Secure Email Gateway Market, 2017-2021

SCOPE

This study provides an analysis of the Secure Email Gateway market in 2017 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 help protect against email related threats by filtering out spam, viruses, and other malicious or unwanted messages. Email continues to be the leading vector of malware penetration.

- Spam and Malware detection continue to be the main functions of Secure Email Gateway solutions. Spam detection needs to be able to deal with graymail (i.e. emails that users may have signed up for at one time but no longer want), as well as correctly identify spam without generating a high rate of false positives. Malware can include spyware, viruses, worms, rootkits, and much more. Key to malware detection is the ability to identify and protect against malicious email attachments, as well as malicious URLs contained in email messages.

- In addition, organizations must guard against phishing attacks (email-borne attempts to gather sensitive information, such as passwords, credit card numbers, and more),

spear-phishing (targeted phishing attacks), and URL manipulation (emails carrying links that lead to corrupted websites).

- Phishing and spear-phishing threats are becoming more targeted and personal. Blended attacks which present users with some information they recognize and request that they connect to a site to input more information, are becoming 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. Increasingly, support for industry standards, such as DMARC, SPF, and DKIM is becoming key to helping identify spoofed emails.

- Secure Email Gateways, today, are deployed in many different form factors, including on-premises, appliance, virtual appliance, cloud-based services, or hybrid.

- Vendors of Secure Email Gateway solutions are increasingly adding Data Loss Prevention (DLP), and email encryption capabilities to their solutions, as well as integrating with Advanced Threat Prevention (ATP) solutions.

- The Secure Email Gateway market is also seeing renewed investment and innovation from all vendors due to the need to keep up with evolving email-borne threats and the critical importance of feeding email attack/malware detection information to broader enterprise-wide security services (e.g. ATP, endpoints, and more).

- The Secure Email Gateway market, once considered very mature, is seeing very strong growth due to continued threats posed by email to organizations of all sizes. The worldwide revenue for Secure Email Gateway solutions is expected to top $2.0 billion in 2017, and grow to over $3.2 billion by 2021.

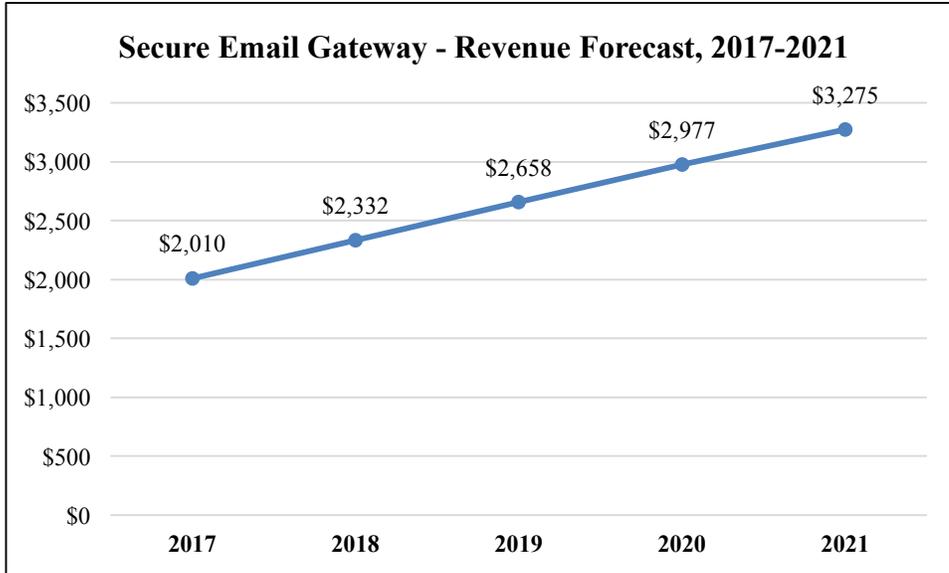**Secure Email Gateway - Revenue Forecast, 2017-2021**

Figure 1: Secure Email Gateway Market Revenue Forecast, 2017 – 2021

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