THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM
WWW.RADICATI.COM
TEL. 650 322-8059

Secure Email Gateway Market, 2018-2022

SCOPE

This study provides an analysis of the Secure Email Gateway market in 2018 and its potential growth over the next four years. It offers a detailed analysis of worldwide market trends, market size and growth forecasts, market share by vendor, vendor products and strategies, and more.

The Secure Email Gateway market consists of solutions that can be deployed at the mail server or SMTP gateway level to filter out spam, viruses, phishing/spear-phishing attacks, and other malware from messaging traffic. Data Loss Prevention (DLP) and email encryption are also often part of a complete Secure Email Gateway solution.

This report focuses exclusively on corporate deployments, which include civilian government organizations and educational institutions. It does not include service provider deployments.

All market numbers, such as market size, forecasts, installed base, and any financial information presented in this study represent *worldwide* figures, unless otherwise indicated. All pricing numbers are expressed in $USD.

METHODOLOGY

The information and analysis in this report are based on primary research conducted by The Radicati Group, Inc. Our proprietary methodology combines information derived from three principal sources:

a. Our Worldwide Database which tracks user population, seat count, enterprise adoption and IT use from 1993 onwards.
b. Surveys conducted on an on-going basis in all market areas which we cover.
c. Market share, revenue, sales and customer demand information derived from vendor briefings.

Forecasts are based on historical information as well as our in-depth knowledge of market conditions and how we believe markets will evolve over time.

Finally, secondary research sources have also been used, where appropriate, to cross-check all the information we collect. These include company annual reports and other financial disclosures, industry trade association material, published government statistics and other published sources.

Our research processes and methodologies are proprietary and confidential.

EXECUTIVE SUMMARY

- Secure Email Gateways are software, appliances, or hosted services that protect organizations against email related threats by filtering out spam, viruses, and other malicious or unwanted messages. Increasingly these solutions must deal with phishing attacks (email-borne attempts to gather sensitive information, such as passwords, credit card numbers, etc.), spear-phishing (targeted phishing attacks), URL manipulation (emails carrying links that lead to corrupted websites), and compromised attachments.

- Spam is a broad term that includes a variety of unsolicited messages, which are usually sent out to a large number of users. Spam is very costly to deal with – users spend valuable time deleting these messages, it also clogs up network bandwidth, and

can often carry viruses and malware. Stopping spam is a top priority for IT administrators, as spam can cost companies millions, severely crippling corporate productivity and clogging corporate networks.

- Viruses have evolved over the years to include a variety of attributes designed to manipulate the computers of end users. Viruses are especially dangerous because of their self-propagating characteristics, meaning that once a virus infects a host computer, it can easily spread to other unprotected computers on a shared network.

- Phishing and Spear-Phishing attacks, which present users with some information they recognize and request that they connect to a site to input more information have become more prevalent and highly successful. The user is typically totally unaware of the attack and simply serves as a pass through allowing a threat to spread through an entire organization's network.

- End user education is key to avoiding or minimizing potential attacks. Technology alone cannot do everything, end users must be trained in safe online behavior and in particular in detecting suspicious emails which may pose a threat. To this effect, a great deal of effort has now been placed on automated anti-phishing training techniques that help train users in safe behavior as well as help assess potentially risky users. Many vendors of secure email gateway solutions now also offer automated anti-phishing training solutions, either as an integral part of their offerings or as an add-on solution.

- The Secure Email Gateway market continues to see strong growth as email remains one of the leading vectors for malware attack and penetration. Organizations of all sizes are investing heavily in solutions to help protect against all forms of email-borne threats, particularly phishing and spear-phishing attacks. User awareness training in dealing with spear-phishing and email borne threats has also become an increasingly important aspect of email security.

- The worldwide revenue for Secure Email Gateway solutions is expected to top $2.3 billion in 2018, and grow to over $3.9 billion by 2022.

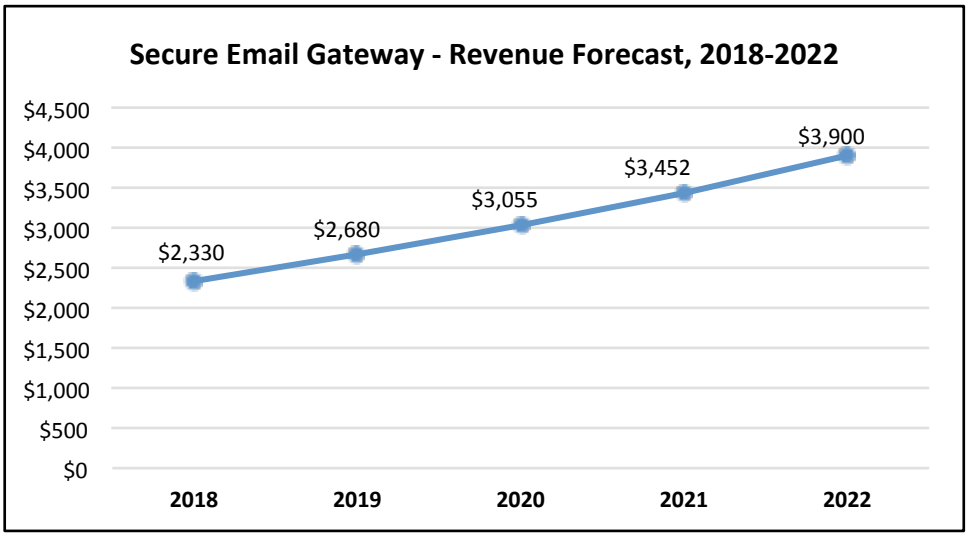

Figure 1: Secure Email Gateway Market Revenue Forecast, 2018 – 2022

To view the complete Table of Contents for this report, visit our website at www.radicati.com.