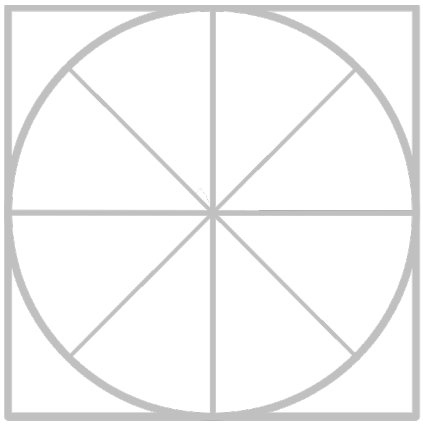
The Radicati Group, Inc.
Palo Alto, CA 94301
Phone: (650) 322-8059
www.radicati.com

THE RADICATI GROUP, INC.

Secure Email Gateway - Market Quadrant 2016



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

November 2016

Radicati Market Quadrant[SM] is copyrighted November 2016 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[SM] 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[SM] 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 *32*

==========

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 a niche product.

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 © November 2016, 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.

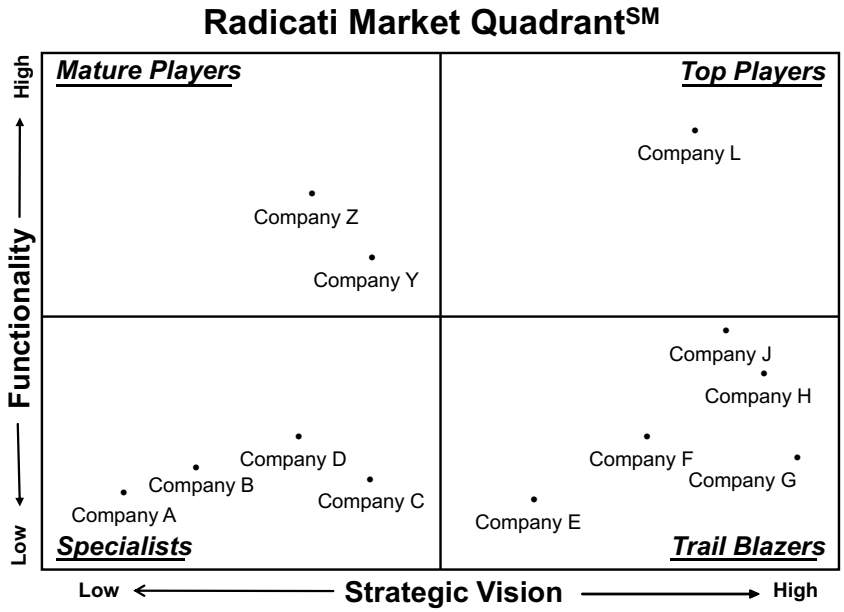


Figure 1: Sample Radicati Market Quadrant

Copyright © November 2016, 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, Forcepoint, Fortinet, Kaspersky Lab, Microsoft, Mimecast, Proofpoint, SonicWALL, Sophos, Symantec,* and *Trend Micro*.

- Secure Email Gateways, today, can be deployed in multiple form factors, including appliances, virtual appliances, cloud services and hybrid models.

- Some Secure Email Gateway vendors target both corporate customers, as well as service providers. However, this report looks only at solutions in the context of their corporate business, ranging from SMBs to very large organizations.

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

- The Secure Email Gateway market is fairly mature, due to the early recognition of email as a leading vector for malware attack and penetration. However, this market is seeing renewed investment and innovation due to the evolving complexity of email-borne threats and the critical importance of feeding email attack/malware detection information to broader enterprise-wide security services (e.g. ATP, endpoints, and more).

