The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Secure Email Gateway - Market Quadrant 2018

An Analysis of the Market for Secure Email Gateway Solutions, Revealing Top Players, Trail Blazers, Specialists and Mature Players.

October 2018

* Radicati Market Quadrant℠ is copyrighted October 2018 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants℠ should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants℠ are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

TABLE OF CONTENTS

RADICATI MARKET QUADRANTS EXPLAINED 2
MARKET SEGMENTATION – SECURE EMAIL GATEWAYS 4
EVALUATION CRITERIA 6
MARKET QUADRANT – SECURE EMAIL GATEWAY 9
KEY MARKET QUADRANT HIGHLIGHTS *10*
SECURE EMAIL GATEWAY - VENDOR ANALYSIS 10
TOP PLAYERS *10*
TRAIL BLAZERS *26*
SPECIALISTS *35*

==========

Please note that this report comes with a 1-5 user license. If you wish to distribute the report to more than 5 individuals, you will need to purchase an internal site license for an additional fee. Please contact us at admin@radicati.com if you wish to purchase a site license.

Companies are never permitted to post reports on their external web sites or distribute by other means outside of their organization without explicit written prior consent from The Radicati Group, Inc. If you post this report on your external website or release it to anyone outside of your company without permission, you and your company will be liable for damages. Please contact us with any questions about our policies.

==========

RADICATI MARKET QUADRANTS EXPLAINED

Radicati Market Quadrants are designed to illustrate how individual vendors fit within specific technology markets at any given point in time. All Radicati Market Quadrants are composed of four sections, as shown in the example quadrant (Figure 1).

1. ***Top Players*** – These are the current market leaders with products that offer, both breadth and depth of functionality, as well as possess a solid vision for the future. Top Players shape the market with their technology and strategic vision. Vendors don't become Top Players overnight. Most of the companies in this quadrant were first Specialists or Trail Blazers (some were both). As companies reach this stage, they must fight complacency and continue to innovate.

2. ***Trail Blazers*** – These vendors offer advanced, best of breed technology, in some areas of their solutions, but don't necessarily have all the features and functionality that would position them as Top Players. Trail Blazers, however, have the potential for "disrupting" the market with new technology or new delivery models. In time, these vendors are most likely to grow into Top Players.

3. ***Specialists*** – This group is made up of two types of companies:

    a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.
    b. Established vendors that offer very good solutions for their customer base, and have a loyal customer base that is totally satisfied with the functionality they are deploying.

4. ***Mature Players*** – These vendors are large, established vendors that may offer strong features and functionality, but have slowed down innovation and are no longer considered "movers and shakers" in this market as they once were.

    a. In some cases, this is by design. If a vendor has made a strategic decision to move in a new direction, they may choose to slow development on existing products.
    b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

c. Companies in this stage will either find new life, reviving their R&D efforts and move back into the Top Players segment, or else they slowly fade away as legacy technology.

Figure 1, below, shows a sample Radicati Market Quadrant. As a vendor continues to develop its product solutions adding features and functionality, it will move vertically along the "y" functionality axis.

The horizontal "x" strategic vision axis reflects a vendor's understanding of the market and their strategic direction plans. It is common for vendors to move in the quadrant, as their products evolve and market needs change.

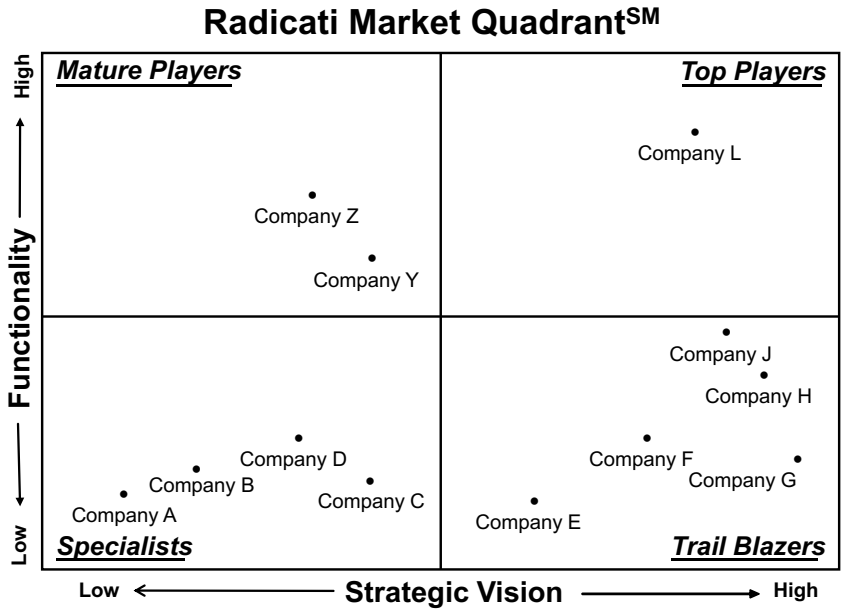

Figure 1: Sample Radicati Market Quadrant

INCLUSION CRITERIA

We include vendors based on the number of customer inquiries we receive throughout the year. We normally try to cap the number of vendors we include to about 10-12 vendors. Sometimes, however, in highly crowded markets we need to include a larger number of vendors.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

MARKET SEGMENTATION – SECURE EMAIL GATEWAYS

This edition of Radicati Market Quadrants[SM] covers the "**Secure Email Gateways**" segment of the Security Market, which is defined as follows:

- **Secure Email Gateways –** any software, appliance, or cloud-based service deployed at the mail server or SMTP gateway level to filter out spam, viruses, phishing/spear-phishing attacks, and other malware from messaging traffic. Some of the leading players in this market are *BAE Systems, Barracuda Networks, Cisco, Clearswift, EdgeWave, Forcepoint, Fortinet, Kaspersky Lab, Microsoft, Mimecast, Proofpoint, Retarus, SonicWall, Sophos, Symantec,* and *Trend Micro*.

- Some vendors of Secure Email Gateway solutions offer products for corporate customers, as well as service providers. This report, however, looks only at solutions aimed at corporate customers, ranging from SMBs to very large organizations.

- Vendors of Secure Email Gateway solutions are increasingly adding Data Loss Prevention (DLP), email encryption, and integrating Endpoint Detection and Response (EDR) and Advanced Threat Prevention (ATP) solutions with their email security solutions.

- 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 grow from over $2.3 billion in 2018, to over $3.9 billion by 2022.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

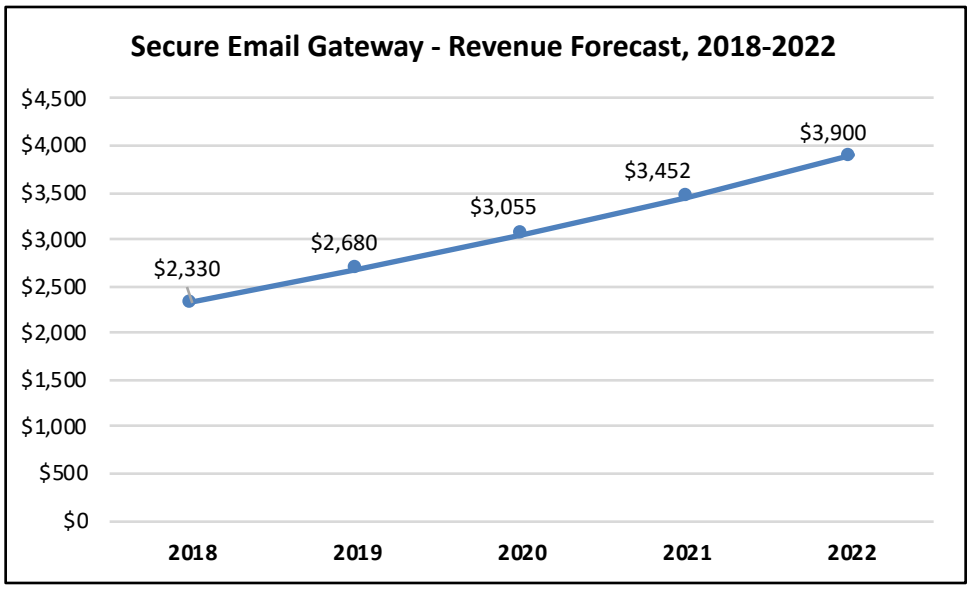

Figure 2: Secure Email Gateway Revenue Forecast, 2018 – 2022

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

EVALUATION CRITERIA

Vendors are positioned in the quadrant according to two criteria: *Functionality* and *Strategic Vision*.

Functionality is assessed based on the breadth and depth of features of each vendor's solution. All features and functionality do not necessarily have to be the vendor's own original technology, but they should be integrated and available for deployment when the solution is purchased.

Strategic Vision refers to the vendor's strategic direction, which comprises: a thorough understanding of customer needs, ability to deliver through attractive pricing and channel models, solid customer support, and strong on-going innovation.

Vendors in the *Secure Email Gateway* space are evaluated according to the following key features and capabilities:

- ***Deployment Options*** – availability of the solution in different form factors, such as on-premises, appliance and/or virtual appliance, cloud-based services, or hybrid.

- ***Spam and Malware detection*** – is usually based on signature files, reputation filtering (proactive blocking of malware based on its behavior, and a subsequent assigned reputation score), and proprietary heuristics. The typical set up usually includes multiple filters, one or more best-of-breed signature-based engines as well as the vendor's own proprietary technology. Malware engines are typically updated multiple times a day. 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. 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. Support for industry standards, such as DMARC, SPF, DKIM, which help identify spoofed emails is key.

- ***URL control*** – detection and remediation of compromised URLs, in emails and attachments.

- ***DMARC, SPF, DKIM support*** – support for leading domain anti-spoofing standards: Domain-based Authentication, Reporting and Conformance (DMARC), Sender Policy

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

Framework (SPF), and DomainKeys Identified Mail (DKIM).

- ***Email application controls*** – templates and customizable policies to block/allow and/or allow specific email traffic.

- ***Reporting*** – real-time interactive reports on user activity as well as long term reports, archiving logs, etc.

- ***Directory integration*** – integration with Active Directory, and/or LDAP allows to set, manage and enforce policies across all users.

- ***Data Loss Prevention (DLP)*** – allows organizations to define policies to prevent loss of sensitive electronic information. There is a broad range of DLP capabilities that vendors offer in their Email Gateway solutions, such as simple keyword-based filtering or full Content-Aware DLP. The inclusion of any DLP technology, is often still a premium feature.

- ***Mobile device protection*** – support for all email activity from mobile devices, such as iOS and Android. The protection of mobile devices needs to be addressed in full, preferably with no visible end user latency.

- ***Encryption*** – integrated email encryption or available add-on. The inclusion of encryption technology, is often a premium feature.

- ***Directory Harvest Attack (DHA) detection*** – detection of attacks designed to "harvest" legitimate email addresses within a particular domain by sending out a massive amount of emails to randomized addresses. Email addresses harvested in these attacks are used later for spam advertisements and fraud attacks.

- ***Detection of Denial of Service (DoS) attacks*** – detection of attacks intended to take down an organization's email system by sending a large number of emails to an address or domain, in the hopes that the email system is overwhelmed and shuts down, disallowing users under that domain to send or receive emails.

