

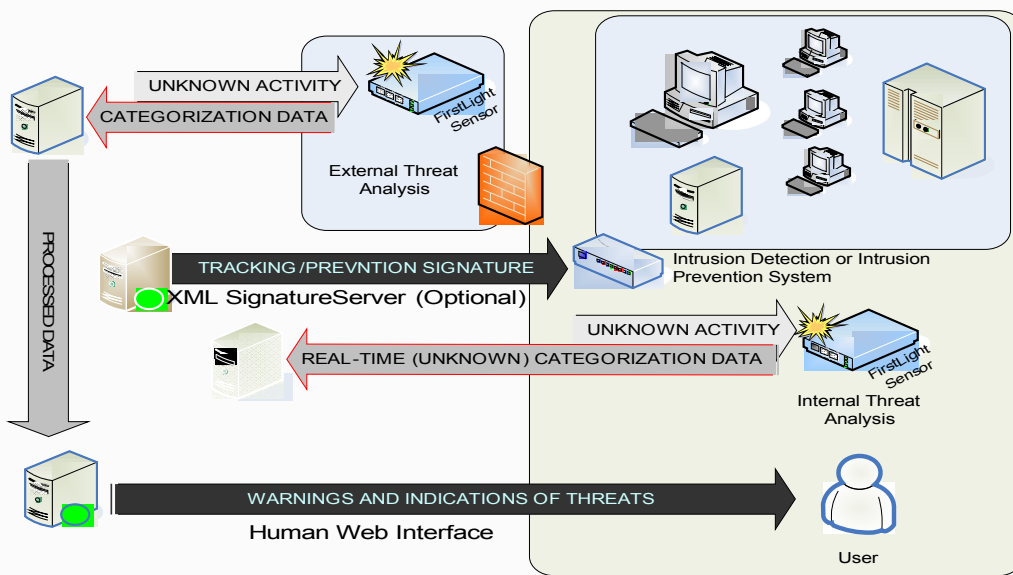
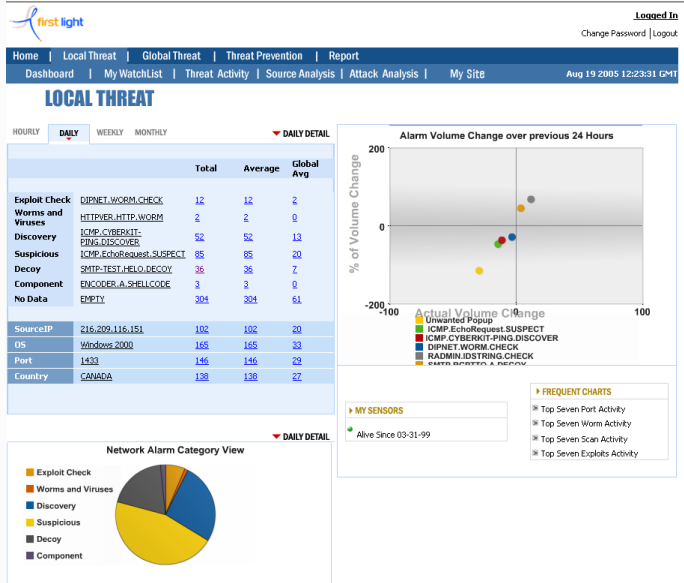
FIRSTLIGHT Early Warning System

Bring you real-time intelligence for attack prevention

To ensure a strong security posture for your network, FIRSTLIGHT Early Warning System delivers early notification of active attacks and potential threats and vulnerabilities of your local network and compares it to global threat and vulnerabilities. The Early Warning System adopts a revolutionary approach to network security focusing on what you don't know. It is the only product designed to look out from your network, unlike firewalls and prevention systems that look in to your network. Consequently, new attacks and variations on attacks come sharply into focus so you can stop them before they enter your network. By leveraging FIRSTLIGHT proactive threat and intelligence, companies can deploy specific counter measurement to prevent the threats from impacting their business.

Key Advantages

- ❖ A managed service requires no configuration. Just plug it in and login to a secure web portal to see your data.
- ❖ Spots spikes in malicious traffic on busy ports, even with port overload, to improve network vision.
- ❖ Advanced data correlation simplifies incident investigation and focuses response.
- ❖ Localized early warning: For timely, proactive notification of potential threats, FIRSTLIGHT Early Warning System tracks global security events and your local security events, providing localized early warning of active attacks as they develop, on a real-time basis.



Correlated Attacks brings focus to incident response

FIRSTLIGHT Early Warning System collects data, processes *unknown traffic*, and generates alerts and ML Prevention Signatures to keep attacks out of your network.

FIRSTLIGHT Early Warning Features At Glance

| Features | Benefits |
|--|---|
| Dedicated Threat Appliance Monitors Live Traffic | Attacks are isolated at the application layer and the payload/stream is fingerprinted. This enables you to stop the attack regardless of its source IP address. |
| High Speed Pattern Matching Algorithms | Complex anomaly content is "learned" the first time and reduced to simple pattern matches. Future attacks are quickly prevented without having to verify the anomaly. |
| Advanced Data Correlation | Categorize all attacks into severity groups so that you can focus on dangerous botnets and scripted attacks. |
| Open Architecture/Vendor Compatible | Easy integration with existing SIM, trouble ticket management framework and ability to enhance third-party firewall and IPS products with XML prevention signature updates. |
| Secure Web Interface | Live security overview, status, analysis and reporting are all delivered via secure Web portal or Web Services; reduces cost of staff to manage and interpret events. |
| Community Infrastructure | Compare your local office attack profile to your industry group profile and share XML signatures that are created from attack data to reduce exposure to attacks. |
| Holistic Network View | See all attacks against your network. Enables you to fingerprint the attack infection as well as the propagation of the worm, botnet, etc. |
| Real Time Technical & Compliance Reporting | FIRSTLIGHT Dashboard XML pages automatically refresh and template reports can be generated on a regular basis. |
| Rapid Signature Downloads | FIRSTLIGHT can allow new signatures to auto-download and update with approval. |
| Incident Response Capable | FIRSTLIGHT offers signatures for new attacks that can be run in multiple vendor firewall and prevention products. |

System Requirement:

- FIRSTLIGHT Threat Sensor may be purchased as a complete hardware and software Appliance, or you may purchase hardware separately. Customer sourced hardware and software information:
- Threat Sensor Hardware Spec: Intel compatible motherboard; Pentium 2.4 GH; 512 MB RAM; 1 NIC; 40 GB HD.
- Threat Sensor Software: Linux Fedora Core 3.0, English Installation; No services running except SSH
- User interface: Microsoft internet Explorer, Mozilla Firefox

Endeavor Security, Inc.

Endeavor Security is a software development company focused on solving operational security issues. Its technology suite includes a real-time Early Warning System, Auto-Signature Generation, and Intrusion Prevention Software, which offer solutions to everyday obstacles in managing a secure information infrastructure.

1420 Spring Hill Road, Suite 600
 Mclean, VA 22102
 phone: +1.703.286.5820
 fax: +1.703.738.4530
www.endeavorsecurity.com