Managed Intrusion, Detection, & Prevention Services (MIDPS)

Why E-mail Sorting Solutions?

Why ProtectPoint?

PROTECTPOINT
Network Security

Why?

Focused on Managed Intrusion Security

Superior-Architected Hardened Technology

Security Operation Center

Carrier-class support call center facilities with power and back-up power supplies with 24/7/365 availability.

24/7/365 Reporting Portal: RADAR

AASP MIDPS provides secure Web access to real-time security reports and research tools. Enables enterprises to efficiently analyze their security stance, manage compliance requirements and enforce their network security policy.

Harware and Software Included

AASP MIDPS managed services **includes** the hardware and software updates necessary to vigilantly defend our your networks.

Supported by Intrusion Analysts

Experienced intrusion analysts monitor all network traffic inbound, internal and outbound for unauthorized usage or malicious threats. As data packets are humanly identified as a threat, notifications are immediately made by phone, the connection is blocked, and the analyst remains with the network administrator until the threat is completely diffused.

Focused on Intrusion Security Software since 1998

Why?

Own Well-Architected Intrusion Technologies

- Major Component to PCI Requirements
- SAS 70 Certified designed to enforce compliance and regulations
- Flexible to adapt to a multitudes of network environments
- Mature Service Technology
- Industry-acclaimed
- **> 9 years >100's of Clients**
- **Millions of Packets Scanned Daily**
- **Multiple awards for performance and value**

Technology Protection and Support:
ProtectPoint managed services include the hardware and software updates necessary to vigilantly defend our customer's networks. Customers receive unlimited access to technical support from the Security Operation Center by phone, email or through the RADAR portal. ProtectPoint operations adhere to internationally recognized SAS 70 Type II auditing standards. SAS 70 Type II auditing standard validate that a service organization has completed an in-depth audit and testing of their control activities, which include controls over information technology processes.

The Included Network Security Appliance provides a fully integrated suite of security services, consisting of hardware, software, consulting, monitoring, and management tools to actively assess and defend an organization's Internet network vulnerabilities and exposures. Our internal systems automate many of the labor-intensive tasks involved with monitoring various system logs used to detect anomalies and attacks. Customers have the flexibility to create and implement with our analysts an easy-to-use, yet uniquely tailored set of security policies, regardless of dedicated access speeds, network size, or types of Internet applications.

PROTECTPOINT
Network Security

Together… Focused on Intrusion Threats Beyond the Firewall

Network Intrusion Detection & Prevention monitors network traffic to identify malicious activity, resource misuse, attempts to gain unauthorized access and network attacks. Intrusion Detection & Prevention service supplements your firewall by providing deep analysis of the traffic legitimately permitted through open ports which is essential in recognizing and responding to network attacks. ProtectPoint provides vigilant 24/7/365 real-time monitoring, detection, analysis and response to internal and external network security threats. This active approach permits us to identify security events before systems are compromised, eliminating time-consuming and costly security incidents.

Full-time security experts manage your network 24/7, 365 days a year, include the hardware and software as part of the service, and prevents expensive security incidents by catching them and diffusing them at the same time.

Live Monitoring Defenses:

1. Hacking Attempts
2. Reconnaissance / Scans
3. Web Attacks
4. Vulnerability Exploits
5. Unauthorized Access Attempts
6. Ddos Attacks
7. Worms / Viruses / Trojans / Keyloggers
8. Spyware / Botnets / Malware

PROTECTPOINT Network Security

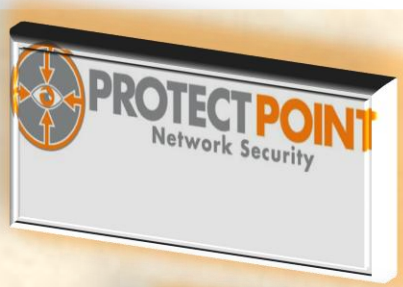
Why?

Focused on Managing Data Security since 2003

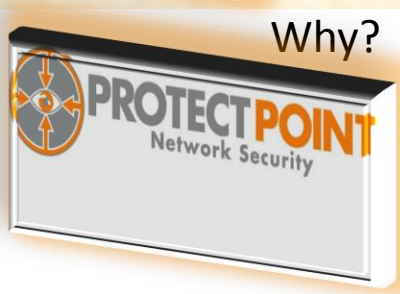
Over the years, we've answered the requests of our end user focus groups and our channel partners by **PROVIDING**:

•No risk, guaranteed service, cancelable at will.
•No set up fees, maintenance fees or upgrade fees.
•No hardware or software purchases or licenses needed, no changes to legacy systems.
•No-long term contracts, just month to month actual billing.
•Private Labeling – Create market confidence with your **own brand name** premium MIDPS services, instill assurances backing ***your*** service with the ProtectPoint name offer seamless and quickly noticed upgrades – whether converting from current internal services or outsourced.
•The ability to **create your own channel partners** and re-label again to as many selling partners as the market will bear within street pricing limits.
• Virtual ownership of our World-class Security Operations Center, use our centers to guarantee phone support when an intrusion is detected.
•Volume license sharing in the World-renowned, award winning ProtectPoint MIDPS through us, with exceptional performance and price.
•Web based management center for Administrators.
•Free 30-day trial period for qualified enterprises.