- ***ATP and/or Enterprise-wide attack correlation*** – ability to feed attack/malware detection information to broader enterprise-wide security services (e.g. ATP, web gateways, endpoints, and more).

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- ***Administration*** – availability of a single pane of glass management across all users and resources. In hybrid (i.e. mixed on-premises and cloud deployments) it is particularly important that a single administrative interface be available across both types of deployments.

In addition, for all vendors we consider the following aspects:

- *Pricing* – what is the pricing model for their solution, is it easy to understand and allows customers to budget properly for the solution, as well as is it in line with the level of functionality being offered, and does it represent a "good value".

- *Customer Support* – is customer support adequate and in line with customer needs and response requirements.

- *Professional Services* – does the vendor provide the right level of professional services for planning, design and deployment, either through their own internal teams, or through partners.

Note*: On occasion, we may place a vendor in the Top Player or Trail Blazer category even if they are missing one or more features listed above, if we feel that some other aspect(s) of their solution is particularly unique and innovative.*

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

MARKET QUADRANT – SECURE EMAIL GATEWAY

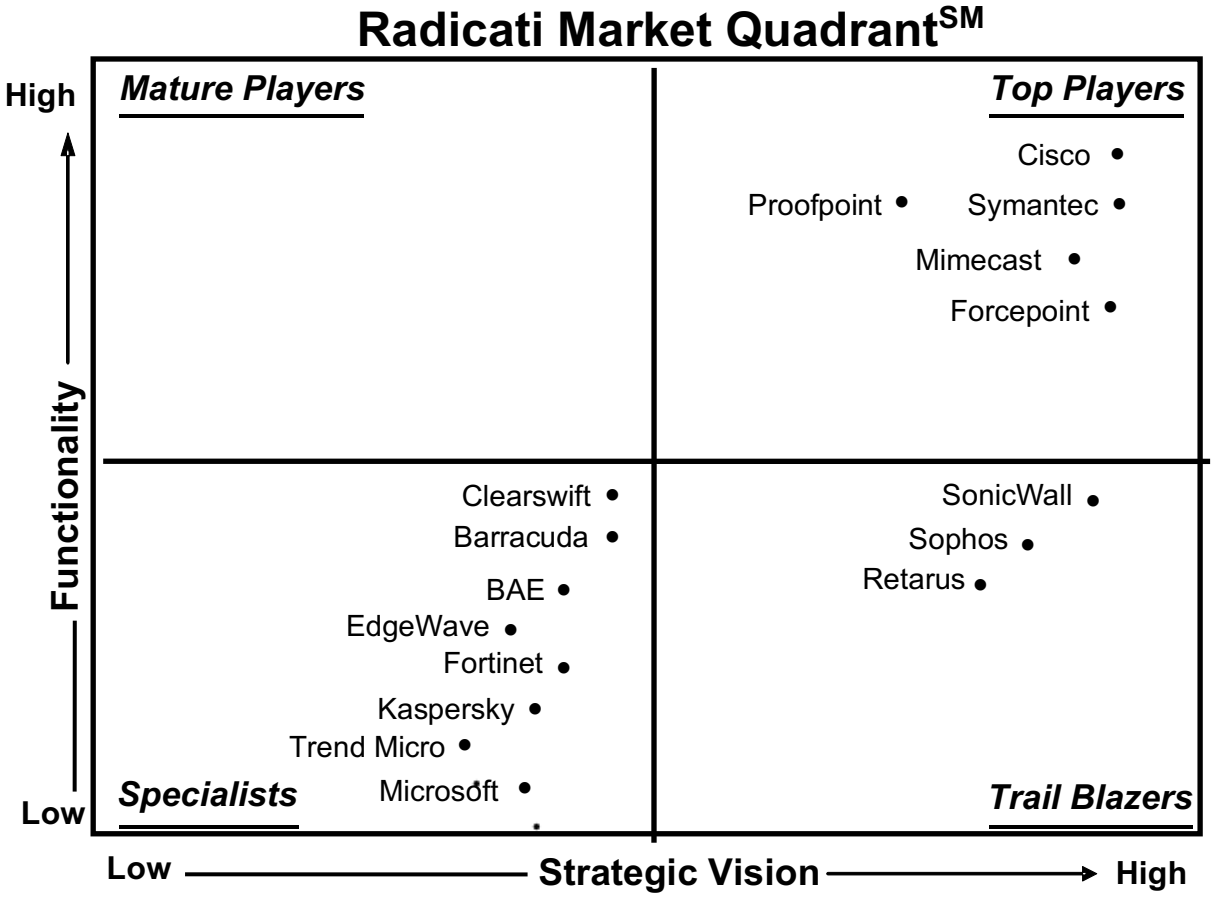

Figure 3: Secure Email Gateway Market Quadrant, 2018*

* Radicati Market Quadrant℠ is copyrighted October 2018 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants℠ should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants℠ are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

KEY MARKET QUADRANT HIGHLIGHTS

- The **Top Players** in the market are *Cisco, Symantec, Proofpoint, Mimecast* and *Forcepoint.*
- The **Trail Blazers** quadrant includes *SonicWall, Sophos,* and *Retarus*.
- The **Specialists** quadrant includes *Clearswift, Barracuda Networks, BAE Systems, EdgeWave, Fortinet, Kaspersky Lab, Trend Micro,* and *Microsoft*.
- There are no **Mature Players** in this market at this time.

SECURE EMAIL GATEWAY - VENDOR ANALYSIS

TOP PLAYERS

CISCO

170 West Tasman Dr.
San Jose, CA 95134
www.cisco.com

Cisco is a leading vendor of Internet communication and security technology. Cisco has invested in a number of acquisitions over the last four years, including OpenDNS, Cloudlock, Sourcefire, Cognitive, and ThreatGrid. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos), made up of leading threat researchers. Cisco is publicly traded.

SOLUTIONS

Cisco Email Security protects organizations from ransomware, email spoofing, phishing, advanced malware and other threats with simple, open, automated, and effective security across the entire attack continuum. It is available in four form-factors, as follows: Cloud Email Security (CES), Email Security Appliance (ESA), Virtual Email Security Appliance (ESAv), and Hybrid (Cloud and On-Premises).

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

All deployment options have feature parity. Cisco Email Security supports customers across all segments, with subscriptions starting as small as 100 users with the same features and deployment options available to customers of all sizes. Hybrid deployments offer consistent policies and a familiar user interface across on-premises and cloud environments, as well as allow customers to change the number of on-premises versus cloud users at any time during the term of their subscription.

Cisco's Email Security solutions comprise the following capabilities:

- **Spam & Threat Filtering** – includes the following:
  - *IP Reputation filtering* – is a first line of defense provided through SenderBase Reputation Filtering. For each inbound connection a SenderBase Reputation Score (SBRS) is assigned and maintained by Talos.
  - *Sender Domain Reputation Filtering* – enhances IP based reputation, by gathering additional information about the domain of the sender and returns a verdict based on multiple factors and intelligence gathered by Talos.
  - *Connection Controls* – are based on the score determined during reputation filtering, additional controls can be applied to limit the number of messages, connections or size of the message that can be accepted.
  - *External Threat Feeds* – provide the ability to leverage the STIX over TAXII standard to consume customized threat feeds to help automate workflow from SOC or Security teams to Operations.
  - *Anti-Spam* – Cisco also has "always on" Adaptive Rules based on heuristics that look for known characteristics of malware and viruses, that reside on-box, inside the Context Adaptive Scanning Engine (CASE).
- **Anti-Phishing and Malicious URL Detection** – Cisco offers deep inspection of URLs in five distinct phases during the scanning of messages, as follows:
  - *URL Filtering* - Known bad URLs are filtered as part of the antispam engine.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- *Content Filters* – are customizable filters with different options to control URLs, found in emails, this includes actions on their reputation and/or web categorization, as well as replacing the hyperlink with text (e.g. "This URL is blocked by policy").

- *Outbreak Filters* – look more closely into the context and construction of a message if an incoming email contains a suspicious URL.

- *Web Interaction Tracking* – allows for administrators to see the URLs that were re-written by Content or Outbreak filters, who the message was targeting and if they had clicked on the URL.

- *Advanced Phishing Protection* – further augments sender authentication and business email compromise (BEC) detection capabilities, by integrating machine learning and behavior analytics to protect against identity deception–based threats.

- **Anti-Spoofing** – includes offers the following detection methods:

  - *DMARC, DKIM and SPF analysis* – is done on incoming emails, and can also be leveraged within content filters in combination with other threat metrics.

  - *DANE support* – leverages DNSSEC to provide effective detection of DNS poisoning attacks with TLSA support.

  - *Forged Email Detection* – detects spoofed and fraudulent messages with a forged sender address (From: header) and performs specified message actions to protect high-valued executive names.

  - *Domain Protection* – automates the process of using email authentication to prevent phishing, protect brands from fraud and maintain email governance by analyzing, updating and taking action against senders misusing their domain to send malicious emails.

- **Malware and Attachment Control** – offers multiple layers of protection to block hidden threats within attachments:

  - *Antivirus* – multi-layer signature-based antivirus protection is offered through Sophos

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

and/or Intel (McAfee) antivirus engines. Customers can run both antivirus engines in tandem to dual-scan messages for more comprehensive protection.

- *Macro and FileType filtering* – full inspection of PDF, OLE and Office file type attachments for macro or script presence is available in the 11.0 release.

- *Bad URL document scanning* – allows scanning for malicious URLs inside PDF, OLE and Office file type attachments.

- **Advanced Malware Protection (AMP)** – consists of four phases:

  - *File Reputation* – AMP captures a fingerprint of each file as it traverses the gateway and sends it to AMP's cloud-based intelligence network for a reputation verdict checked against zero-day exploits.

  - *File Sandboxing* – when malware is detected, AMP gleans precise details about a file's behavior.

  - *File Retrospection* – deals with the problem of malicious files that pass-through perimeter defenses, allowing customers to begin remediation quickly if a breach occurs.

  - *File Remediation* – offers the ability to auto-remediate malware for mailboxes hosted in Microsoft Office 365.

- **Threat Visibility and Investigation** – includes:

  - *Cisco Threat Response integration* – Cisco Email security integrates with Cisco Threat Response to provide investigative capabilities on threats based on URL, SHA values or domains and pivoting into Message Tracking data to simplify the investigation of threats.

- **Outbound Control** – includes the following:

  - *Data Loss Prevention (DLP)* – is offered as a built-in engine that uses pre-tuned data structures along with optional data points such as words, phrases, dictionaries, and regular expressions to quickly create accurate policies with low false positives.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- *Encryption* – is available through two products: on-premise key storage encryption featuring the ZixGateway with Cisco Technology; or cloud key storage encryption with Cisco Registered Envelope Service (CRES). The products cover all use cases including push, pull, transparent secure delivery (TLS) and S/MIME. CRES is available as part of the Cisco Outbound Essentials bundle, while ZixGateway with Cisco Technology may be purchased as an add-on.