- The worldwide revenue for Secure Email Gateway solutions is expected to grow from nearly $1.7 billion in 2016, to over $1.9 billion by 2020.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

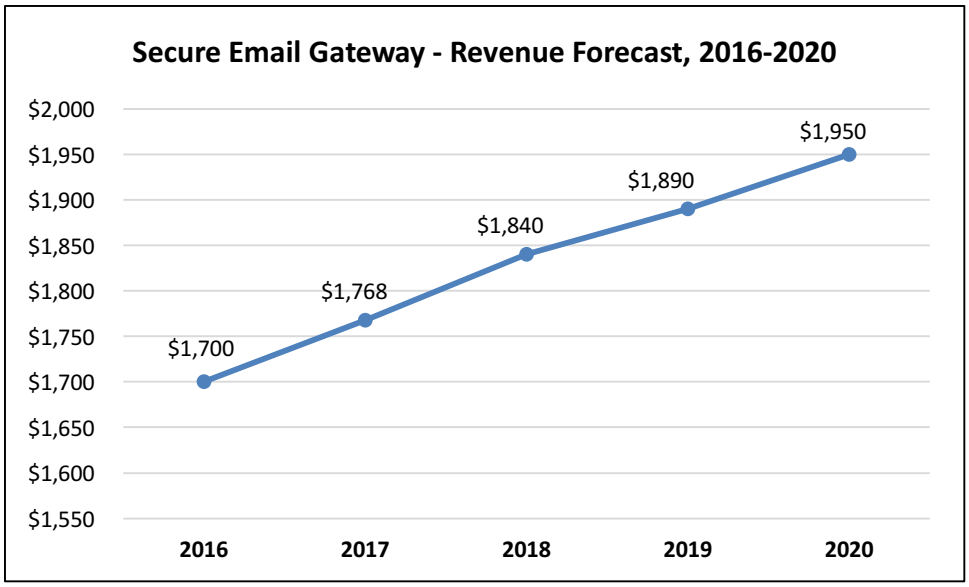


Figure 2: Secure Email Gateway Revenue Forecast, 2016 – 2020

Copyright © November 2016, 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.

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

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

- ***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, endpoints, and more).

- ***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:

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

- *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 © November 2016, The Radicati Group, Inc. Reproduction Prohibited