1-866-660-4292



Why?



Focused on Intrusion Technology since 1998

MIDPS TECHNOLOGY

Our AASP MIDPS through **ProtectPoint** is non-intrusive to your network and includes the ability to detect and block more than 2600 vulnerabilities and attack signatures and is automatically updated as new vulnerabilities are discovered.

Other specific details of the MIDPS include: We **Detect, Alert and Block** for security threats including buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners, backdoors, Trojans, and operating system and application system vulnerabilities, DdoS clients, and many more.

Signatures are rapidly developed and deployed by our security analysts to ensure you are protected from the latest threats.

We record packets in their human-readable form from the offending IP address in a hierarchical directory structure and store this information our encrypted security server for future analysis or prosecution.

Can be deployed in stealth mode as a "passive trap" to record and report on the presence of unauthorized traffic that should not be found on a network, such as NFS or Napster connections. **MIDPS** detects incidents originating from inside and outside the network perimeter.

Anomalous Traffic Pattern Detection: If a host on your network exceeds average usage patterns, a security ticket will be created and the traffic will be investigated.

AASP MIDPS responsible for detecting anomalous, inappropriate, or other data that may be considered unauthorized on a network. A regular firewall is configured to allow or deny access to a particular service or host based on a set of rules. If the traffic matches an acceptable pattern, it is permitted regardless of what the packet contains. However, the **AASP MIDPS** enables our Security Operations Center (SOC) to capture and inspect all traffic, regardless of whether it's permitted or not. Based on the contents, at either the IP or application level, an alert is generated.

PROTECT POINT
Network Security

Why?

Focused on Working with your Technology

How does MIDPS work?

Beginning with a complete network consultation process, all access to your network is identified for intrusion vulnerabilities then targeted for protections.

How we make it work…

• We perform a penetration study, on your network under your supervision, to find all weaknesses and access points requiring traffic analysis.

•We establish sensor placement needs based on the penetration study (appliance placements).

• When appliances are networked, we work with you to identify inbound, internal and outbound network traffic patterns and packet content.

When all is in place, our analysts go to work to identify malicious activity, resource misuse, attempts to gain unauthorized access and network attacks. Intrusion Detection & Prevention service supplements your firewall by providing deep analysis of the traffic legitimately permitted through open ports which is essential in recognizing and responding to network attacks. AASP MIDPS provides vigilant 24/7/365 real-time monitoring, detection, analysis and response to internal and external network security threats. This active approach permits us to identify security events before systems are compromised, eliminating time-consuming and costly security incidents.

Provisioning:

1. **Identify Incident Handling Procedures, Contacts,** assign administrator(s), establish web access credentials
2. **Appliance Installation,** setting up hardware with embedded software post firewall on your network with a hardened technology.

Why?

Focused on Effortless Administration
"Set it and forget it?" Not with MIDPS

Intrusion Detection Systems generate high volumes of alerts that must be analyzed to determine the nature of the event and appropriate action to be taken. This requires dedicated resources with the technical skill set to understand the situation and necessary response. Not to mention the burden of constantly evaluating and distributing signature updates to ensure protection from the latest threats. AASP supplements your staff by offloading these tedious tasks involving them with only high-level incidents that require immediate attention. Escalation and response is tailored to fit your corporate security policies, allowing your staff to focus on internal security policies, procedures and daily business activities.

Instantly Implement Best Practices: Security experts leverage industry best practices and our own proprietary methodologies to identify real security events before systems are compromised, eliminating time-consuming and costly security incidents. We watch every security mailing list, CERT advisory; FBI Bulletin and we work very closely with the Honeynet Project to ensure that your network is protected from every new security threat. Use our secure Browser based reporting tool to see how we are defending your network at your convenience.

Dedicated and Credentialed Security Professionals: Implementation and management of security systems is a distinct and mature discipline, requiring skills separate than those required to install and maintain PC's and networks. Having an extensive team of dedicated security professionals whose sole responsibility is to be aware of and respond to the latest security threats is likely to be more competent than professionals who only deals with security on a part-time basis. We manage thousands of networks so we see hundreds or thousands of potentially destructive attacks every day providing us with tremendous insight on on-going security issues.

Guaranteed Responsiveness: Once a security event is detected, escalation begins within seconds to identify the source of the problem and block it before it affects your operations. Aggressive Service Level Agreements (SLAs) ensures that you will be notified immediately with the appropriate amount of information.