

>>> Espion EX3000 and SP5000 Network Disaster Protection Appliances



- > Generate fine-grained signatures in seconds, even for zero-day attacks – without relying on out-of-date signature databases
- > Neural network technologies rapidly detect the emergence of previously unseen and unknown threats.
- > Packet-based analysis eliminates reliance on and weaknesses of flow-based systems.
- > Real-time analysis at gigabit speeds.

> ABOUT ESPHION

Esphion protects enterprises, service providers and Governments from network disaster. Esphion's breakthrough technology uses neural, behavior-based, real-time analysis to detect known and unknown threats within seconds. It then generates fine-grained signatures, allowing you to stop even the most aggressive attacks and eliminate internal network threats and insider misuse. Launched in 2002 by industry veterans, Esphion is backed by leading venture capital firms. Its customers include Fortune 100 enterprises and major service providers and financial institutions. For more information visit www.esphion.com

Introduction

Designed to protect the world's most demanding service provider and enterprise networks from disaster, Esphion EX3000 and SP5000 appliances detect, in real-time, network anomalies such as denial of service attacks (DDoS), worm outbreaks, and other threats, even if previously unseen and unknown.

Neural network and behavior-based, real-time analysis provides a comprehensive view of network security through a user-friendly, web-based GUI. By continually profiling the behavior of network traffic, normal behavior is learnt. Anomalies that have the ability to impact network availability or performance are instantly recognized.

Without relying on signature databases or complex rule-sets, zero-hour events can be detected in just seconds, and through a patent-pending analysis process signatures for those events can be extracted in seconds. These signatures can then be applied to already existing network infrastructure elements, such as routers, firewalls or intrusion prevention systems, in order to surgically remove the offending traffic, while allowing legitimate traffic to continue to flow.

Esphion is used by leading enterprises and service providers to detect and eliminate:

- > New, unseen and unknown threats such as worms or DDoS attacks that routinely result in network disasters.
- > Inappropriate internal activity such as insider attacks.
- > Violations of internal policies, such as excessive peer-to-peer usage, that expose enterprises to legal risk and waste internal resources.
- > Network mis-configurations, which result in performance impacting network traffic anomalies.

A World-class Security Architecture

Esphion EX and SP appliances are designed to complement existing security elements, introducing a first and final line of defence.

As a complementary security layer providing a critical new view and real-time signatures, Esphion extends the life-span of already existing security and infrastructure investments, thereby not only improving uptime, availability and security, but also the ROI of those investments.

Esphion can be deployed as either stand-alone or distributed solution at the network core or at access switches or routers, depending upon the outcomes needed.

Solutions for Enterprises:

- > Stand-alone systems: Esphion EX3000 incorporating the Esphion controller and the intelligent neural agent in a single, industry-standard system
- > Distributed Systems: Esphion EX3000c controller and a number of Esphion EX3000i intelligent neural agents

Solutions for Service Providers:

- > Stand-alone systems: Esphion SP5000 incorporating the Esphion controller and the intelligent neural agent in a single, industry-standard system
- > Distributed Systems: Esphion SP5000c controller and a number of Esphion SP5000i intelligent neural agents

Intelligent neural agents are deployed at key intelligence gathering points within the network including access links, in or before mission critical subnets in the network. Multiple intelligent neural agents are aggregated by a single controller, which provides a unified reporting infrastructure and multi-user, secure GUI.

Esphion is deployed either via network taps or via spanning ports transparently on the network – avoiding any latency or points of failure while remaining safe from attack.

Fine grained analysis of each IP packet and traffic patterns are conducted in real time up to gigabit speeds. Storage and recording features allow forensic examination of historical traffic and anomaly data.

New Breakthroughs In Network Disaster Protection

Espion's EX3000 and SP5000 family of appliances introduce a specialized module for the rapid detection of 'swarms'. Swarms are detected anomalies in host behavior, such as self-propagating worms. Using a combination of sophisticated behavioral anomaly detection algorithms, Espion can now identify even slow-scanning worms in just seconds, providing network administrators with the crucial early warning, which allows the successful prevention of a worm outbreak.