MARKET QUADRANT – SECURE EMAIL GATEWAY

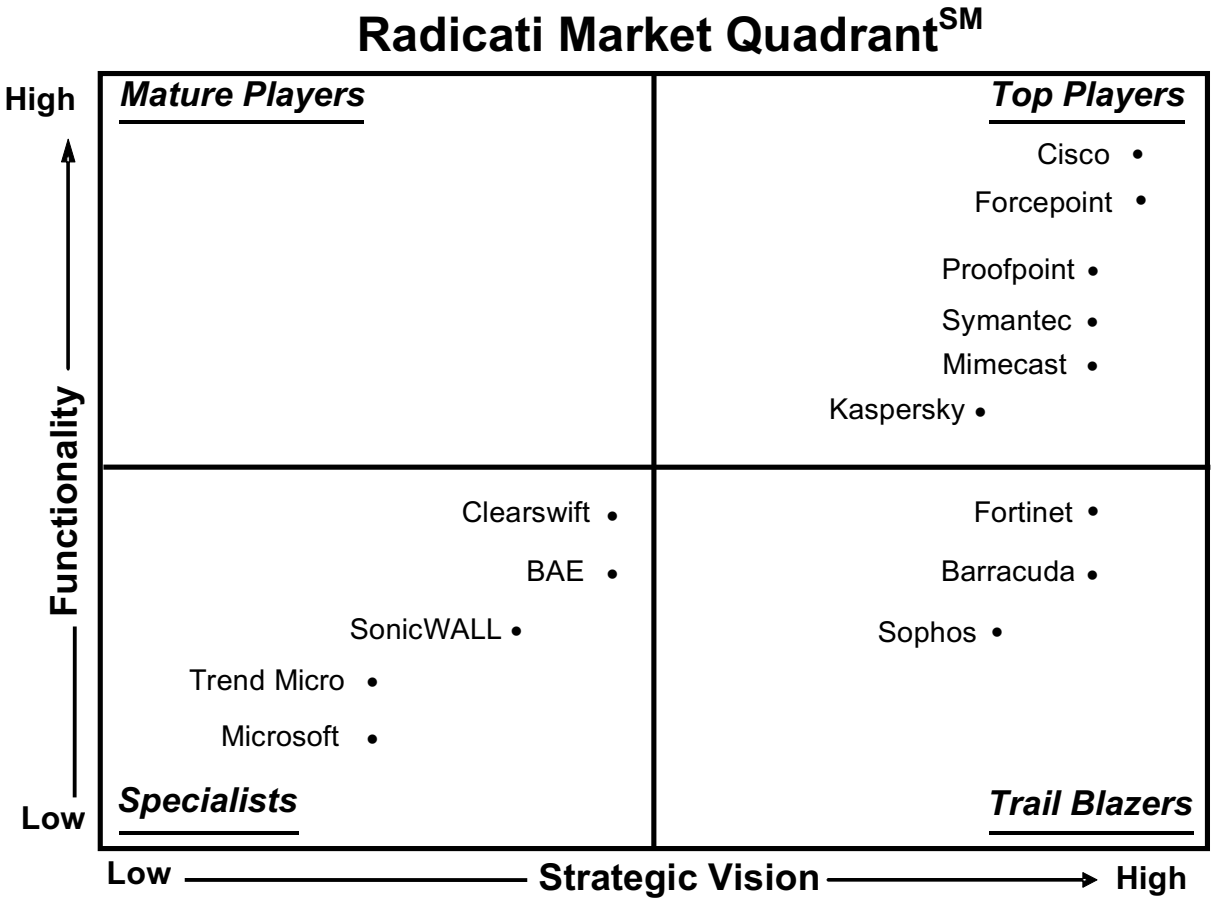


Figure 3: Secure Email Gateway Market Quadrant, 2016

· Radicati Market Quadrant℠ is copyrighted November 2016 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 © November 2016, The Radicati Group, Inc. Reproduction Prohibited

KEY MARKET QUADRANT HIGHLIGHTS

- The **Top Players** in the market are *Cisco, Forcepoint, Proofpoint, Symantec, Mimecast* and *Kaspersky Lab.*
- The **Trail Blazers** quadrant includes *Fortinet, Barracuda,* and *Sophos*.
- The **Specialists** quadrant includes *Clearswift, BAE Systems, SonicWALL, 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. In 2014, Cisco acquired ThreatGRID, which offers a cloud-based malware analysis and on-premises sandboxing appliance. In 2015, Cisco acquired OpenDNS, which offers a cloud-delivered network security service that protects at the DNS layer, and in May 2016, it acquired CloudLock, a cloud access security broker (CASB) platform that extends security to SaaS applications. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos) which is made up of more than 250 leading threat researchers.

SOLUTIONS

Cisco Email Security protects organizations from ransomware, email spoofing, advanced malware and other threats with simple, open, automated, and effective security across the entire

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

attack continuum. It is available in four form-factors, as follows:

- Cloud Email Security (CES)
- Email Security Appliance (ESA)
- Virtual Email Security Appliance (ESAv)
- Hybrid

All deployment options have feature parity. Cisco Email Security supports customers across all segments, with subscriptions starting as low as 100 users with the same features and deployment options available to customers of all sizes. Also, 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:

- **Antispam** – multi-layered defense which combines reputation filtering and sender verification. Cisco also offers advanced graymail handling capabilities, including a safe-unsubscribe link that recipients can use confidently. Cisco also has "always on" Adaptive Rules that reside on-box, inside the Context Adaptive Scanning Engine (CASE). Adaptive Rules have finely tuned heuristics that look for known characteristics of malware and viruses, such as the use of extension spoofing and malformed headers. Adaptive Rules are monitored, tested and optimized by Cisco to protect against the evolving techniques of virus writers and are updated regularly.