STRENGTHS

- Cisco's Email Security solutions can be deployed as physical or virtual appliances, cloud-based, or hybrid solution, with a consistent user experience across all form factors.

- Cisco Email Security leverages the threat detection capabilities of Talos, its advanced threat detection network which helps prevent zero-hour attacks by continually generating new rules that feed updates to its security products.

- Cisco Email Security is integrated with the AMP for Endpoint console and with Cisco Threat Response, this provides customers with tight control and visibility from the perimeter of the network to the endpoint.

- Cisco Email Security supports multi-layer defense capabilities that combine big data analytics harvested from signature-based analysis, reputation services, and behavioral analytics to deliver thorough risk analysis and low false positives.

- All Cisco cloud deployments are dedicated build-outs (rather than multi-tenant offerings), which provides greater overall security for customers concerned about moving to cloud.

- Cisco also offers a dedicated Microsoft Office 365 solution, aimed at the needs of budget-conscious small and medium businesses.

WEAKNESSES

- While Cisco already offers integration with Microsoft Office 365, it needs to add integration with Microsoft Exchange for malware auto-remediation, as well as tighter integration with Google G Suite.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- Cisco needs to work to extend the integration of its Email Security solutions with other components of its newly expanded security portfolio, such as Duo and OpenDNS Investigate. However, this integration is on the roadmap for future releases.

- Cisco Email Security solutions, while feature-rich, are somewhat more expensive than competing vendor solutions. However, Cisco also offers consumption based pricing which gives customers greater flexibility.

- Cisco Email Security does not currently offer user phishing awareness training which is becoming common with many email security vendors. The vendor has this on their roadmap.

SYMANTEC

350 Ellis Street
Mountain View, CA 94043
www.symantec.com

Symantec offers a wide range of security solutions for the enterprise and for consumers. Symantec operates the largest civilian cyber intelligence network, allowing it to see and protect against the most advanced threats. Symantec is publicly traded.

SOLUTIONS

Symantec offers several email security solutions in different form factors, as follows:

Symantec Email Security.cloud – is a multi-tenant, cloud-based email security service built to protect any combination of email deployments, including Microsoft Office 365, Google G Suite, hosted mailboxes and traditional on-premises email systems, such as Microsoft Exchange. Symantec Email Security.cloud blocks targeted attacks, spear phishing, ransomware, viruses and malware, business email compromise attacks, spam, and bulk mail with anti-malware and antispam services. It includes technologies, such as advanced heuristics, deep evaluation of links before email delivery, and impersonation controls. It also controls sensitive data and helps meet compliance and privacy requirements with built-in data loss prevention (DLP) and policy-based encryption policies. Integration with the Symantec DLP solution enables more comprehensive DLP controls for protection of data across multiple channels.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

Advanced Threat Protection:Email – is a service that can be added to detect new and stealthy targeted and advanced attacks while providing deep visibility into the attack landscape to accelerate remediation. It uses cloud-based sandboxing and payload detonation capabilities to identify and stop complex targeted and advanced threats, including attacks that are virtual machine-aware. Deep evaluation of suspicious links at the time of click helps block advanced phishing attacks that weaponize a link after an email is delivered. It also provides detailed data on targeted attacks that attempt to enter an organization via email, as determined by Symantec research analysts. The solution provides advanced email security analytics on every incoming clean and malicious email scanned. This includes 60+ data points such as URL information, file hashes, sandboxing data, sender and recipient information, and targeted attack information. The data can easily be exported to third-party Security Incident and Event Management (SIEM) solutions, Symantec Advanced Threat Protection, Symantec Managed Security Services, and other security tools via a granular API, which accelerates threat investigation and response. ATP:Email also provides Microsoft Office 365 customers with auto-remediation capabilities that can claw back emails from an inbox if they are detected as malicious post-delivery.

Symantec also offers a Phishing readiness service as part of ATP:Email so that customers can identify risky users, and improve end user awareness by enabling administrators to send simulated phishing attacks.

Symantec Email Threat Isolation – is an add-on service that stops advanced email attacks by insulating users from spear phishing, credential theft, and ransomware attacks. It prevents spear phishing attacks by isolating malicious links, stops credential theft by safely rendering webpages in read-only mode, and can shut down ransomware by shielding trusted applications from weaponized attachments.

Symantec Messaging Gateway – is an on-premises appliance (available as a physical or virtual appliance) which secures email with real-time antivirus and anti-malware protection, targeted attack protection, advanced content filtering, Symantec Data Loss Prevention integration, and optional email encryption.

Messaging Gateway integrates with Symantec Content Analysis, an advanced content filtering and malware analysis platform, to provide advanced threat protection. This provides offloading of messaging content for further inspection by Symantec Content and Malware Analysis, including actionable intelligence that combines static, dynamic, reputational, and YARA rules analysis techniques. An adaptive and customizable sandbox delivers comprehensive malware

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

detonation to quickly analyze suspicious files, interact with running malware to reveal its complete behavior, and expose zero-day threats and unknown malware.

All Symantec email security solutions are backed by the Symantec Global Intelligence Network, its global threat intelligence network.

STRENGTHS

- Symantec email security solutions are available as on-premises as well as cloud based solutions, which can be combined to also provide a hybrid solution.

- Symantec Email Threat Isolation is a valuable add-on which offers integrated threat isolation for corporate email and helps prevent advanced threats, such as credential phishing or ransomware.

- Symantec offers effective, accurate threat protection with low false positives through the use of multi-layered detection technologies, such as advanced heuristics, Real-Time Link Following, and intelligence from its own threat intelligence network.

- Symantec provides deep insight into targeted and advanced threats by exposing data on both clean and malicious emails, such as URL information, file hashes, sandboxing data, sender and recipient information, and targeted attack information. In addition, integration with SIEM solutions and other security tools enables security analysts to easily correlate threats across multiple security products.

- Symantec Email Security solutions are a part of the Symantec Integrated Cyber Defense Platform, which unifies cloud and on-premises security to protect users, information, messaging and the web. The integrated platform helps defend against advanced threats, and accelerate threat response across the whole security environment.

- Symantec's cloud and on-premises email solutions both support strong integration with Directory services, which allows easy policy-based administration.

- Symantec email security solutions enable customers to prevent data leakage and ensure compliance through granular DLP and encryption controls. This includes integration with

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

Symantec's stand-alone DLP solution.

WEAKNESSES

- Symantec has been working diligently to bring together and harmonize its portfolio of email security solutions across Email Security.cloud and Messaging Gateway. However, customers should check carefully that the features they expect are available in the deployment form factor they are selecting. Customers choosing a hybrid deployment should also expect differences in administration procedures across the different solutions.

- Symantec currently offers isolation for URLs, but lacks isolation for attachments in email. The vendor is working to address this and has it on its roadmap for future releases.

- Email Security.cloud and Messaging Gateway do not offer email archiving capabilities, but can integrate with third-party archiving solutions.

PROOFPOINT

892 Ross Drive
Sunnyvale, CA 94089
www.proofpoint.com

Proofpoint is a next-generation cybersecurity company protecting people, data, and brands from advanced threats and compliance risks. The company delivers solutions for inbound email security, outbound data loss prevention, email encryption, compromised accounts, eDiscovery, and email archiving. Proofpoint is publicly traded.

SOLUTIONS

Proofpoint offers email security solutions with capabilities which include: email filtering, analysis and classification, advanced threat protection, email authentication, web isolation, threat simulation, security awareness training, and information protection. Proofpoint solutions are available in a wide range of deployment options, which include: cloud, dedicated appliance, virtual appliance, or hybrid deployments.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

Proofpoint Email Protection – available as an on-premises or cloud based solution, serves to prevent phishing, including emails from lookalike domains, with granular search capabilities and visibility into all messages. It offers the following capabilities:

- *Targeted Attack Protection* – analyzes all URLs and attachments in email and cloud based applications both statically and dynamically in Proofpoint's cloud-based sandbox, accurately identifying widespread attacks and highly targeted attacks. All threat forensics, screenshots and threat landscape intelligence are visible in the management dashboard allowing administrators to understand the incidents, campaigns and threat actors. Proofpoint surfaces Very Attacked People (VAPs) within organizations, and highlights the threats that are targeting them to allow security teams to take additional steps to secure them.

- *Block email fraud* – offers visibility and control over email fraud attempts across employees, partners and customers, detecting all email fraud tactics including domain spoofing, lookalike domain spoofing and display name spoofing.

- *Account Compromise Detection* – provides analysis of all internal email to identify and remove spam and malware.

- *Secure Personal Email Usage* – protects against threats and data exfiltration, via employee use of personal email accounts, such as Gmail or Outlook.com.

- *Outbound information protection* – provides controls for encryption and data loss prevention, to protect against the loss of private or sensitive data including that associated with GDPR, or email fraud.

- *Automated Response* – includes the ability to automatically remove potentially malicious email from an end user inbox, as well as automated abuse mailbox monitoring. It also supports other actions, such as blacklisting IP addresses, quarantining an infected endpoint and requiring password resets.

- *Threat Simulation & Security Awareness Training* – is part of a people-centric approach to security, which helps assess end user vulnerability and puts in place corrective training to enhance the user's ability to identify and report threats.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

STRENGTHS

- Proofpoint offers a wide choice of deployment options including cloud, dedicated appliance, virtual appliance or a hybrid deployment.

- Proofpoint Email Protection integrates with threat intelligence and forensics about malware, phishing and email fraud to allow security teams to better understand threats, campaigns and the threat actor groups that carry out attacks.

- Proofpoint provides extensive reporting for email, threat forensics and DLP. DLP events are displayed in a dashboard with prioritization so administrators know which events to investigate.

- Proofpoint can protect against malicious URLs in attachments, and threats that are delivered as password protected attachments.

- Proofpoint offers the option to analyze internal emails to identify threats that may originate from inside the organization from compromised accounts.

- Automated response capabilities allow IT and security teams to resolve security incidents without incurring additional management overhead.

WEAKNESSES

- Proofpoint offers a best-in-breed secure email gateway solution combined and strong threat detection and protection from cloud applications, however, it does not offer endpoint protection or web security solutions. Customers wanting an integrated solution that combines secure email gateways, web security and endpoint protection will need to look elsewhere.

- Proofpoint's reporting capabilities could be enhanced through greater customization. The vendor is working to address it in future releases.

- Proofpoint solutions are still best known in North America, the company has increased sales coverage in Europe, but could invest further to improve its international presence.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

MIMECAST

CityPoint, One Ropemaker Street
Moorgate
London
EC2Y 9AW
www.mimecast.com

Mimecast is a provider of cloud-based email security and information management services for organizations. The core of Mimecast's services, include: email security, continuity and archiving services. Founded in 2003, Mimecast is registered and headquartered in London, UK, and has its North American headquarters in Boston, MA, with offices worldwide. Mimecast is a publicly traded company.

SOLUTIONS

Mimecast's Secure Email Gateway with Targeted Threat Protection protects against malware, spam, advanced phishing, impersonations, and other emerging and targeted attacks, while preventing data leaks. Mimecast also offers services for email Continuity and Enterprise Information Archiving which can be delivered as an integrated bundle with Email Security. Mimecast services are provided as cloud-based services, hosted in their global data centers.

