

Email Security: Trends and Spending Plans for US Businesses

Executive Summary

Few would disagree that email has become the most popular application on the Internet. While email has made conducting day-to-day business easier, its prevalence has also introduced an abundance of threats to the corporate network. In addition, regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and Gramm-Leach-Bliley (GLB) give companies strong incentives to ensure that corporate mail systems are stable and secure.

In the past, organizations addressed email security with a variety of point products, both at the gateway and inside the network on servers and desktops. The result is an email infrastructure that can be complex and challenging to manage.

Email security products protect the email infrastructure of a company by performing spam blocking, virus protection, content filtering, and messaging security. These products can be standalone for a specific function, such as spam blocking, or integrated with multiple security functions.

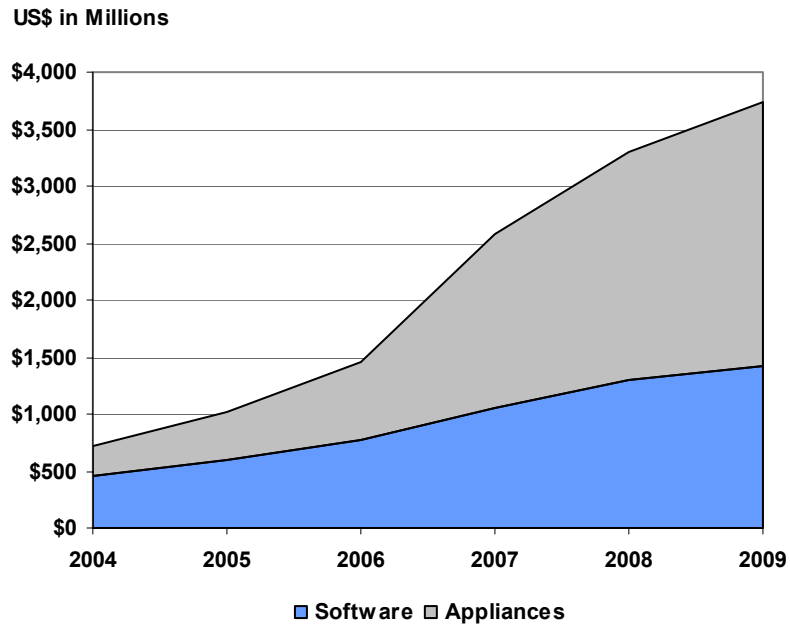
To gain visibility into the email security market segment, In-Stat conducted a decision-maker survey to discover trends in email security product usage and plans for future purchases.

Key findings include:

- Viruses and spam continue to be the top email security concerns with decision makers.
- 66% of the decision makers plan to purchase email security products within the next two years.
- More than 30% of the decision makers don't know whether the planned purchase will be software, an appliance, or a hosted service.
- By a high margin, reliability was the most critical factor in the purchasing decision.

The email security market is poised for strong growth during the forecast period, reaching a total of \$3.7 billion by 2009, as shown in Figure 1.

Figure 1. Email Security Software and Appliance Forecast



Source: In-Stat 4/05