



Sentinel IPS™ with Network Cloaking™

What it is:

An easy to install and manage 'Intrusion Prevention System' that protects all 'open ports' on your internet connection. An "in-line" gateway that stops malicious traffic from reaching your private network.

What it does:

Inspects, detects and drops malicious packets so fast that the destination IP address appears unused to the offender. Each packet is inspected, correlated, the event logged, a copy of the packet recorded for administrative use, the network admin is alerted, the packet is dropped and a new rule is written preventing the source IP from communicating with a Sentinel IPS™ Protected Network before the packet can leave the Sentinel Appliance. This is accomplished so quickly as to be imperceptible to the users of the network.

Where it fits:

Installs between the internet router and the firewall, outside of your protected network. Requires no network modifications or changes to firewall settings.

Network Cloaking™ "You can't hack what you can't see".

An EcoNet.com proprietary Patent Pending technology that results in Sentinel Protected Networks being invisible to the malicious user while maintaining the utility of the network for valid users. Sentinel IPS™ protected networks cannot be scanned, port scanned, stealth port scanned or penetration tested with standard tools while maintaining the full utility of the network for all other uses. The act of looking for Sentinel IPS™ protected network becomes the reason for a malicious user's inability to find it.

The System Includes:

SWS - Sentinel Warning System

All Sentinels participate in the SWS. Sentinel IPS™ has an absolute and unique ability to determine malicious source IP addresses, even if no correlation information is available. Such source IP's are reported through the SWS, for use in early threat detection, investigations, and new prevention strategies.

Sentinel IPS™ Alerts

Alerts via email or small text messaging contain type of attack, time stamp, malicious source IP, destination IP and reference links for more information about the type of attack.

Sentinel IPS™ Administration

Logon from any web browser on the protected network and control the alerts list, white-list, user/password administration, and view reports. Sentinel IPS "Looking Glass" enables viewing of malicious packet activity dynamically, while it is passing through the gateway.

Sentinel IPS™ Reporting

Blocked IP address reporting includes a time stamp of the last packet from the malicious IP.

Network Gateway Assessment reporting for threat analysis and remediation.

Compliance reporting for organizations that fall under GLB, SO, and HIPAA requirements.

Forensics reporting including packet payload capture and time stamping for attack analysis.

Compatible with most security events management systems.

Sentinel IPS™ Service

The Sentinel IPS™ is a 'Managed Service' security appliance' and includes the hardware, custom configuration for integration to your network, 24/7 monitoring and automated updates, maintenance, and backups. Also including are OS upgrades, application updates, version upgrades, attack database updates, and support.

Availability: Sentinel IPS™ products are available Integrated Platforms, Inc.; Houston, TX.