Mimecast employs a multi-layered approach for spam, malware blocking and anti-phishing, which relies on a mix of established AV engines, reputation lists, file sandboxing, static file analysis, URL rewriting and related web site analysis, as well as proprietary heuristics to provide AV and AS filtering.

Mimecast offers a single integrated administrative console complete with templates and customizable policies that enables administrators to monitor, report, and change the block/allow decisions of the system, and manage many other aspects of their services.

Mimecast provides extensive logging to ensure visibility of user and overall organizational activities. DLP logs from emails offer breakdowns showing which DLP policy was triggered, by whom and what action was applied. In addition, Mimecast provides an API, inclusive of threat intelligence data, and out-of-the box integrations with SIEM systems (e.g. Splunk, IBM Q-Radar, LogRhythm) to enable data integrations to systems of the customer's choosing.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

Mimecast Targeted Threat Protection services extend traditional email security (AS/AV) to defend against targeted attacks, including malicious links in email, malware attachments and malware-less social-engineering attacks (i.e. business email compromise or impersonations). Real-time scanning and blocking of suspect websites, attachment sandboxing and static file analysis prevent employees from inadvertently downloading new or customized malware or revealing credentials to attackers. Inbound emails are also inspected to detect impersonations of internal domains, business partners, or well-known internet brands. Dynamic user awareness capabilities reinforce email security policies and engage employees in assessing risks on an ongoing basis as they click. Internal-to-internal and outbound emails are also inspected and remediated, to prevent the spread of attacks or policy violations in the movement of sensitive content.

Mimecast recently released the Mimecast Web Security service, which protects against malicious web activity initiated by user action, or malware attacks (i.e. ransomware or other malicious software). It is a fully cloud-based service, which also blocks access to inappropriate business websites, based on preset policies.

Mimecast also recently acquired, Ataata, a company which offers security awareness training and cyber risk management that helps combat information security breaches caused by employee mistakes.

STRENGTHS

- Mimecast offers a single integrated solution which can deliver email security, continuity, and archiving for inbound, outbound, and internal emails. This combination can be particularly useful when dealing with potentially destructive attacks, such as ransomware, that require prevention, failover, and recovery services.

- Mimecast solutions are fully cloud-based, providing automatic scalability and reliability while completely removing the customer's need to manage software and hardware.

- Mimecast's email security solution combines antispam, antivirus, attachment sandboxing/static file analysis and immediate safe file conversion, URL-protection/rewriting, DLP, secure messaging, large file send, and impersonation protection.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- Mimecast's solution integrates with the customer's Active Directory (AD) and Google G-Suite environments such that log-in is accomplished with the user's credentials and attributes about the user are used to determine access and security policy execution. AD and Google G-Suite information is also used to detect potential employee impersonations in inbound emails.

- Mimecast includes DLP capabilities based on its own technology. It also adds a fuzzy hashing capability which scores attachments based on content, and enables administrators to apply rules to make block/allow/encrypt decisions on outbound emails.

WEAKNESSES

- Mimecast provides email security, along with email continuity and information archiving, and web security gateway capabilities. While this is useful for some customers, it does not satisfy customers who may be seeking to acquire email security and with endpoint protection from a single vendor.

- Mimecast has been working to make its administration console more intuitive for administrators, however, the vendor still needs to improve on this in future releases.

- Customers we spoke to indicated that the DLP functionality could be improved through better filtering and reduced false positives.

FORCEPOINT

10900 Stonelake Blvd
3rd Floor
Austin, TX 78759
www.forcepoint.com

Forcepoint is a joint venture of Raytheon Company and Vista Equity Partners that was formed in 2015 out of a combination of Websense, Raytheon Cyber Products, and the Stonesoft and Sidewinder firewall assets it acquired from Intel Security in early 2016. In 2017, Forcepoint acquired the Skyfence CASB business from Imperva, as well as acquired RedOwl, a vendor of user behavior and security analytics. Forcepoint offers Web, data, and email content security,

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

cloud access security, next generation firewall, insider threat detection, user behavior analysis, and threat protection solutions to organizations of all sizes.

SOLUTIONS

Forcepoint Email Security delivers protection against multi-stage advanced threats that often exploit email to penetrate the environment. Core email defenses include phishing detection, phishing education, email spoofing detection, URL wrapping, DLP, embedded URL filters, and attachment filters. Additional security capabilities such as email encryption and advanced malware sandboxing are also available. Forcepoint solutions are available in all form factors, including cloud, on-premises, or hybrid. The on-premises and hybrid products can be deployed as physical or virtual appliances.

Forcepoint Email Security is available in the following form factors:

- *Email Security* – is the on-premises gateway-based core email security solution.

- *Email Security Cloud* – is a pure cloud-based solution.

- *Email Security Hybrid* – is the hybrid gateway-based email security solution. Hybrid means that the console and gateways are on premise, but all the malware detection and email pre-filtering is done in the Forcepoint cloud infrastructure.

Forcepoint Email Security applies Forcepoint's ACE threat analytics to detect dangerous emails and is part of the ThreatSeeker Intelligence network which shares threat intelligence across all Forcepoint solutions. Email attachments may be sent to the Forcepoint Advanced Malware Detection (AMD) sandbox, which available as either a cloud or on-premises solution. Phishing education and URL sandboxing are included with hybrid and cloud subscriptions. Unified management and reporting functions are provided across Email Security, Web Security and multiple DLP security solutions.

Forcepoint Email Security supports inbound SPF authentication and alignment, DKIM authentication, and DMARC validation across all form factors (on-premise, hybrid, cloud). Email Security also supports outbound DKIM signing across all form factors.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

Email DLP is included with Forcepoint Email Security at no charge and enables organizations to discover and protect sensitive data in the cloud, on-premises or hybrid. Custom or out-of-the-box policies, help secure personal data, intellectual property and meet compliance requirements quickly.

Additional modules that can be added to Forcepoint Email Security include:

- **Email Encryption Module** (cloud based) – provides advanced push-based encryption to secure confidential email communications. It is available as an add-on module for cloud and Hybrid core products.

- **Image Analysis Module** (available on-premises, hybrid or cloud based) – provides powerful illicit image detection capabilities to help employers monitor images distributed through email, educate staff members and enforce an organization's policies.

- **Advanced Malware Detection** (available cloud based or on premises) – offers a full system emulation sandbox to entice malicious behavior for detecting highly evasive zero-day and other advanced malware. It supports all deployment options of Forcepoint Email Security, as well as Forcepoint's CASB, next-generation firewall (NGFW), and Web Security solutions.

STRENGTHS

- Forcepoint's Email Security is available in a variety of form factors, giving customers a complete breadth of email security deployment options. Forcepoint's licensing model allows customers to change deployment architectures at any time during their subscription, at no additional cost.

- Forcepoint Email Security can leverage strong malware detection benefits as part of the Forcepoint security platform which integrates email security, web security and DLP into a cohesive platform.

- Forcepoint Email Security offers strong protection for Microsoft Office 365 with regards to both inbound and outbound email security.

- Forcepoint Email Security integrates with Forcepoint's broader security portfolio, customers owning both Forcepoint Web Security and Email Security have the ability to add URL

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

Categories via an API so both products can leverage the same custom list for their policies.

- The core Forcepoint Email Security offering includes enterprise-class DLP, pull encryption, URL sandboxing and phishing education services as standard modules with no additional fees.

- Forcepoint has revised its pricing and licensing structure, including its pricing for technical support, which makes it a more attractive solution for organizations of all sizes.

WEAKNESSES

- Forcepoint Email Security could be enhanced to leverage more security analytics and machine learning techniques already deployed in other Forcepoint products.

- Forcepoint Email Security does not yet integrate with SIEM solutions. The vendor has this on its future roadmap.

- Forcepoint Email Security does not yet integrate with Forcepoint's CASB solution, which is a missed opportunity.

- Forcepoint currently has data classification capabilities (i.e. Microsoft AIP, and Boldon James) as part of its DLP solution, but not in the Email Security solution. The vendor is working to address this in future releases.

TRAIL BLAZERS

SONICWALL

1033 McCarthy Boulevard
Milpitas, CA 95035
www.sonicwall.com

SonicWall solutions provide network security, mobile and endpoint security, identity and access management, email security, compliance and IT governance and security services aimed at the needs of SMB through the enterprise level customers, across all major verticals. SonicWall was

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

part of Dell Software Group until June 2016, when it was sold to private equity firms Francisco Partners and Elliott Management.

SOLUTIONS

SonicWall Email Security provides multi-layered protection from advanced email threats such as ransomware, zero-day threats, spear phishing and business email compromise (BEC), while enforcing data loss prevention (DLP) and compliance policies. The solution leverages real-time threat intelligence feeds from more than a million security sensors deployed globally as part of the SonicWall Capture Cloud Platform. SonicWall Email Encryption is available as an add-on cloud service for the secure exchange of sensitive data.

The solution provides the following key capabilities:

- *Antispam and Antivirus* – delivers anti-spam and anti-virus engines, to protect against known malware, spam and directory harvest attacks (DHA).

- *Anti-phishing* – utilizes a combination of methodologies such as Machine Learning, heuristics, reputation and content analysis to stop sophisticated phishing attacks.

- *Advanced Threat Protection* – isolates and blocks unknown threats found in suspicious file attachments and URLs using Capture ATP service with patent-pending Real-Time Deep Memory Inspection (RTDMI).

- *Data Loss Prevention* – helps enforce strong data-loss prevention polices to help organizations remain in compliance with regulations, such as HIPAA and PCI.

- *Administration* – provides an intuitive management interface, with a customizable dashboard that provides real-time visibility and monitoring, and comprehensive reporting.

The solution is available in the following form factors:

- **Hosted Email Security** – is a cloud-based email security solution offered in the SaaS model. It offers full support and easy integration with O365 and G Suite. It also includes email continuity to minimize business impact during planned and unplanned outages.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- **Email Security Appliances** – safeguard inbound and outbound email using a single appliance or clustered appliances environment. Designed for organizations with 25 or more users, the appliances come with a hardened Linux-based OS and the SonicWall Email Security application installed.

- **Email Security Virtual Appliance** – provide inbound and outbound email protection in a highly scalable VMware environment. It delivers the same security as a SonicWall Email Security Appliance, but in a virtual form.

- **Email Security Software** – delivers inbound and outbound email protection on one system with the flexibility to change, update or add on to existing Windows-based servers. Designed for organizations of 25 of more users, it offers the same features as SonicWall Email Security Appliance.

- **Comprehensive Antispam Service (CASS)** – eliminates inbound junk email at the gateway, before it enters the network. It is ideal for smaller organizations and distributed enterprises of up to 250 users that receive email at multiple locations and need gateway-based inbound email protection to reduce network traffic.

SonicWall Email Security offers MSPs a simplified user experience that supports a multi-tenant solution, with granular role based management, tenant level configuration, as well as reporting and branding.

STRENGTHS

- The SonicWall email security solution provides flexible deployment options, designed for high scalability and resilience.