- **Antivirus** – multi-layer signature based antivirus protection is offered through Sophos and/or Intel (McAfee) antivirus engines. Customers can run both antivirus engines in tandem to dual-scan messages for more comprehensive protection. After emails are scanned with traditional detection methods, they are sent through virus Outbreak Filters to look for emerging viruses such as zero-day malware. Virus Outbreak Filters quarantine unknown messages and continually check against the latest threat intelligence to determine if a file is malicious.

- **Reputation filtering** – inbound connections are dropped, throttled or permitted depending on the sending domain's SenderBase Reputation Score (SBRS), maintained by Talos. SBRS is based on more than 200 parameters, including email volume, domain blacklists and safelists,

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

registration dates and when the domain started sending mail.

- **Attachments** – Cisco Email Security offers multiple layers of protection to block hidden threats within attachments.

- **Advanced Malware Protection (AMP)** – consists of three 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. AMP then combines that data with detailed human and machine analysis to determine the file's threat level in a sandbox. Based on the verdict of the analysis, the email is released from quarantine or deleted.

  - *File Retrospection* – deals with the problem of malicious files that pass through perimeter defenses, but are subsequently deemed a threat. When a breach occurs, customers can see where the file traveled in their environment to begin remediation quickly. Cisco also offers malware auto-remediation for Office 365, where customers can configure the Cisco Cloud Email Security solution to perform auto-remedial actions on the messages in users' mailboxes when a threat verdict changes.

- **URL protection** – Cisco offers deep inspection of URLs due to integration with its Web Security portfolio and two other detection methods:

  - *Content Filters* – are customizable filters that enable customers to control what enters the network. Different options allow to control URLs, such as rewriting or blocking based on their reputation and/or web categorization, or replacing the hyperlink with text (such as "This URL is blocked by policy").

  - *Outbreak Filters* – if an incoming email contains a suspicious URL, Outbreak Filters will look more closely into the context and construction of the message to determine whether it is a harmful site. If a URL remains unknown, the email will be released in a rewritten form to protect the end user.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

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

- **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. An executive name violation is copied into the message's X-header and replaced with the external sender's address. This process serves to document the fraud and warns the recipient of the external sender's action. Executive name violations are included in admin reports that list: the abused Executive Name, how many messages have targeted that name and a link to message tracking that specifies the internal recipients of that fraud.

- **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.

- **Encryption** – is available through two products which cover the breadth of use cases including push, pull, transparent secure delivery and S/MIME. On-premises key storage encryption is provided through the use of Zix Corporation's ZixGateway solution; while cloud key storage encryption is provided through the Cisco Registered Envelope Service (CRES).

STRENGTHS

- Cisco's Email Security solutions can be deployed as appliances, cloud-based, network integrated, or hybrid solutions.

- 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 leverages multi-layer defense that combines multiple techniques, such as big data analytics harvested from signature-based analysis, reputation services and behavioral analytics to ensure thorough risk analysis with low false positives.

- Additional strengths include Cisco's Advanced Malware Protection (AMP) which helps monitor and reconstruct all stages of a file's network traversal, as well as its deep URL

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

inspection techniques.

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

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 Apps for Work.

- Cisco needs to work to extend the integration of its Email Security solutions with other components of its security portfolio, such as Identity Services Engine, Cognitive Threat Analytics and AMP for Endpoints. 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. Cisco is working to address this by introducing consumption-based billing models for Cloud Email Security. Cisco also has a dedicated Office 365 offering, which is aimed at budget-conscious small and medium businesses.

- While Cisco's Cloud Email Security (CES) solution is aimed at customers with 100 seats or more, it may be missing some opportunities by not also targeting customers with smaller seat counts.

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. Forcepoint offers Web,

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

data, and email content security, user behavior analysis, and threat protection solutions to organizations of all sizes.

