

# PRODUCT BRIEF



ATTACK MITIGATOR  
IPS 5500

# Attack Mitigator IPS 5500

## First IPS to Deliver Non-Stop Protection

### Introduction

Today, the vast majority of businesses throughout the world use the Internet in some way to conduct business and many rely on the Internet as a primary source of revenue. Until recently, the only form of effective network security involved using a combination of firewalls and intrusion detection systems ("IDS") as the primary defenses. Today, these technologies are woefully inadequate at combating sophisticated hybrid attacks or devastating brut force attacks that can render an organization helpless and, in many cases, unable to conduct business, resulting in lost profits and customer dissatisfaction. CSO's and CIO's are well aware that the threat landscape has changed significantly in recent years with a growing number cyber crime incidents, ranging from system penetration attempts, insider abuse, spoofing, data sabotage, unauthorized access, Denial of Service (DoS), and the constant onslaught of worm and virus attacks.

In response to this changing threat landscape, Top Layer had developed the Attack Mitigator IPS 5500, the worlds first [Non-Stop Intrusion Prevention System](#) that delivers dynamic, real-time proactive defense for network and application-based attacks. The Attack Mitigator stops intrusions, automatically blocking internal and external cyber threats and other bad traffic before they can degrade and/or damage critical IT infrastructures.

The Attack Mitigator is the only high performance in-line IPS product built from the ground up, designed to tackle the most advanced hybrid attacks and brut force attacks known today and expect in the future. The Attack Mitigator scales to provide non-stop protection in the worlds most advanced networks and has the performance capacity to [protect while under extreme traffic loads](#).

Top Layer's Non-Stop Protection approach to IPS focuses on integrating the best [Protection, Performance, Management and Reliability](#). With those design elements in mind, the Attack Mitigator 5500 was introduced in the summer of 2004 as the most technologically advanced IPS system ever launched. As a testament to the superior in-line protection and performance offered by the Attack Mitigator, over 300 major corporations now use Top Layer's IPS products, many having realized a return on their security investment within days or even hours.

The Attack Mitigator™ IPS 5500 is the worlds only IPS to provide Non-Stop Protection against network and application-based attacks. The Attack Mitigator seamlessly integrates protection, performance, management, and reliability to create the only solution to provide Total Network Integrity by allowing good traffic to reach their destinations when under attack. The powerful integration of these components means that the Attack Mitigator provides the best protection at the highest throughput and lowest latency of any IPS product in the market.

Protecting against today's sophisticated attacks is easy with the Attack Mitigator, which can be deployed and providing full protection within minutes, even in networks that need the high availability ProtectionCluster™ solution that operates at an unprecedented throughput of 8.8Gbps.

## Protection

The Attack Mitigator uniquely protects against undesired access, content-based and rate-based attacks, including malformed packets and well-known exploits like Blaster, SQL Slammer and many others as well as advanced DDoS attacks.

- **Un-Compromised Inspection and Detection** – The latest hybrid attacks and advanced hacker evasion techniques necessitate a highly integrated multi-method approach to accurately detect and block cyber attacks. The Attack Mitigator [inspects 100% of the packets](#) and integrates many protection mechanisms, including its [Deep Packet Inspection and Stateful Analysis Engines](#) to understand application behavior and usage across the entire session.
- **High Detection Accuracy** – Unlike IPS solutions that primarily rely on signatures and are notorious for generating false positives, the Attack Mitigator's [Advanced Protocol Validation Modules](#) eliminate false positives.
- **Protection Against Zero-Day and Unknown Exploits** – The Attack Mitigator's proprietary Advanced Protocol Validation Modules provide leading edge protection against application-level attacks. Current and emerging exploits take advantage of application vulnerabilities. Many of these vulnerabilities are protected by the Advanced Protocol Validation Modules, resulting in the best protection against zero-day exploits. These Advanced Protocol Validation Modules work by inspecting every packet and determining whether the stream of packets that makes up a transaction is compliant with [Permitted Protocol Usage](#) policies.
- **Best In Class DDoS Protection** – DDoS attacks account for the greatest financial losses to businesses worldwide, and no IPS would be complete without comprehensive protection from the most sophisticated and devastating DDoS attacks. The Attack Mitigator, using [patented DDoS protection mechanisms](#), offers the most comprehensive protection from all types of DoS and DDoS attacks. The Attack Mitigator offers the best protection against hybrid attacks where it can even pick out a single intruder while under heavy load, or while exploits are hidden in DDoS traffic.
- **Advanced Stateful Firewall Filters** – Many attackers gain undesired access to critical resources via compromised or non-performing firewalls. The Attack Mitigator has tightly integrated [Advanced Stateful Firewall Filters](#) and always-on Stateful inspection that works with all of its other advanced IPS protection mechanisms. This results in high-performance, comprehensive protection against undesired access to critical resources.
- **Continuously Stateful** – The Attack Mitigator maintains the most context (state) of any IPS device, by an order of magnitude. This is crucial for protection against slow,