- SonicWall Email Security offers strong expertise with email security and management technologies, including: multi-engine sandboxing with RTDMI for attachments and URLs, antivirus, antispam, phishing and fraud prevention, policy and compliance, data loss prevention, and email encryption in a variety of form factors that fit different customer needs.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- SonicWall Email Security is fully integrated with SonicWall's cloud-based Capture ATP multi-engine sandbox for analysis and detection of malicious attachments and URLs, that enables administrators to set granular inspection, remediation and quarantine policies.

- SonicWall Email Security supports DMARC, DKIM, and SPF message handling and reporting for anti-spoofing.

WEAKNESSES

- SonicWall Email Security currently lacks the level of sophisticated spear-phishing technology that is increasingly available from competing vendors.

- Encryption is provided through a technology partner, and is available as an add-on subscription service.

- SonicWall could add improved email archiving capabilities.

- SonicWall still lacks visibility in the Secure Email space, however, the vendor is working to address.

SOPHOS

The Pentagon Abingdon Science Park
Abingdon
OX14 3YP
United Kingdom
www.sophos.com

Sophos provides IT security and data protection products for businesses on a worldwide basis. Sophos offers security solutions such as endpoint and mobile security, enterprise mobility management, encryption, server protection, secure email and web gateways, next-generation firewall, UTM and email phishing attack simulation and user training. The company is headquartered in Oxford, U.K., and is publicly traded on the London Stock Exchange.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

SOLUTIONS

Sophos provides Secure Email Gateway solutions in both cloud and appliance models, as follows:

- **Sophos Email** – is a secure cloud email gateway that protects against unwanted and malicious email threats, including spam and phishing attacks. It integrates with artificial intelligence and sandbox technology to detect and block unknown threats and ransomware. Sophos Email works seamlessly with Microsoft Office 365, Google G Suite and on-premises solutions (including Exchange). It is delivered through the Sophos Central management console, which relies on Sophos Synchronized Security, a connected cybersecurity system that lets organizations manage multiple cybersecurity products from a single console.

- **Sophos Email Appliance** – is an all-in-one solution for email encryption, DLP, antispam and threat protection, which provides advanced protection from phishing attacks. It is available as an appliance or in virtual machine configurations. It can integrate with Sophos Sandstorm cloud sandbox for predictive threat protection using deep-learning technology. Sophos uses its own DLP engine and Content Control Lists, which are available at no extra cost in its Email Appliance. Sophos Email Appliance also includes encryption at no extra cost.

- **Sophos XG Firewall** – delivers a consolidated solution for network security, including: email, web, application and network protection. It is available as a physical or virtual appliance and can be managed through the Sophos Central console. It allows customers to benefit from Sophos Synchronized Security, a connected cybersecurity system that connects Sophos XG Firewall and Sophos Endpoint in order to automate threat detection and response.

Sophos uses its own technology for antivirus and antispam scanning, augmented with additional third-party technology as necessary. In addition, Sophos has data sharing agreements with threat protection labs that enhance its antivirus and antispam effectiveness.

The Sophos Central management console allows customers to manage multiple products including email, phishing attack simulation and computer-based training, web, Intercept X next-generation endpoint, mobile, server, encryption and wireless through a single cloud console. Customers can enforce the same policies and required level of data protection for endpoints and gateways, which greatly eases administration.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

STRENGTHS

- Sophos Email active threat protection (ATP) leverages time-of-click URL protection and Sophos Sandstorm, its cloud sandboxing technology, to identify and stop known and unknown malware, including ransomware, and unwanted applications before they execute.

- Sophos supports Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain Message Authentication Reporting & Conformance (DMARC) standards to identify and allow legitimate emails from trusted domains.

- Sophos's Email Appliance includes DLP protection and policy-driven encryption.

- Sophos Central management console allows customers to manage multiple Sophos products including email, phishing attack simulation and computer-based training, web, Intercept X next-generation endpoint, mobile, server, encryption and wireless through a single cloud console.

- Sophos is working to fully integrate its Email Security solutions with its Synchronized Security technology. The vendor plans to have automatic identification and clean-up of infected endpoints sending malicious outbound email, and targeted security awareness training, released by year-end.

- Sophos email security solutions, while feature-rich, are simple to use and attractively priced for customers of any size.

WEAKNESSES

- Sophos email security solutions currently provide email archiving only in the United States, through its hosting partner, Reflexion Networks. However, the vendor is working to extend availability to each of its datacenters worldwide. Organizations wanting to acquire email security and email archiving services from a single vendor, should check carefully on availability in their region.

- Sophos currently offers encryption as a standard feature only with its Email Security Appliance and XG Firewall solutions. The vendor plans to also make this available for its Sophos Email cloud-based solution.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- Sophos's cloud-based and appliance-based email security solutions offer somewhat different feature sets. Customers should check carefully to determine which solution best fits their protection needs.

- Sophos email security solutions are a best fit for small to medium sized customers.

RETARUS

Global Headquarters:
Aschauer Straße 30
81549 Munich, Germany
www.retarus.com

Retarus, founded in 1992, provides information logistics that support enterprise messaging services including email security, transactional messaging, digital document processing and delivery, as well as marketing communications. Retarus is based in Germany, with offices in the US, and worldwide. The company is privately held.

SOLUTIONS

Retarus **E-Mail Security** is a cloud-based solution providing protection for business communication while ensuring deliverability, compliance, ease of use, control and transparency. The solution provides protection at the gateway level, as well as post-delivery. Retarus E-Mail Security integrates with leading email infrastructures, including: Microsoft Office 365, Google G Suite, Microsoft Exchange, IBM Domino, and others. Key features of Retarus E-Mail Security include:

- *Spam and Malware* – detection is provided through licensed AV and AS technology. Retarus adds its own technology for rule set definition and filtering options. Incoming emails are spam-checked using multilingual content analyses as well as other intelligent filter, pattern, and identification rules that are updated continuously.

- *Email Application Controls* – black- and whitelisting on corporate, profile and user level is provided for inbound traffic. Sender reputation is carried out by validating the SPF (Sender Policy Framework) and using DKIM (DomainKeys Identified Mail). Retarus large email

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

handling allows recipients to receive large attachments despite any size limitations defined by their mail server. For outbound email communication Retarus offers additional services for transmission of both high volume and transactional emails. An Attachment Blocker prevents the delivery of files attached to incoming emails when these match criteria defined by the customer, for example blocking .exe, .zip, and Microsoft Office files with macros.

- *CxO Fraud Detection* – supports identification of fraudulent emails from fake senders (spear phishing). Retarus uses algorithms that identify from-spoofing and domain-spoofing, to detect falsified sender addresses (e.g. from C-level executives).

- *Sandboxing* – offers in-depth analysis of specific file attachments to provide advanced threat assessment, based Palo Alto Networks technology. Emails identified as infected are either deleted or quarantined, and a notification is sent to the intended recipient.

- *Time-of-Click Protection* – automatically defends against malicious links by rewriting URLs in emails. These links are checked for suspected phishing target addresses and users receive a security warning, if they try to click through to a suspected phishing site.

- *Monitoring & Reporting* – monitoring options in the administration portal give administrators an overview over the current traffic situation. An E-Mail Live Search tool allows administrators and helpdesk personnel to quickly find emails in real-time, release quarantined messages, and see all relevant processing steps of email through the gateway service.

- *Directory integration* – the Retarus DirSync Synchronization Wizard facilitates synchronization with directory data. It integrates with Microsoft Active Directory and LDAP directory services.

- *DLP* – checks emails to external recipients for defined patterns such as credit card and bank account numbers (IBAN). In addition, Retarus offers policy-based Data Leakage Prevention with the option to monitor email traffic to specific recipients/ from specific sender groups.

- *Encryption* – offers managed E-Mail Encryption key management service and supports standard encryption formats (e.g. PGP, SMIME, OpenPGP). Retarus also offers Secure Webmailer, a key management service which supports advanced encryption methods, alternatively customers can have the entire content of their encrypted message delivered to

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

the recipient inside a password-protected PDF document. This service is available as an extra cost option.

- *Patient Zero Detection* – provides early recognition and alerting of previously unknown malware and phishing URLs through its own patent-pending patient zero technology. The technology also uses digital fingerprinting to back-track, detect and clawback any threats in emails that have already been delivered.

- *Forensic SIEM Integration* – provides forensic data, in the form of events, for ingestion into SIEM solutions (security information and event management).

STRENGTHS

- Retarus delivers an attractive portfolio of email security capabilities in an efficient cloud-based solution that meets the needs of small to medium customers.

- Retarus recently launched a complete set of ATP solutions, including sandboxing, deferred delivery scan, Time-of-Click Protection (for URL rewriting) and CXO Fraud Protection (for anti-spoofing and spearphishing) and plans to continue innovating in this area.

- Retarus Patient Zero Detection extends email security to post-delivery, providing new levels of risk mitigation.

- The Retarus Enterprise Administration Portal offers easy to use real-time email live search including analytics and IT forensics.

- Retarus provides flexible access management and end-to-end encryption.

WEAKNESSES

- Retarus E-Mail Security is entirely cloud-based, which may not suit organizations that are still reluctant to rely entirely on cloud-based security.

- Retarus E-Mail Security does not currently support DMARC, however the vendor is working to address this.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- Retarus offers email encryption, through its Retarus E-Mail Encryption module, however this is available at an extra cost.

- Retarus currently lacks visibility in the enterprise security market, particularly in North America.

SPECIALISTS

CLEARSWIFT

1310 Waterside
Arlington Business Park
Theale, Reading RG7 4SA
United Kingdom
www.clearswift.com

Clearswift is an information security company with offices in the USA, UK, Australia, Germany and Japan with over 20 years of secure content, email and web security expertise. In 2017, Clearswift was acquired by Swiss defense company, RUAG and forms the product group for their Cyber Security Business Unit.

SOLUTIONS

The **SECURE Email Gateway** performs both email hygiene and advanced data loss prevention (DLP) and can be deployed as either hardware, software, hosted, or as a managed service.

The Gateway protects customers from new and existing malware using a combination of dual antivirus engines from Sophos and/or Kaspersky (a third AV will be added before the end of 2018). All engines provide real-time Cloud lookups which allow detection of the latest malware, leveraging both heuristic and behavioral based scanning. This is augmented by Clearswift active code detection mechanisms which can detect, and optionally remove, active code in html, Office, PDF and OpenOffice, allowing a safe document to be rapidly delivered to the recipient.

Antispam detection is provided by a layered solution utilizing IP reputation, grey-listing, anti-spoofing, RBL, SPF, DKIM, DMARC, sender validation and spam signatures and offers 99%+

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

spam detection with reliability. Clearswift offers message sanitization and URL's are checked against a real-time URL feed, as well as heuristics are applied to detect phishing exploits.

The product is designed to scan messages in either direction comprising of any language based upon a granular policy. There is a policy engine that performs message and attachment decomposition and also rebuilding. Format decomposition is provided without the use of third party technologies and allows the Clearswift solution to modify the data, for example redacting and sanitizing content.

