

Product Datasheet

Sentinel EPS: Extrusion Protection Sensor

Designed to supplement our Intrusion Prevention Systems (Sentinel IPS), the Sentinel EPS keeps an eye on your network's internal infrastructure. The Sentinel EPS records malicious traffic originating from your network, giving you the power to identify potentially compromised machines on your LAN.

Product Features

Identifies specific machines on your LAN that may be compromised by trojans, botnets, and other forms of malware.

Easy to use browser-based administration with many configuration options and reporting tools, including current EPS activity, activity summaries, packet detail, and many more.

Reporting tools are a great aid for compliance-related documentation.

An appliance and security management service. Includes 24/7 monitoring, remote management services, update services, upgrades and enhancements.

Monthly fee structure substantially reduces capital expenditure and frees up time and money for other initiatives.

Additional Services

Sentinel EPS is offered as a supplement to our IPS services. In addition, we offer Network Gateway and Vulnerability Assessments, presentation opportunities, and ad-hoc security consulting.

Want to learn more? Don't hesitate to ask us at (972) 991-5005.

What is 'EPS'?

EPS is our Extrusion Protection Sensor. It runs on your LAN, and analyzes traffic originating from your network. If it identifies malicious traffic, it records the offending internal IP address and the type of attack. It does not, however, block the traffic. That's the job of your Sentinel IPS.

Product Options

There are three hardware options, and each receives the same level of personal, professional service and support:

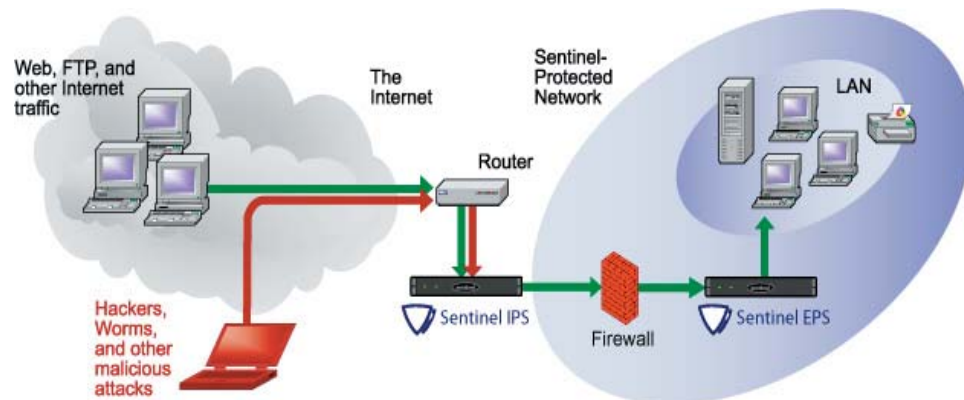
Premium Our standard, rock-solid 1U rackmount unit with gigabit NICs

Advanced Adds bypass functionality, fail-open NICs, and beefier hardware

Ultra Adds enterprise-level performance in the same 1U form factor

What does a typical installation look like?

The Sentinel EPS is installed as a Layer 2 Bridge, behind your network's firewall, and in front of your LAN. The EPS unit is typically given an internal IP address, and its web interface is accessible on that IP via https.



Would you like to know if one of your network's computers is infected with the latest malware or botnet?

Sentinel EPS can tell you which computers are infected, and what they are infected with, in real-time. Combined with Sentinel IPS and your existing anti-virus software, Sentinel EPS is another way Econet.com helps you keep your network safe.