### Yankee Group Quote

“Companies in every industry are struggling to cope with the onslaught of IT security issues, from worms to application-level attacks to zero-day exploits,” said Jim Slaby, senior analyst, the Yankee Group. “Top Layer’s Attack Mitigator IPS 5500 delivers protection from all of these threats with the high performance necessary to stop attacks in-line, in real-time -- a critical requirement in today’s security environment.”

but debilitating attacks, ensuring high detection accuracy and avoiding hacker evasion techniques. Continuously Stateful operation is required for protection in dynamic application environments, like VoIP and FTP.

- **TopResponse Service** – Top Layer’s [TopResponse Service](#) draws upon the security expertise of a Vulnerability Research Team, Network Security Research Team, Security Engineering Team and a Technical Research Team. The TopResponse Service is a key element to providing customers with [immediate protection against newly discovered vulnerabilities](#). In addition, Top Layer has relationships with a number of partners who see new attack types before they become widespread, allowing the TopResponse team to provide better protection, earlier.

## Performance

Performance is critical for an in-line IPS. The key performance aspects for an in-line IPS are latency, throughput, DDoS rejection rates, operation under load, and scalability. The Attack Mitigator delivers industry-leading performance across all the key attributes and in many cases; the Attack Mitigator operates at 3 – 5 times the performance levels offered by competitive products.

- **Lowest Latency Of Any IPS Device** – The Attack Mitigator is the first IPS to seamlessly integrate multiple protection mechanisms on a distributed ASIC platform. The result, [latency measuring below 50 microseconds](#) when protection mechanisms are enabled.
- **Scaleable Performance and Capacity** – The Attack Mitigator [ProtectionCluster™](#) provides the highest level of performance by using unique load sharing mechanisms. The [ProtectionCluster™](#) provides a scaleable solution that not only increases capacity, but also provides better protection through advanced state sharing and awareness.
- **Outstanding Throughput** - It is very difficult for any security administrator to be able to characterize the traffic on their network with a high degree of accuracy. What is the average bandwidth? What are the peaks? Is the traffic mainly one protocol or a mix? What is the average packet size and level of new connections established every second? The Attack Mitigator has been designed to eliminate these concerns by being able to operate in the most demanding networks with [throughput of 8.8 Gbps](#) with the [ProtectionCluster](#).
- **Industry Leading DDoS Rejection Rates** – Today, DDoS attacks can be launched simultaneously from computer armies of 35,000 compromised machines, delivering seemingly harmless legitimate traffic at rates approximating a gigabit per second. Today, attackers target e-commerce site, email servers, DNS servers and VoIP providers prevent legitimate transactions or data from reaching the desired target.

### Gartner Reference

“Effective network intrusion prevention must be inline, perform at the rated throughput without packet loss, and have acceptable performance even when handling a variety of packet sizes,” said Greg Young, a research director with Gartner. “Performance with minimal latency, the backing of good research and updates, a clear configuration and management interface, and predictable behavior under load are some of the essential elements of IPS.”

Only the most advanced DDoS capabilities, designed in hardware, can stop these attacks while allowing legitimate traffic to continue to flow to the intended destination. Top Layer has been at the leading edge of stopping high volume DDoS attacks for many years. The Attack Mitigator incorporates this technology in all of its IPS products and allows customers to combine traditional IPS protection features with full DDoS protection.

- **Performance When Under Load** – This is the one performance metric missing from most vendors datasheets. As a result of the tight integration of the protection mechanisms with the hardware architecture, datasheet performance for the Attack Mitigator is what you can expect when deployed in live networks (with small packets), even when under attack.

## Management, Ease of Use and Deployment

The Attack Mitigator can be set up in minutes with carefully designed out-of-the-box configurations that provide immediate protection as well as offering meaningful and actionable reporting.