Data Redaction permits the modification of text, html, PDF, Office and OpenOffice formats and allows textual modification by replacing keywords and phrases to be replaced with the "*" character. In items such as Credit Cards, all but the last 4 digits are replaced. This can also be performed on document footers/headers, watermarks and tracking comments. The bi-directional approach provides protection against unwanted data acquisition, as well as Data Loss Prevention, which is in line with new GDPR legislation where receipt of unauthorized information can create issues.

Document Sanitization allows for document properties such as Author, Subject, Status, Comments, etc. to be removed (properties can also be whitelisted to exclude from being sanitized, e.g. classification labels from Titus or Bolden James). Sanitization can also remove potentially embarrassing change tracking comments which may carry data which could represent a data leak.

Structural Sanitization identifies and removes active code from files such as HTML, Office, PDF and OpenOffice. These files can carry VBA, ActiveX, Javascript and OLE objects which could be used to launch an attack, including ransomware, on a message recipient. The Gateway can remove the active code from the file, and deliver a safe version in real-time.

All policies can be applied on both inbound and outbound email, which is key in adhering with compliance initiatives, such as the EU's GDPR. Tight integration with Active Directory or LDAP services enables reduced operational costs.

The Gateway also supports multiple types of encryption that permit the most appropriate technology to be used. Along with TLS as standard, customers can license the message encryption features of S/MIME, PGP and Password formats, or they can license the Portal based

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

approach with can be used in both push and pull modes. Portal options are available for both cloud-based or on-premises solutions.

The Gateway can be peered together with other email gateways to form a "Cluster", but it can also be peered with Microsoft Exchange or Office 365, to provide additional internal email inspection and DLP functionality, or with Web Gateways to provide a consistent policy across multiple communication platforms.

Clearswift also offers a variant of their SECURE Email Gateway, **ARgon for Email**, which is designed to augment existing email security gateway solutions from other vendors with Clearswift's DLP and Adaptive Redaction functionality.

STRENGTHS

- Clearswift's SECURE email gateway is available in a variety of deployment models, including on-premises appliance, software, virtual machine, cloud based hosted (support for Azure, AWS and other cloud vendors), and as a managed service to help meet diverse customer needs.

- Clearswift offers Adaptive Redaction features in all its Gateway products. This is a differentiator that is often missing in competing products.

- Integrates with Clearswift SECURE Web Gateway to help combat increasingly sophisticated threats, such as Dynamic malware on URLs.

- Clearswift can scan internal email traffic as well as traffic that crosses the organizational boundary. This includes both on-premise Exchange installations, as well as Office 365.

- Clearswift's SECURE email gateway forms the basis of a complete DLP solution when coupled with Clearswift SECURE Web Gateway and End Point solutions (customers can license additional advanced DLP features, including Optical Character Recognition (OCR), as required on-top of the base hygiene product).

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

WEAKNESSES

- Clearswift solutions would benefit from integration with sandboxing solutions. This is scheduled for 2019.

- Clearswift SECURE email gateway would benefit from more support for customized threat feeds.

- Clearswift SECURE reporting could be improved, through more granularity and greater customization. The vendor has this on their roadmap.

BARRACUDA NETWORKS

3175 S. Winchester Blvd
Campbell, CA 95008
www.barracuda.com

Founded in 2003, Barracuda Networks provides content, network and application security and data protection services to organizations. Barracuda Networks is a publicly traded company.

SOLUTIONS

Barracuda Email Security Gateway solutions are available through flexible deployment options which include hardware appliances, virtual appliances, cloud hosted, and public cloud instances (e.g. AWS, Azure, vCloud Air). It offers the following solutions:

- **Barracuda Email Security Gateway** – is an appliance-based solution which manages and filters inbound and outbound email traffic to protect organizations from email-borne threats and data leaks. It is available as a virtual appliance, or in a public cloud environment, such as Amazon Web Services (AWS), Microsoft Azure, or VMware vCloud Air.

- **Barracuda Essentials** – is a cloud-based email security solution that combines several layers of protection for inbound and outbound email to secure against advanced email borne attacks, and email spooling to ensure business continuity. Barracuda offers a multi-layered antispam protection approach that involves connection management including rate control, IP

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

reputation including RBLs, sender and recipient authentication and content scanning policies including attachment filters, URL/image investigation, and custom policies. Essentials includes attachment sandboxing as well antivirus, anti-phishing, and typo-squatted link protection to secure against sophisticated targeted attacks. It includes data loss protection and email encryption to keep sensitive data secure, as well as email continuity services in the event the primary email service becomes unavailable. Barracuda Essentials is email-system agnostic and supports all email systems, including Microsoft Office 365.

- **Barracuda Sentinel** – is a real-time spear phishing and cyber fraud defense that combines three layers to protect people, businesses and brands: AI for Spear Phishing Detection, Domain Fraud Protection, and Anti-Fraud Training.

- **Barracuda PhishLine** – helps protect against social-engineering threats through continuous simulation and training for employees. It allows organizations to embed antiphishing attack simulation into everyday business processes, to help users recognize and stop email fraud, data loss and brand damage.

Barracuda also offers **Total Email Protection**, which combines Essentials, Sentinel and PhishLine into a single bundle, for easy adoption by cloud-oriented organizations.

Barracuda's email security solutions include DLP capabilities at no additional cost. Customers can prevent or block outgoing emails based on content in the subject, body, header, attachments, or using Barracuda's pre-defined filters. Barracuda's email security solutions also offer pull based encryption capabilities at no extra charge. Customers can send out encrypted emails via policies defined by administrators, or via an Outlook add-in.

Barracuda's Advanced Threat Protection (ATP) combines behavioral, heuristic, and sandboxing technologies to protect against zero hour and targeted attacks. ATP automatically scans email attachments in real-time; suspicious attachments are detonated in a sandbox environment to observe behavior. In addition to blocking attachments, the results are fed back into the Barracuda Real Time System providing protection to all other customers.

Barracuda offers an easy to use dashboard view that summarizes what the solutions have blocked and allowed for both incoming and outgoing email. In addition, the Barracuda Cloud Control administrative interface, which is available at no charge, allows customers to add in other Barracuda products and manage all products through a central user interface.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

STRENGTHS

- Barracuda Email security solutions are available in a number of form factors to satisfy a broad range of customer needs.

- Barracuda solutions are easy to install, manage and monitor through centralized on-premises management with or without a separate management box, or through Barracuda's Cloud Control administrative interface.

- Barracuda Real-Time Protection offers strong protection to stop rapidly propagating threats.

- Barracuda solutions are attractively priced at different price points to meet the needs of small, medium and large sized organizations.

WEAKNESSES

- Barracuda provides only basic DLP functionality, customers with more advanced requirements will need to add a special-purpose DLP solution.

- Barracuda's support for mobile devices could be improved, as it currently only provides the ability to manage quarantine email and appliances through mobile device browsers.

- Barracuda's DMARC/DKIM/SPF capabilities could be improved, to more fully cover both outgoing and incoming email traffic.

- Customers we spoke with indicated that setup and administration of Barracuda's email spoofing detection capabilities could be improved.

- Barracuda's traditional email security solutions have lacked market visibility. However, the vendor is gaining market awareness with its Essentials and Sentinel solutions.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

BAE SYSTEMS

265 Franklin Street
Boston, MA 02110
www.baesystems.com/businessdefense

BAE Systems provides on-premises and managed threat analytics as well as cloud-based messaging, compliance, and cyber security services to governments and businesses of all sizes on a software-as-a-service (SaaS) platform.

SOLUTIONS

BAE Systems offers enterprise-grade, Software-as-a-Service (SaaS) **Email Protection Services (EPS)**, which seamlessly integrate into any on-premises or cloud email system such as BAE Systems' Managed Microsoft Exchange, or Microsoft Office 365. BAE Systems derives intelligence from a broad client base of large enterprise and government clients, which gives it high visibility into attacks worldwide. BAE email security is part of the vendor's broader offering of products and services around threat detection and response. EPS is a modular solution that allows companies to protect their email infrastructures against email-borne malware and remain compliant with regulations such as HIPPA, FINRA, FRCP, and SEC.

EPS consists of the following components:

- *Targeted Attack Protection* – uses a combination of static and dynamic analysis to catch advanced malware. These techniques use proprietary live browser analysis technology and instrumented application methods to isolate and defeat attempted attacks that traditional sandbox scanning may miss. Also, Targeted Attack Prevention includes click-time protection which provides real-time detection and blocking capabilities to protect against malicious links.

- *Data Loss Prevention* – allows companies to block, quarantine, redact or automatically encrypt emails depending on business policy requirements. It can also be used to detect similar domains, look for urgency terms, or provide SPF, DKIM, and DMARC authentication checks to detect Business Email Compromise (BEC). Data Loss Prevention includes industry-specific policy packs to help customers in highly regulated markets with the compliance to GLBA, HIPAA, and PCI DSS for best-in-class policy management and hardened protection against confidential and proprietary information loss.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- *Antivirus and Antispam* – provides multi-engine antivirus and antispam scanning to block malicious emails at the gateway. It is a cloud-based solution that is compatible with on-premises and cloud-based email services.

- *Social Engineering Protection* – defends against social engineering based attacks, including look-a-like domains, display name abuse, and other forms of business email compromise (BEC). The solution uses machine learning algorithms to scan historical email and identify patterns of communication, automatically detecting and blocking BEC without requiring any customer input. It generates a score assigned to each message, indicating the level of risk, which can be customized to determine delivery preferences and/or display the risk to the end user through a banner applied directly into the body of the email.

- *Email Encryption* – provides configurable policy-based and user-level encryption enabling secure communications. Users read their email using a web portal resulting in no additional software being required.

- *Compliance Archiving* – provides tamper-proof compliance archiving and eDiscovery capabilities to retrieve messages.

- *Email Continuity* – service ensures that email is always accessible even when an email server is down. It securely stores all inbound and outbound email messages offsite in BAE Systems' data centers. In the event of an email server outage, users can access their emails using a webmail interface.

BAE Systems also offers **Security Management Console**, a web-based administration system that incorporates an incident dashboard, real-time message tracing, workflow analysis, and comprehensive reporting. It allows administrators to manage a variety of BAE Systems security applications including Targeted Attack Protection, Data Loss Prevention, Social Engineering Protection and Managed Security Services (MSS).

STRENGTHS

- BAE Systems offers a full suite of cloud-based email security solutions that defend against known and unknown malware, phishing-style emails, spam, viruses, zero hour threats, malicious email attachments and business email compromise.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- Email Protection Services from BAE Systems are fully integrated with one another, and easily controlled with BAE Systems' web-based Security Management Console.

- BAE Systems delivers strong DLP capabilities, including comprehensive DLP Professional Service packs that provide support for tailoring customer policy based on the organization's threat landscape.

- BAE System's Email Protection Services generate Email event logs that can be exported to SIEM platforms, such as ArcSight and QRadar.

- BAE Systems offers policy-based email encryption that allows users to easily send encrypted email to anyone regardless of their email system. No software is required at the user level as BAE Systems operates the infrastructure, and access to the encrypted email is via a login over SSL to a secure server which ensures integrity and confidentiality of the delivery.

- BAE Systems' EPS is attractively priced for the comprehensive set of services it provides.

WEAKNESSES

- BAE Systems relies on third party vendors for its antispam and antivirus engines.

