

USA.NET® eArmor®

PROTECT YOUR MESSAGING INFRASTRUCTURE WITH INDUSTRY-LEADING TECHNOLOGY FOR VIRUS PROTECTION, SPAM CONTROL, CONTENT FILTERING AND MORE.

USA.NET®

Global eMessaging

You run your business. We'll run your eMessaging.™

Today, the need to protect your information infrastructure from a broad range of malicious threats goes without question.

The critical issue is whether your technology resources should be focused on protection from email-borne threats, rather than your organization's core mission.

PROTECTION AT THE GATEWAY

Junk mail, viruses, fraudulent messages and inappropriate content impact enterprise-based messaging systems in multiple ways: Lost productivity, increased network bandwidth, increased storage, wasted IT resources and a host of other vulnerabilities.

USA.NET's eArmor provides a layer of filtration and protection right at the gateway. eArmor uses industry-leading technologies to identify and block viruses, spam and unwanted content before they enter your firewall and email systems. eArmor is the ideal solution for customers who wish to retain their existing email infrastructure, but desire state-of-the-art protective technology without investing precious capital or diverting critical IT resources.

SPAM BLOCKING

eArmor protects your users from the crushing burden of unsolicited bulk email. The system incorporates multiple protection strategies, including dynamic real-time spam detection and IP address/domain name blacklisting compiled by leading watchdog agencies.

VIRUS SCANNING

All messages and attachments are scanned prior to delivery using the industry's leading anti-virus technology for the enterprise. eArmor uses 24x7 real-time monitoring plus automatic continuous updates to keep your messaging system secure from the latest threats.

CONTENT FILTERING

eArmor makes it easy for organizations to implement e-policies regarding inappropriate content. An easy-to-use Web interface lets you set thresholds, comply with legal requirements, increase productivity and reduce network congestion.

MESSAGE QUEUING

In the event of an in-house email problem, eArmor queues incoming messages destined to your legacy email system until they can be successfully delivered to your in-house email servers. USA.NET's messaging architecture reacts immediately to ensure no loss of messages.

NETWORK PROTECTION

eArmor offers an additional layer of network protection against distributed denial of services attacks and directory harvest attacks. By pointing your MX record to USA.NET and creating a firewall rule that only allows connections to your legacy mail system from USA.NET, your network will be protected from direct encroachment.

MESSAGING REPORTS

eArmor gives you complete access to statistical graphs and reports detailing your email traffic activity, spam messages blocked and viruses that were cleaned and removed.

Email security is critical to the success of your enterprise. Ensure the reliability and continuity of your most valuable information assets by outsourcing this mission-critical responsibility to USA.NET.