- **Out-Of-The-Box Protection** – Deployment of the Attack Mitigator typically requires no changes to network topology and can be installed in minutes. Once installed, users can select from several predefined Protection Configurations with one click of a button. Unlike competitive products that claim to have broad protection capabilities, but only enable a small sub-set for fear of generating false positives, the Attack Mitigator can be set to [block all attacks in minutes](#) because of its more intelligent protection mechanisms.
- **Flexible Management** – The Attack Mitigator is the only network IPS that allows users to [configure protection profiles for up to 64 independent departments or assets](#). Each department or asset can have unique protection policies and security reports providing users with meaningful protection and information.
- **Provisioning, Reporting and Correlation** – Using Top Layer's *SecureCommand+*™ Centralized Threat Management System, employing our unique [Rapid Threat Recognition and Response Engine](#), users can react immediately to distributed and dynamic security threats with the industries' first integrated Centralized Management and Security Event Correlation solution.

## Reliability, Availability and Resilience

- **Reliability and Availability** – The Attack Mitigator can easily be deployed and managed in a [High Availability Configuration](#) (Active/Active or Active/Passive) that provides continued protection in the event of a system failure or power loss. In addition, the Attack Mitigator's can be deployed to handle asymmetric traffic without any degradation in performance or required changes to the routing infrastructure.

- **Resilience** – The Attack Mitigator has been built with long life in mind. There are no rotating storage media, no chip-mounted cooling fans; it has redundant hot-swappable power supplies and fan tray assemblies. Because of these design innovations, the Attack Mitigator will continue to provide protection for many years.

## **Immediate Return on Investment**

**Top Layer has received numerous testimonials from customers stating that an immediate benefit of the Attack Mitigator is to reclaim network bandwidth from malicious and unwanted traffic as well as offloading critical infrastructure such as switches and routers. In addition, security and network administrators have been able to free up their time from emergency and ad-hoc responses to repair damaged resources resulting from cyber attacks.**

**The Attack Mitigator offers a compelling return on investment.**

## **Protection**

Top Layer's Attack Mitigator IPS 5500 product line provides dynamic, real-time, proactive defense against network and application-based attacks. Today's attacks are more sophisticated than ever before and defending against them requires invoking multiple protection mechanisms. The Attack Mitigator is the only IPS to seamlessly integrate all of these protection mechanisms in hardware, which means that no matter how an attack payload is delivered, it will be stopped every time with minimal performance impact.

The Attack Mitigator provides Total Network Integrity using six separate, real-time protection mechanisms to detect and block threats dynamically; Protocol Validation Filters, Attack Signatures, Advanced Firewall Filters, Intelligent Rate-Based Filters, Packet Filters, and Patented DDoS Algorithms. In addition, the Attack Mitigator is ready to accept a plug-in module that incorporates best of breed third party security applications for anti-virus, anti-spam and content filtering, to name a few.

**Protocol Validation** Filters offer superior protection as the primary line of defense against application attacks. Most application attacks, by their very nature, contain malicious code that would cause the attack packet stream to violate acceptable protocol usage. Simply put, since it is clearly known whether or not a packet stream is compliant with acceptable protocol usage, any data stream that violates that acceptable usage is deemed malicious and consequently blocked.

Example: Blaster and Lovsan were caused by sending a malformed DCOM activation packet with a very large "servername" entry in the UNC path parameter of a remote request over the Microsoft RPC protocol. An attack signature might work for known variants, but small changes to the attack would pass through the IPS and infect the network and assets. By using the Attack Mitigator's Protocol Validation Filters, all variants of the exploit were stopped because the packets were identified as not conforming to an acceptable protocol use.

The proprietary Protocol Validation Filters operate by invoking several simultaneous detection mechanisms that detect whether a packet stream is allowed to pass through or not. Together, these mechanisms provide the most comprehensive IPS protection while at the same time eliminating false positives, the bane of the network administrator.

- **Fragment Reorder Engine** – Dedicated ASIC to receive and reorder packets that make up an entire session which are then forwarded to the Deep Packet Inspection Engine where key checks are performed. This engine avoids common hacker evasion techniques and improves IPS performance and downstream network operation.
- **Deep Packet Inspection Engine** - Dedicated FPGA that performs checks against acceptable protocol use. If the entire transmission violates acceptable use, the transmission is blocked, reported on and sent to a discard port for forensics.
- **Session Aware Application Inspection Engine** – To prevent attackers from using evasion techniques such as slow attacks, the Session Aware Application Inspection Engine maintains real-time intelligence on over two million IP addresses. If malicious transmissions from any of these IP addresses are seen, any future traffic originating from them will automatically be closely scrutinized.
- **Security Profiles** – Security policies developed for application and network behavior that define expected and compliant operation. These profiles are developed via a white-list approach – defining what is “good” and stopping everything else. This protects critical resources from design vulnerabilities and implementation vulnerabilities.