SOLUTIONS

TRITON AP-EMAIL, part of Forcepoint's TRITON APX solution suite, delivers security by protecting against multi-stage advanced threats that often exploit email to penetrate the IT environment. It applies real-time behavioral sandboxing, enterprise-grade DLP and other advanced defense technologies to identify targeted attacks, high-risk users and insider threats. TRITON AP-EMAIL monitors outbound email to prevent leaks of sensitive information, and it enables workers to safely adopt technologies like Microsoft Office 365.

TRITON AP-EMAIL is powered by Forcepoint's TRITON ACE and ThreatSeeker Intelligence Cloud, which work together in real time to identify and classify network traffic, apply policies and detect threats. Unified management and reporting functions streamline work for security teams, helping them minimize the dwell time of attacks and prevent the exfiltration of data. Forcepoint's common TRITON APX architecture also makes it simple to deploy TRITON AP-EMAIL separately, or in any combination with TRITON AP-WEB, TRITON AP-DATA and TRITON AP-ENDPOINT.

TRITON AP-EMAIL is available in the following form factors:

- *AP-EMAIL* – which is the on-premises gateway-based email security core solution.

- *AP-EMAIL Hybrid* – is the hybrid gateway-based email security core 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.

- *AP-EMAIL Cloud* – is the pure cloud-based solution.

Additional modules that can be added to TRITON AP-EMAIL include:

Email DLP Module (included as either cloud-based or on-premises based) – the Forcepoint DLP Module enables organization to discover and protect sensitive data in the cloud or on-premises. Custom or out-of-the-box policies, help secure personal data, intellectual property and meet compliance requirements quickly.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

Email Encryption Module (cloud based) – provides advanced push-based encryption. 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 the organization's policies.

Threat Protection Cloud Module (cloud based) – offers a scalable, easy-to-deploy sandbox solution that integrates seamlessly with TRITON® AP-WEB and TRITON AP-EMAIL on-premise, cloud, or hybrid deployment options.

STRENGTHS

- Forcepoint's TRITON AP-EMAIL is available in a variety of form factors, giving customers a complete breadth of email security deployment options.

- Forcepoint TRITON AP-EMAIL offers strong outbound email protection with integrated enterprise-class DLP functionality.

- Forcepoint TRITON AP-EMAIL can leverage strong malware detection benefits as part of the TRITON security platform which integrates email security, web security and DLP from a cohesive platform.

- Forcepoint TRITON AP-EMAIL offers strong protection for Microsoft Office 365 with regards to both inbound and outbound email security.

WEAKNESSES

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

- The Forcepoint TRITON AP-EMAIL solution is somewhat more expensive when compared to others in the space, particularly when fully integrated with other TRITON APX offerings.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

- Forcepoint TRITON solutions tend to be aimed mainly at the complex needs of mid-size and large customers, although AP-EMAIL cloud may be a good fit for smaller businesses and SMBs.

PROOFPOINT

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

Proofpoint is a next-generation security and compliance company that delivers solutions for inbound email security, outbound data loss prevention, privacy protection, email encryption, eDiscovery, and email archiving.

SOLUTIONS

Proofpoint offers email security solutions with capabilities for email filtering, analysis and classification, advanced threat protection, email authentication and information protection. Proofpoint offers a choice of deployment options which include: cloud service, dedicated appliance, virtual appliance or a hybrid deployment. Customers also have the ability to select different deployment options for particular services, for instance stopping inbound threats in the cloud, while enforcing DLP policy on-premises.

Proofpoint Email Protection – available as an on-premises or cloud based solution, serves to block unwanted, malicious and impostor (business email compromise) email, with granular search capabilities and visibility into all messages. It offers the following capabilities:

Targeted Attack Protection – analyzes all URLs and attachments both statically and dynamically in Proofpoint's cloud-based sandbox, accurately identifying both widespread attacks (such as Dridex, Locky & Ursnif) as well as highly targeted attacks (such as credential phishing). Proofpoint has added DMARC visibility for advanced email spoofing protection.

