In-depth Attack Footprint Analysis, Attack Details and Statistics					
<b>Management</b>	SNMP V1, 2C, 3, HTTP, HTTPS, SSH, Telnet, Console					
<b>Availability</b>	Fail-Open Bypass: Internal for copper ports for all models. External for fiber ports available for DP-3020, DP-1020 and DP-620. Dual Power Ready for DP-3020, DP-1020 and DP-620. Advanced Overload mechanism maintaining maximum security coverage under extreme traffic load.					
<b>Physical</b>						
Dimensions (W x D x H) mm	432x455x88	432x455x88	432x455x88	298x215x44	298x215x44	298x215x44
Weight (lb, kg)	15.4, 7.0	15.4, 7.0	15.4, 7.0	4.785, 2.175	4.785, 2.175	4.785, 2.175
Power Supply	Auto range: 100V-120V/200V-240V AC 50-60Hz or 38-72VDC			Auto range: 100V-120V/200V-240V AC 50-60Hz		
Power Consumption	108W	108W	108W	20W	20W	20W
Heat Dissipation (BTU/h)	368.758	368.758	368.758	68.3	68.3	68.3
Operating Temperature	0-40C					
Humidity (non-condensing)	5% to 95%					
Safety Certifications	EN 60950, UL 1950, CSA 22.2 No. 950			EN 60950, UL 1950, CSA 22.2 No. 950		
EMI	EN 55022, class A, EN 55024, FCC, part 15B, class A			FCC part 15B class A in process		
<b>Warranty</b>	1-year hardware and software maintenance					
<b>Support</b>	Certainty Support Program					

(1) Actual performance figures may change per network configuration, traffic type, etc.

(2) 1,600,000 sessions supported with 1024MB memory. 550,000 sessions supported with 512MB. Specifications subject to change without notice.

(3) Bundled for DP-102, DP-202, DP-502. Optional module for DP-1002, DP-620, DP-1020, DP-3020.

(4) Available with hardware revisions 2.40 or later