Because the Protocol Validation Filters do not match signatures against specific exploits, they effectively act as a virtual software patch for unprotected vulnerabilities, including those susceptible to buffer overflow attacks. This is important in the context that we continue to see a narrowing of the time between discovering a vulnerability and the time an exploit is launched, making Zero-Day Attacks more of a reality. IPS products that do not perform deep packet inspection on entire sessions (with the packets reordered to their original form) cannot provide adequate protection from the complex hybrid attacks now commonly seen. The Attack Mitigator is able to effectively detect and block attacks that are received in fragmented form, even in asymmetric networks.

Protocol Validation Filters only block packet streams that breach acceptable application protocol usage rules, good traffic is never blocked, a key differentiator to those IPS solutions that use attack signatures as a first line of defense.

[Attack Signatures](#) are used to protect against known exploits where the exploit is not recognized by the Protocol Validation Filters. This protection mechanism is a secondary line of defense compared to the Protocol Validation Filters. Within hours of a new vulnerability or exploit being published, Top Layer's TopResponse Service provides users with an attack signature. Where practical, the vulnerability protection will be added to the Protocol Validation Filters within days of the attack signature being issued. This will better protect against new variants of the same exploit and provide IT administrators the necessary time to carefully patch vulnerable servers.

[Advanced Stateful Firewall Filters](#) block traffic based on origination, destination and transport content. The filters look at all communication layers and extract only the relevant data, enabling highly efficient operation.

[Intelligent Rate-Based Filters](#) allow for connection and application rate limiting, which in conjunction with [Patented DDoS Algorithms](#), provide industry leading DDoS protection capabilities. The two million IP address table that is used to keep state on IP address behavior is expanded to five million when the Attack Mitigator is defending against a DDoS attack. During an attack, the Attack Mitigator will continue to pass good traffic with no discernable change in performance or latency.

[Packet Filters](#) examine IP headers for IP traffic and the payload for ARP packets to ensure no malformed or incorrect protocol traffic pass through the Attack Mitigator.

### **Non-Stop Protection In The Real World**

**To operate effectively in the real-world, the Attack Mitigator performs all protection mechanisms at gigabit speeds without dropping good packets and without the need to continuously configure the device. To do that effectively, the Attack Mitigator integrates protection with performance.**

## **Performance**

There are numerous ways to measure performance in the context of an IPS device, but the true measure is how the device works in a real world environment. An IPS must allow all good traffic to pass through, while blocking all bad traffic at peak loads. The core technology behind the Attack Mitigator is built upon a distributed, purpose-built ASIC and FPGA architecture to provide the maximum performance with a high degree of flexibility. The ASICs are interconnected with high-speed buses, creating a network device with extremely low latency, high throughput and no data path bottlenecks that you would expect to find with PC-based or hybrid solutions. Five of the ASICs have a RISC core imbedded in them to allow functions to be changed by firmware update without compromising performance. The FPGAs allow complex functions to be programmed into the hardware architecture rather than relying on software add-on that would dramatically reduce performance.

**Content-based performance** for traditional IPS functions (Protocol Validation Filters, Attack Signatures and Advanced Firewall Filters) can process up to 3.6 million packets per second and can set-up and tear down 90,000 connections per second, both of which are an order of magnitude higher than any other IPS product.

**Rate-based performance** for DDoS protection is rated at a full gigabit of DDoS traffic while allowing legitimate transactions to flow uninterrupted. The high performance is achieved by automatically expanding the IP address table size during an attack from two

million to five million. Since the state is maintained in hardware, the expansion of the table provides greater capacity without any reduction in performance.

**Latency** for the device is measured in microseconds with all protection mechanisms enabled and while under load. This level of latency can only be achieved by tightly integrating protection with performance under real-world conditions, a unique differentiator for the Attack Mitigator.

### Non-Stop Protection

**An IPS device that misses attacks under load or adversely effects legitimate traffic for any reason is unacceptable. The Attack Mitigator IPS 5500 was built to provide protection at the highest levels of performance.**

### Next Steps

To find out more about how the Attack Mitigator IPS 5500 can help protect your network, call Top Layer at 1 508-870-1300, email [info@TopLayer.com](mailto:info@TopLayer.com) or locate your local sales office at [http://www.toplayer.com/content/contact\\_us/offices/index.jsp](http://www.toplayer.com/content/contact_us/offices/index.jsp)



Double NSS Approved

Top Layer Networks, 2400 Computer Drive, Westboro, MA 01581

Phone: 508-870-1300, Fax: 508-870-9797, [www.TopLayer.com](http://www.TopLayer.com)