Outbound information protection – controls include encryption and data loss prevention, to protect against the loss of private or sensitive data.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

Email continuity capabilities – ensure business communications can continue as normal in the event of an email outage.

Response capabilities – include the ability to automatically remove potentially malicious email from an end user inbox, as well as other actions such as blacklisting IP addresses and quarantining an infected endpoint.

STRENGTHS

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

- Proofpoint Email Protection offers flexibility for policy creation allowing organizations to define the rules that they need for email control and routing. The availability of predefined policies for threats help ensure that organizations are secure as soon as they start to use the product.

- Proofpoint provides extensive reporting with visibility into: email flow and deliverability, message tracing, DLP events, threats, impacted victims and threat forensics to help understand where threats may be originating. DLP events are displayed in a dashboard with prioritization so administrators know which events to investigate.

- Proofpoint can also scan and sandbox SSL encrypted websites to identify malicious behavior including malware and credential phishing. Proofpoint also supports TLS encryption for server-to-server security.

- Proofpoint offers full directory integrations across a wide range of different directory technologies. Proofpoint emails policy based rules and routing based on user group to help customers enforce policy with minimal management overhead.

- Proofpoint offers its own DLP functionality integrated into the email gateway. Administrators can quickly and easily create DLP rules minimizing the time to value for protecting data via email.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

WEAKNESSES

- Proofpoint offers a best-in-breed secure email gateway solution and strong threat detection, 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 solutions are a best fit for mid-size and large organizations, SMBs will find the solutions somewhat pricey and overly feature-rich for their needs.

- Proofpoint solutions are best known in North America, the company could work to improve its international presence.

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 one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

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 Apps, hosted mailboxes and traditional on-premises email systems, such as Microsoft Exchange. Symantec Email Security.cloud blocks targeted attacks, spear phishing, viruses and malware, business email compromise attacks, spam, and bulk mail with anti-malware and antispam services. In addition, it 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 © November 2016, 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 the Symantec Cynic™ cloud-based sandboxing and payload detonation capabilities to identify and stop complex targeted and advanced threats, including attacks that are virtual machine-aware. Advanced Threat Protection: Email also provides detailed data on targeted attacks that attempt to enter an organization via email, as determined by Symantec research analysts. The solution provides deep threat intelligence on targeted and advanced threats, including URL information, file hashes, and targeted attack information. The data can easily be exported to a third-party Security Incident and Event Management (SIEM) solutions.

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

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 offers effective, accurate threat protection with low false positives through the use multi-layered detection technologies, such as Skeptic 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 such URL information, file hashes, and targeted attack information to customers. In addition, integration with SIEM solutions enables security analysts to easily correlate threats across multiple security products.

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

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

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

WEAKNESSES

- Following the Blue Coat acquisition, Symantec is still in the process of integrating Email Security.cloud and Messaging Gateway with Blue Coat products such as Content Analysis System (CAS) and Malicious Analysis Appliance (MAA), as well as the Blue Coat Global Intelligence Network.

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

- In the past, customers reported issues with Symantec's customer support organization. Following on from the recent company re-focusing and Blue Coat acquisition, Symantec is working to address this.

MIMECAST

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

Mimecast is a provider of cloud-based email and information management services for businesses. The core of Mimecast's services, include: email security, continuity and archiving services. Founded in 2003, Mimecast is headquartered in London, UK, and has offices in the US, Australia, and South Africa. Mimecast is a publicly traded company.

SOLUTIONS

Mimecast Email Security protects against malware, spam, advanced phishing and other emerging and targeted attacks, while preventing data leaks. Mimecast also offers services for Mailbox Continuity and Enterprise Information Archiving which can be delivered as an

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

integrated bundle with Email Security. Mimecast services are provided as a cloud-based service, hosted in their global data centers.

