



Ernst & Young AB Using WebMarshal to Stop Web Mail Viruses Before They Do Damage

Client:

Ernst & Young AB

Web Site:

<http://www.ey.com/SE>

Requirements:

Webmail Filtering

Filtering Solutions:

WebMarshal

“It’s hard to put a value on threat prevention, but the software has done exactly what we wanted.”

Ludwig Brogård
NT-Manager
Ernst & Young AB

Financial consultancies and professional services companies are only as good as their communications. Whether written, spoken, posted or emailed, these companies live or die by how well they can transfer words and concepts from one person to another. The Internet has revolutionized the whole industry and has opened a number of new opportunities. But with opportunities come risks.

Global companies have come to rely on their Internet-based communications for any number of client-based and internal functions and have to ensure these information networks remain operational. They can’t wait for an incident to take place... they have to stop all threats before they become a problem.

Background

Ernst & Young AB is the Swedish branch of Ernst & Young. It is a global professional services company offering clients expert advice and consulting in auditing, accounting advice, tax compliance, planning and corporate finance transactions. As a global organization with global clients, it is essential that their systems are kept up and running and operating at peak efficiency.

Ernst & Young AB, were acutely aware there were many external threats to their network and wanted to ensure they could continue to provide uninterrupted support to their client base. “We hadn’t experienced any problems,” says Ludwig Brogård, ITManager at Ernst & Young AB, “and we wanted to ensure that it stayed that way.”

“We have a written security policy that specifies how our users should use digital information, but there was the possibility that perhaps something might slip through the cracks. We already had an anti-virus program in place,” says Brogård, “but it didn’t go far enough.”

“The growing popularity of web-based email has opened up very real risks that viruses and other threats to the network can sneak in past our traditional anti-virus defences. Again, we hadn’t had any incidents, but we wanted to guarantee that we would have no incidents in the future. With more than 2000 users on our network, it only takes one person to circumvent the rules and cause irreparable harm to the network and our reputation.”

So Brogård started a process of investigating what solutions on the market could prevent these types of threats from infecting their network. “We were fortunate in that we knew exactly what to look for in the solutions we examined,” says Brogård. “We undertook some very basic benchmarks and identified key features and benefits in the various solutions. After looking at the available solutions, we selected WebMarshal due to its web scanning capabilities and the fact that it provided the best cost/performance ratio.”

“Setting up WebMarshal across the network went very well.”

Ludwig Brogård
NT-Manager
Ernst & Young AB

The Ernst & Young AB network consists of a Windows 2000 network that connects approximately 80 offices throughout Sweden. The various offices connect to the Internet at speeds ranging from 384 Kb to 4 Mb.

Key Reasons for Selecting WebMarshal

- Best performance of all solutions examined
- Easy to set up and operate
- Can support extended operations from centralized management

Key Benefits

- Prevents viruses from entering the network via web mail
- Enforces formal Internet Acceptable Use Policy
- Ensures the network remains virus-free and operational

“Setting up WebMarshal across the network went very well,” says Brogård. “We installed and configured WebMarshal with our existing Internet Authentication Service (IAS) Server. We had a few questions with the exact configuration for the rules set up, but a few calls to our WebMarshal supplier, Inuit AB, cleared up all of the issues. We tested the rules and then went live.”

Conclusion

Since installation, WebMarshal has performed excellently. “We are still virus-free,” says Brogård. “It’s hard to put a value on threat prevention, but the software has done exactly what we wanted. It is great software for content scanning of proxy traffic, one of the hidden threats that can cause damage if undetected. We undertook some very basic benchmarks and identified key features and benefits in the various solutions and are very happy with M86.” Ludwig Brogård, NT-Manager at Ernst & Young AB.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers’ networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Asia-Pacific
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Auckland, New Zealand

Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 08.24.09