- BAE Systems' EPS is entirely cloud-based, which may not suit organizations that are still reluctant to rely on cloud-based security or are looking for hybrid solutions.

- BAE Systems EPS does not currently scan internal emails. The vendor has this on its future roadmap.

- BAE Systems offers antiphishing awareness training in partnership with a third party vendor. However, the solutions are not currently integrated into a common console, a capability which is becoming common among many email security vendors.

- BAE System's EPS has been improving its administrative reporting capabilities, but still lacks some of the granularity available in other vendor solutions. The vendor is aware of this and continues to invest in this area.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

EDGEWAVE

4225 Executive Square, Suite 1600
La Jolla, CA 92037
www.edgewave.com

EdgeWave, founded in 1995, recently refocused exclusively around email security and the ongoing phishing challenge. EdgeWave delivers a multi-layered Email Security Platform that provides pre- and post-delivery security and incident response. The platform is powered by EdgeWave ThreatTest, an automated anti-phishing solution the uses both machine learning and expert human review to analyze suspicious email activity. The company is privately held.

SOLUTION

EdgeWave ePrism Email Security Gateway is a multi-layer solution that combines machine learning with expert human analysis. ePrism Email Security Gateway can be deployed on-premises, as a cloud solution, or as a hybrid solution. It provides the following key capabilities:

- *Spam & Malware* – relies on Third party AV engines and reputation filters, which are complemented by spam & malware detection custom rules written by the EdgeWave Threat Detection Analysts.

- *URL detection* – ePrism uses both URL reputation lists as well as its internal iGuard database derived from its web security solution. Customers can configure whether to render the compromised URL intert (un-clickable), or to quarantine the entire email.

- *DMARC support* – ePrism supports SPF, DKIM and DMARC equally across all deployment models.

- *Email Application controls* – ePrism supports numerous controls for blocking/allowing email, including content filters looking for keywords, and domain fuzzing to help detect spoofing attacks.

- *Reporting* – the ePrism console provides numerous pre-built reports, many of which can be displayed on the customizable console dashboard. The advanced reporting capability allows administrators to build reports from over 50 different fields.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- *Directory integration* – ePrism supports numerous directory integration options, including LDAP, Microsoft Office365, and Google G Suite. Based on directory integration, ePrism provides administrators the option to configure filtering options at the mailbox/user level.

- *Data Loss Prevention* – EdgeWave offers are two options for DLP: customers can create their own custom filters and define the content to be identified, or use an extra cost DLP feature identify PII across credit cards, SSN, health, finance and profanity.

- *Encryption* – TLS support is available for all customers. Park-and-pull and push encryption options, developed by EdgeWave, are available at an extra cost.

- *Administration* – is provides through a web based portal that allows access to all configuration data, reporting and log access. The portal is based HTML5 and supported on all browsers without the need for additional plug-ins or technology.

STRENGTHS

- The EdgeWave Email Security Platform offers customers a holistic email pre-delivery, post-delivery, and incident response solution.

- The ePrism Email Security Gateway provides a high level of policy control granularity.

- ePrism Email Security Gateway provides strong, customizable reporting features.

- ePrism Email Security Gateway offers flexible deployment options including on-premises, cloud, and hybrid, which can be administered through a single-pane of glass management console.

- The EdgeWave Email Security Platform is attractively priced for SMBs and larger customers.

WEAKNESSES

- ePrism Email Security Gateway lacks integration with sandboxing capabilities, which many competing vendor offer. The vendor has this on its roadmap.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- While ePrism Email Security Gateway provides URL detection, it currently lacks URL rewriting. The vendor has this on its roadmap.

- The ePrism Email Security Gateway lacks support for iOS and Android apps.

- Encryption is available at an extra cost.

- DLP features, while available, are fairly basic.

- EdgeWave needs to invest to help raise its market visibility.

FORTINET

899 Kifer Road
Sunnyvale, CA 94086
www.fortinet.com

Founded in 2000, Fortinet is a global provider of next-generation firewall, network security appliances and security subscription services for carriers, data centers, enterprises, distributed offices and MSSPs. Fortinet is publicly traded.

SOLUTIONS

Fortinet's **FortiMail** is a secure email gateway solution designed to protect against inbound attacks, including advanced malware, as well as outbound threats and data loss. It includes: antispam, anti-phishing, antimalware, sandboxing, data leakage prevention (DLP), identity based encryption (IBE), and message archiving. Fortinet solutions leverage the Fortinet Security Fabric service, which delivers broad protection and visibility across network segments, devices, and appliances, to help enforce policies, coordinate threat responses, and manage different security solutions through a single console.

FortiMail is available in a broad range of form factors, including: high performance physical appliances, purpose-built virtual appliances (including virtual appliances optimized for Microsoft Azure and Amazon Web Services), SaaS managed by Fortinet, and MSSP managed by partners.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

FortiMail utilizes its own technologies for spam and malware detection. Low impact detection methods based on globally observed external malicious behavior (FortiGuard services) or locally observed malicious behavior (Dynamic Sender Reputation, Connection Rate Limiting) detect and prevent spam with minimal impact on the devices. The antimalware engine combines signature matching, behavior analysis, code emulation and decryption and unpacking. The engine is powered by Fortinet's own patented Content Pattern Recognition Language (CPRL) which enables much more sophisticated analysis than typical hash matching. Organizations optionally leverage on-premises or cloud based sandboxing of URLs and attachments for even deeper dynamic analysis.

New threat outbreaks are quickly detected by real-time data analytics of requests to the FortiGuard service from millions of global endpoints, which allows new threats to be blocked in a matter of minutes.

Fortinet, recently added several new features including: Content Disarm & Reconstruction, to handle malicious embedded code; Impersonation Analysis, to address Business Email Compromise that may not include malicious URLs or files.

FortiMail includes flexible email access control policies based on internal, external, group or LDAP defined routes. Policies can be applied to incoming or outgoing email, and blocked or simply rate controlled.

FortiMail supports policy enforcement over industry-standard TLS and S/MIME encrypted email, as well as proprietary identity-based encryption.

Identity Based Encryption is an integrated component and developed in-house. It is included at no additional charge with physical or virtual appliances.

DLP is also an integrated component comprised of smart identifiers, preset dictionaries and more.

For reporting, FortiMail offers a real-time dashboard which presents current information on email activity. The latest version, 6.0, is a complete overhaul of version 5.4 to be more intuitive for administrators. It also provides widgets and topology icons for the Fortinet Security Fabric, . On-box logging and reporting provide robust information based on capacity, with the ability to also share logs to off-box central reporting.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

FortiMail integrates with other Fortinet security solutions, and works in concert with other Fabric-ready technology partners, which form part of the Fortinet Security Fabric which helps stop advanced threats while maintaining regulatory compliance.

STRENGTHS

- Fortinet's FortiMail is available in all form factors, including physical and virtual appliance (including those optimized for Microsoft Azure and Amazon Web Services), SaaS or as a Managed Security Service, which helps address the complex deployment needs of a broad range of customers.

- FortiMail, along with FortiSandbox, can be easily deployed as a supplement, rather than replacement of existing secure email gateways, giving customers a quick way to address advanced email threats without switching out their production email infrastructure.

- FortiMail is an all-in-one solution which comprises advanced data protection features, such as DLP, encryption and archiving with its "core" threat prevention capabilities.

- Fortinet also offers Content Disarm and Reconstruction, a threat neutralization technique, and has added Impersonation Analysis to address Business Email Compromise.

- FortiMail is part of Fortinet's broader Fortinet Security Fabric which ensures seamless security through integrations into network security, ATP, sandboxing and more.

- Fortinet products are all developed in-house (without relying on OEM products), which allows the vendor to deliver solutions with broad threat insight, consistently high effectiveness and seamless operation across products.

WEAKNESSES

- While Fortinet supports all form factors it lacks a consolidated management interface across its appliance and cloud deployments to help support hybrid deployments.

- While DLP is an integrated component of FortiMail which offers strong detection capabilities its associated compliance workflow capabilities are still limited.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- Fortinet needs to offer streamlined integration with cloud email services, such as Microsoft Office 365 and Google G Suite.

- Fortinet support for outbound DMARC functionality could be improved. The vendor has this on its roadmap.

- Fortinet does not currently phishing awareness training, a functionality which is becoming increasingly popular with competing solutions.

KASPERSKY LAB

39A Leningradsky Highway
Moscow 125212
Russia
www.kaspersky.com

Kaspersky Lab is an international group, which provides a wide range of security products and solutions for consumers and enterprise business customers worldwide. The company's security portfolio includes endpoint protection, as well as specialized security solutions and services to combat evolving digital threats. The company has a global presence and is privately held.

SOLUTIONS

Kaspersky Security for Mail solutions, including Kaspersky Security for Microsoft Exchange, Linux-based mail servers and IBM Domino, provides protection from spam, phishing, generic and advanced malware threats, in complex heterogeneous infrastructures. Protection against confidential data loss through emails and attachments is also provided for Microsoft Exchange Server environments.

These solutions address specific customer needs, as follows:

- **Kaspersky Lab's Secure Mail Gateway | Virtual Appliance (KSMG)** – is designed to run on VMware ESXi, or Microsoft Hyper-V installations. An ISO build is also available, which can work on any hypervisor supporting ISO-based Virtual Machines, or can be installed on

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

bare metal. Deployed as a mail gateway or relay, the virtual appliance provides secures in-and-outbound mail from malware, spam, phishing and zero-day threats. The solution is also offered in the Microsoft Azure marketplace.

- **Kaspersky Security for Linux Mail Server** – provides anti-malware protection of Linux mail servers with rapid and accurate detection of malicious email attachments including unknown and advanced malware used in targeted attacks. It is designed for highly loaded mail servers under Linux and FreeBSD systems and supports Postfix, Sendmail, CommunigatePro, Qmail and Exim.

- **Kaspersky Security for Microsoft Exchange Servers** – provides protection and centralized management of Microsoft Exchange servers. It includes embedded DLP-like functionality which allows searches for specified text patterns in email communications. A single administration console with centralized reporting is integrated into Microsoft's Management Console to manage the security of all Microsoft Exchange servers. Security management and confidential information distribution management activities can also be assigned to separate roles and individuals if needed.

- **Kaspersky Security for Microsoft Office 365** – is a separate solution offered as part of Kaspersky's cloud solutions that provides security for Microsoft Exchange Online and Microsoft Office 365.

STRENGTHS

- Kaspersky Lab's Secure email solutions include advanced spam detection technologies based on the vendor's longstanding expertise in identifying and blocking unwanted traffic.

- Kaspersky Lab's antispam technologies offer minimal latency while providing a very low rate of false positives. Solutions deliver high throughput without significantly affecting system performance.

- Kaspersky's latest anti-phishing module also achieves high detection rates thanks to real-time updates from the cloud-based Kaspersky Security Network (KSN).

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- Kaspersky email security applications integrate with Kaspersky Anti Targeted Attack (KATA), which features file- and network-based threat detection engines, sandboxing and an event cross-correlation engine.

