

## >>> Espion: The Global Leader in Network Disaster Protection

- > Detect unseen and unknown threats to your business, protecting against network disaster
- > Meet new compliance and regulatory requirements at a fraction of the cost of traditional security solutions
- > Eliminate internal network threats and insider misuse
- > Secure disaster protection and business continuity plans

### > 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](http://www.esphion.com)

Every day businesses around the world are besieged by Internet security attacks. At worst, these attacks bring businesses to a standstill for days at a time and at tens of millions of dollars of cost. At best, they represent an ever-increasing expense to enterprises and service providers also facing the additional complexity of new compliance and regulatory requirements.

Esphion delivers the world's first technology for real-time detection and prevention of unknown or unseen threats that result in network disasters.

### Business and Industry Drivers

With information technology now fully integrated into the fabric of business, organizations have become more dependent on IT than ever. Regulatory compliance requirements such as Sarbanes Oxley, the Hong Kong Personal Data Ordinance and Japan's Personal Information Protection Act bring a new level of urgency to solving today's security challenges.

Any interruption to IT comes at a significant cost to revenue and productivity. The Australian Computer Crime and Security 2003 Survey recorded that 42% of companies experienced an attack which harmed the integrity and availability of network data and systems. Other studies indicate that the average cost of an hour of downtime for data center applications is US\$35,000, while the lost productivity will cost an average of US\$438 per employee per day. These financial losses and disruptions are material to enterprises, often requiring increased investments over time to identify the cause and restore customer confidence. A study by the Computer Security Institute (CSI), conducted in partnership with the FBI's Computer Intrusion Squad, stated that 78% of respondents in a 2003 study had experienced "frequent" attacks on their networks from the Internet. The CSI study also found that 75% of respondents suffered significant financial loss due to security breaches of their networks. Aggregating those who were willing or able to quantify their losses, the total came to US\$201.8 million.

### Current Solutions Are Insufficient

Traditional security defenses such as firewalls, anti-virus and virtual private networks (VPNs) are insufficient in defending against highly sophisticated, fast-spreading network-based attacks. The proliferating threats grouped under the heading "malware" are perhaps the worst—and the fastest-growing. Malware includes Internet viruses and worms which can cause denial of service attacks, lead to a security breach of a corporate network, or bring a network down for an extended period.

A self-propagating worm can also dramatically reduce the performance of the network or cause it to stop working all together by swamping it with malicious traffic. Worms exploit common security holes, and reproduce at incredible speed, often "mutating" to make detection even more difficult.

Canadian network monitoring company Sandvine Inc. estimated that worm attacks cost North American service providers some \$245 million in 2004, up 60% from 2003 and that on any given day between 2% and 12% of Internet traffic is malicious.

### The Solution

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

Esphion's 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, Esphion can detect even zero-hour events in just seconds, and through a patent-pending analysis process extract signatures for those events.

[www.esphion.com](http://www.esphion.com)

[sales@esphion.com](mailto:sales@esphion.com)

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

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

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 enterprise (EX) and service provider (SP) appliances are designed to complement existing security elements, introducing a first and final line of defense. 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's distributed network anomaly detection and visibility architecture is deployed as either a stand-alone solution consisting of either the Esphion EX3000 or Esphion SP5000 appliance. Alternatively, Esphion can be deployed as a distributed solution at the network core or at access switches or routers, depending upon the outcomes needed. Distributed solutions use the Esphion EX3000c or SP5000c controllers along with EX3000i or SP5000i intelligent neural network agents respectively.

Intelligent neural network 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 network agents are aggregated by a single controllers, 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. Unlike traditional solutions, Esphion delivers:

- > Real-time, fine grained signature generation that accelerates response time from hours to seconds without interrupting applications or business services,
- > Neural network analytics to reduce false negatives and eliminate dependency on signature databases,
- > Packet-based, real-time monitoring that doesn't interrupt flow of network traffic, slowing transactions or business,
- > Carrier-grade architecture for high-volume, heterogeneous IP networks,
- > Integrated tools for automated and 'one-click' investigation and response.

## Measuring Return On Investment in Days

With Esphion in place, 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, and
- > Bandwidth requirements due to the identification of malicious network behavior, and a reduced requirement for additional bandwidth or disaster recovery systems.

Find out how Esphion can reduce your IT costs and prevent network disasters today.



© 2000-2005 Esphion Ltd. All rights reserved.

Esphion and netDeFlect are registered trademarks and the Esphion logo is a trademark of Esphion 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 Esphion and its licensors. If any, third-party software, including font technology, is copyrighted and licensed from Esphion suppliers.

This document was developed on the basis of information and sources believed to be reliable. This document is to be used "as is." Esphion 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. Esphion accepts no responsibility to inform the reader of changes in the data. In addition, Esphion may change its view of the products, services, analysis and companies described in this document. Esphion 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.