Espion is now ideally equipped for deployment not only on the network's perimeter, but also inside the network. There it can detect and analyze anomalies that emerge from within the organization such as an infected mobile device.

New Features:

- > Detect swarms. New specialized module for the rapid detection and prevention of traffic 'swarms'.
- > More network defense. Now deploy Espion alliances anywhere inside or outside the network - outside of your firewalls to detect DDoS attacks or inside your network to detect worm outbreaks.
- > Highly sensitive detection algorithms. Now detect even slow-scanning worms which scan at less than one packet per second.
- > Support larger groups and develop new services. Define up to 200 customer groups per controller. Managed service providers (MSPs) can use Espion's user portal to allow individual users access to information and alerts about their network traffic. Because individual intelligent neural network agents can now handle separate group sets, it is possible to take multiple Espion Ex3000i or SP5000i appliances and position them around the perimeter as well as inside of the network, and still manage them all from a single controller.
- > Support for detailed, real-time Crystal reporting. Gain insight as to the port and protocol, as well as the IP addresses (hosts) that are involved in a

swarm and normal types of network anomalies.

- > Real-time traffic sampling and reporting. Specify an analysis of all traffic to/from a certain port, as it takes place. Or, to/from a certain IP address. Detailed reports contain information such as the packet size histogram, top peer ports and top peer IP addresses.
- > Improved usability. New graphing and reporting capabilities via Espion's web-based GUI. Key windows and graphs continuously show up-to-date information, making Espion well suited for 'mission control' style monitor screens. Notification filters can have the number of involved hosts as a criteria, enabling customers to be alerted to activities that involve more than just one host.
- > Greater resiliency. Data is buffered on the intelligent neural network agents in case of a lost network connection to the controller. Once the connection has been restored, the data is transmitted.

Measuring Return On Investment in Days

With Espion, a service provider or enterprise can expect rapid payback on the investment in terms of greater uptime, better network performance, reduced outages or slowdowns, and fewer sleepless nights. The return on investment can often be measured in days through reduced:

- > Downtime and business disruption,
- > Security staffing and overtime costs,
- > Intrusions, thereby improving network integrity and lowering additional network investment requirements,
- > Costs related to security policy enforcement and management,
- > Contingency costs for dealing with a major security attack,
- > Compliance costs associated with meeting regulatory requirements in different markets and industries,
- > Bandwidth requirements due to the identification of malicious network behavior, and a reduced requirement for additional bandwidth or disaster recovery systems.

Learn today how Espion can reduce your IT costs and prevent network disasters.



www.espion.com

sales@espion.com

**Espion Corporate
Headquarters
20 William Pickering
Drive, Albany
Auckland
New Zealand
Ph: +64 9 414 2060
Fx: +64 9 415 0228**

**Espion Australia
Level 6. 90 Mount Street
North Sydney
NSW 2165
Australia
Ph: +61 2 9955 3611
Fx: +61 2 9959 5760**

© 2000-2005 Espion Ltd. All rights reserved.

Espion and netDeFlect are registered trademarks and the Espion logo is a trademark of Espion Ltd.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Espion and its licensors. If any, third-party software, including font technology, is copyrighted and licensed from Espion suppliers.

This document was developed on the basis of information and sources believed to be reliable. This document is to be used "as is." Espion Ltd. makes no guarantees or representations regarding, and shall have no liability for the accuracy of, data, subject matter, quality, or timeliness of the content. The data contained in this document are subject to change. Espion accepts no responsibility to inform the reader of changes in the data. In addition, Espion may change its view of the products, services, analysis and companies described in this document. Espion accepts no responsibility for decisions made on the basis of information contained herein, nor from the reader's attempts to duplicate performance results or other outcomes. Nor can the paper be used to predict future values or performance levels. This document may not be used to create an endorsement for products and services discussed in the paper or for other products, analysis and services offered by the vendors discussed.