- Email traffic rules and support for OpenLDAP and Active Directory, help to implement corporate policies and give users the ability to set up their own personal blacklists/whitelists, as well as manage their own quarantined items.

- Reporting and monitoring facilities can be integrated with existing monitoring system (SNMP), or managed via the Kaspersky Security Center.

WEAKNESSES

- Kaspersky currently offers separate Email Security products for on-premises Microsoft Exchange and Microsoft Office 365. This creates complexity for customers which wish to manage hybrid scenarios. Kaspersky is working to address this as part of its roadmap.

- The Kaspersky Email Security solution for Microsoft Office 365 is currently less mature than its on-premises Email Security solution. The vendor is working to address this as part of its roadmap.

- Reporting can be improved as different Email Security solutions currently generate separate reports rather than a single consolidate report.

- Products for different platforms, e.g. Microsoft Exchange Server and Linux Mail Server, must be managed separately, centralized management from a single console is not available.

- Customers report that message rules processing is very basic, and could be improved.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

TREND MICRO

Shinjuku MAYNDS Tower, 1-1,
Yoyogi 2-Chome, Shibuya-ku
Tokyo, 151-0053, Japan
www.trendmicro.com

Founded in 1988, Trend Micro provides multi-layered email security solutions for organizations, service providers, and consumers. Its solutions are powered by the cloud-based Trend Micro Smart Protection Network, which brings together threat reporting and analysis based on a worldwide threat assessment infrastructure.

SOLUTIONS

Trend Micro offers a comprehensive line of email security solutions for enterprises that offer antivirus, antispam, anti-spyware, and anti-phishing, along with compliance and content filtering features. The email security solutions work in conjunction with the vendor's XGen Security functionality, which combines machine learning and other techniques, in order to protect against ransomware and advanced attacks. All email solutions integrate with Control Manager for central management and threat sharing with other security layers to improve visibility and overall protection. Trend Micro email security solutions are available as cloud or on-premises solutions in different packages, as follows:

Cloud-based Solutions:

- **Cloud App Security** – is a cloud-based advanced threat protection service that secures email and cloud sharing in Office 365, Box, Dropbox, and Google Drive.

- **Hosted Email Security** – is a cloud-based email gateway service that offers protection against spam, malware, phishing, ransomware, and advanced threats before they enter the customer network. It protects Microsoft Exchange, Microsoft Office 365, Google Gmail, and other hosted and on-premises email solutions.

- **Smart Protection for Office 365** – helps protect against email risks by combining Cloud App Security and Hosted Email Security. It helps prevent phishing attacks and offers antivirus, anti-malware, heuristics, and dynamic sandbox analysis to detect ransomware and

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

zero-day malware. It also provides DLP and advanced malware protection for OneDrive for Business, SharePoint Online, Box, Dropbox, and Google Drive.

- **Phish Insight** – is a free phishing simulation service that lets organizations test and educate employees on recognizing and avoiding phishing attacks.

On-premises Solutions:

- **Deep Discovery Email Inspector** – is an email appliance that provides advanced threat protection against targeted attacks.

- **InterScan Messaging Security** – is an on-premises gateway that defends against spam, malware, ransomware, and targeted email attacks.

- **ScanMail Suite for Microsoft Exchange** – offers mail server security for Microsoft Exchange protecting internal and external email against phishing, ransomware, and targeted attacks.

- **ScanMail Suite for IBM Domino** – offers malware and spam protection as a native IBM Domino server application.

- **Portal Protection for Microsoft SharePoint** – on-premises software for SharePoint server, providing antivirus, content filtering, and data loss prevention.

- **IM Security for Microsoft Skype for Business (now Teams)** – on-premises software to protect Skype and Lync instant messaging from malware, web threats, content violations and data loss.

Trend Micro offers a number of versions of its security solutions tailored to small, medium, and large organizations. Trend Micro also offers a stand-alone archiving and compliance solution.

STRENGTHS

- Trend Micro offers a comprehensive suite of security solutions in all form factors and a variety of different packages to fit the needs of customers of all sizes.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

- Trend Micro email security solutions are easy to deploy and manage.
- A stand-alone encryption solution is available for customers looking for extra security.

WEAKNESSES

- Trend Micro has done some re-naming and re-alignment of its email security portfolio to fit with its XGen branding, however, its solutions are showing signs of aging and don't seem to be updated as frequently as those of its competitors.
- Basic, policy-based DLP is available, but only at an extra cost.
- Trend Micro sells email security in a variety of packages, but not all its email security solutions integrate fully with Advanced Threat Prevention (ATP) for real-time threat correlation.
- Trend Micro email solutions track url usage, but do not support preventive actions such as url replacement or quarantining.
- Customers we interviewed as part of this research, indicated that administration and policy setup for Trend Micro email security solutions is somewhat lacking and could be improved, particularly for hybrid gateway scenarios.

MICROSOFT

1 Microsoft Way
Redmond, WA 98052
www.microsoft.com

Microsoft provides a broad range of products and services for businesses and consumers, with an extensive portfolio of solutions for office productivity, messaging, collaboration, and more.

SOLUTIONS

Microsoft Exchange Online Protection (EOP) is Microsoft's email security solution which is an integral part of Microsoft Office 365. It helps protect against spam and malware, and includes

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

features to safeguard organizations from messaging-policy violations. It does not require client software installation, but is activated by changing the customer's MX record. It can be deployed in the following scenarios:

- *Standalone* – where it provides cloud-based email protection for on-premises Microsoft Exchange Server 2013 environments, legacy Exchange Server versions, and any other on-premises SMTP email solution.

- *Microsoft Exchange Online* – EOP is an integral part of Microsoft Exchange Online which is the email service component of Office 365.

- *Hybrid* – EOP can be configured to protect and control email routing in a mixed environment of on-premises and cloud mailboxes.

Customers can add **Office 365 Advanced Threat Protection (ATP)**, **Data Loss Prevention (DLP)**, and **Office 365 Message Encryption** for a more fully featured security solution.

- **Advanced Data Protection (ATP)** – provides protection against phishing, malware and spam attacks. It also offers near real-time protection against high-volume spam campaigns, with DKIM and DMARC support. It can protect against "zero-day" attachments and harmful URL link, through real-time behavioral analysis and sandboxing. It supports spoofing intelligence to detect and block outbound or inbound spoofing attempts. Messages identifies as spam, bulk mail, phishing mail, containing malware, or matching pre-set email flow rules are quarantined and can be reviewed and acted upon by authorized users. ATP is included free of charge in Office 365 Enterprise E5, Office 365 Education A5, and Microsoft 365 Business plans. It can also be to a number of other plans at an extra charge.

- **Data Loss Prevention (DLP)** – capabilities are available natively in the Office client and SharePoint Online and OneDrive for Business. The Microsoft Compliance Center provides a central policy management console that allows administrators to manage DLP policies across different services. Data Loss Prevention is a premium feature that requires an Enterprise Client Access License (CAL).

- **Office 365 Message Encryption** – allows users to send encrypted messages to other users inside or outside their organization, regardless of the email service in use e.g. Outlook.com, Yahoo, Gmail, or other. Designated recipients of encrypted messages to enter a simple one-

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

time passcode to read it and can send encrypted replies. Office 365 Message Encryption combines email encryption and rights management capabilities, powered by Azure Information Protection. New mobile apps for iOS and Android also allow viewing of encrypted messages on mobile devices.

STRENGTHS

- Microsoft Exchange Online Protection and add-on services for ATP, DLP and encryption come mostly native, free of charge with many Microsoft Office 365 plans. Where an additional fee is required it is usually very small.

- Microsoft is investing heavily to address threats posed by spam, spoofing, phishing attacks, as well as blended attacks through attachments and harmful URLs.

- Microsoft Exchange Online Protection and Advanced Threat Protection solutions are easy to deploy, and administer for customers of all sizes.

WEAKNESSES

- While Microsoft has been investing heavily in its anti-malware, antispam, phishing, spoofing and zero-day protection capabilities, customers still report high degrees of spam, malware and other forms of attack. Most customers tend to deploy additional email security solutions from other security vendors.

- Microsoft offers many different plans at different price points, but it is sometimes difficult for customers to understand exactly what security features they are getting with what plans.

- Microsoft customers we spoke to as part of this research, often indicated that Microsoft's customer support organization is not sufficiently knowledgeable when it comes to security issues.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

THE RADICATI GROUP, INC.
http://www.radicati.com

The Radicati Group, Inc. is a leading Market Research Firm specializing in emerging IT technologies. The company provides detailed market size, installed base and forecast information on a worldwide basis, as well as detailed country breakouts, in all areas of:

- **Email**
- **Security**
- **Compliance**
- **Instant Messaging**
- **Unified Communications**
- **Mobility**
- **Web Technologies**

The company assists vendors to define their strategic product and business direction. It also assists corporate organizations in selecting the right products and technologies to support their business needs.

Our market research and industry analysis takes a global perspective, providing clients with valuable information necessary to compete on a global basis. We are an international firm with clients throughout the US, Europe and the Pacific Rim. The Radicati Group, Inc. was founded in 1993.

Consulting Services:

The Radicati Group, Inc. provides the following Consulting Services:

- Management Consulting
- Whitepapers
- Strategic Business Planning
- Product Selection Advice
- TCO/ROI Analysis
- Multi-Client Studies

To learn more about our reports and services, please visit our website at www.radicati.com.

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited

MARKET RESEARCH PUBLICATIONS

The Radicati Group, Inc. develops in-depth market analysis studies covering market size, installed base, industry trends and competition. Current and upcoming publications include:

Currently Released:

Title	Released	Price*
Microsoft SharePoint Market Analysis, 2018-2022	Jun. 2018	$3,000.00
Corporate Web Security Market, 2018-2022	Jun. 2018	$3,000.00
Email Market, 2018-2022	Jun. 2018	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2018-2022	Jun. 2018	$3,000.00
Cloud Business Email Market, 2018-2022	Jun. 2018	$3,000.00
Information Archiving Market, 2018-2022	Mar. 2018	$3,000.00
Unified Endpoint Management Market, 2018-2022	Mar. 2018	$3,000.00
Advanced Threat Protection Market, 2018-2022	Mar. 2018	$3,000.00
Email Statistics Report, 2018-2022	Mar. 2018	$3,000.00
Social Networking Statistics Report, 2018-2022	Feb. 2018	$3,000.00
Instant Messaging Statistics Report, 2018-2022	Feb. 2018	$3,000.00
Mobile Statistics Report, 2018-2022	Jan. 2018	$3,000.00

*** Discounted by $500 if purchased by credit card.**

Upcoming Publications:

Title	To Be Released	Price*
Endpoint Security Market, 2018-2022	Nov. 2018	$3,000.00
Secure Email Gateway Market, 2018-2022	Nov. 2018	$3,000.00
Enterprise Data Loss Prevention Market, 2018-2022	Nov. 2018	$3,000.00
Cloud Access Security Broker Market, 2018-2022	Nov. 2018	$3,000.00

*** Discounted by $500 if purchased by credit card.**

All Radicati Group reports are available online at http://www.radicati.com**.**

Copyright © October 2018, The Radicati Group, Inc. Reproduction Prohibited