Mimecast employs a multi-layered approach for spam and malware blocking, which relies on a mix of established AV engines, reputation lists, and its own proprietary heuristics to provide AV and AS filtering.

Mimecast offers a single integrated administrative system complete with templates and customizable policies that enables administrators to monitor, 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 outbound emails offer breakdowns showing which DLP policy was triggered, by whom and what action was applied. In addition, Mimecast provides an API and integration with SIEM systems (such as Splunk) to enable data integrations from systems of the customer's choosing.

Mimecast Targeted Threat Protection extends traditional gateway security (AS/AV) to defend against malicious links in email, weaponized attachments and malware-less social-engineering attacks, often called whaling or impersonation. Real-time scanning and blocking of suspect websites and attachment sandboxing prevent employees from inadvertently downloading malware or revealing credentials. Inbound emails are also inspected for the detection of impersonations which are often solicitations related to financial fraud. Dynamic user awareness capabilities reinforce email security policies and engage employees in assessing risks on an ongoing basis.

STRENGTHS

- Mimecast offers a single integrated solution which can deliver email security, continuity, and archiving. This combination can be particularly useful when dealing with potentially destructive attacks, such as ransomware.

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

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

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

- Mimecast's solution integrates with the customer's Active Directory (AD) environment 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. Also AD information is used to accept/deny received emails compared with known good email addresses.

- Mimecast offers DLP capabilities based on Mimecast's own technology (available in its "D1 DLP and Content Security" package) which provide security and compliance for outbound emails. Mimecast added a fuzzy hashing capability which scores attachments based on content and enables administrators to apply rules which leverage scores to make block/allow/encrypt decisions on outbound emails.

WEAKNESSES

- Mimecast tends to bundle its email security solution with email continuity and information archiving. While this is useful for some customers, it does not satisfy the needs of those customers who may be seeking an email security solution that integrates with endpoint and mobile security.

- Mimecast needs to work to improve automation of deployment and initial configuration of new customers.

- Mimecast is working to add security inspection capabilities for emails which are purely internal.

- Mimecast is working to increase the capabilities of the DLP portion of the service for outbound emails.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

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 with offices in 30 different countries.

SOLUTIONS

Kaspersky Security for Mail solutions, including Kaspersky Security for Microsoft Exchange, Linux-based mail servers and IBM Lotus Domino provides protection from spam, phishing, generic and advanced malware threats, even in the most 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. Integrated as a mail gateway or relay, the virtual appliance provides a complete solution for securing in-and-outbound mail from malware, spam, phishing and zero-day threats.

- **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 complete protection and centralized management of all Microsoft Exchange servers in a corporate environment. In addition to anti-malware, antispam and anti-phishing, the solution provides data loss

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

protection and control functionality: outgoing emails are analyzed and messages or attachments that contain confidential corporate data or sensitive information are automatically registered – and can also be automatically blocked. The add-on DLP module contains predefined glossaries for main compliances including HIPAA, PCI DSS and many more. 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.

STRENGTHS

- Kaspersky Lab's Secure email solutions include advanced spam detection technologies that help to minimize the number of spam messages that get through email system 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).

- 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's email security solutions are available as virtual appliances, but are not available as cloud solutions.

- Kaspersky Labs does not currently provide an email security solution for Microsoft Office 365, however this is on the roadmap for 2017.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

- Integration with Kaspersky's anti-APT/sandbox solution is not yet available, but is planned for its next release.

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

- End-user encryption capabilities is not available, but can be provided through third-party solutions.

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

TRAIL BLAZERS

FORTINET

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

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

SOLUTIONS

Fortinet's **FortiMail** is 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, anti-malware, sandboxing, data leakage prevention (DLP), identity based encryption (IBE), and message archiving.

FortiMail is available in a broad range of form factors, including: a line of 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 © November 2016, The Radicati Group, Inc. Reproduction Prohibited

FortiMail integrates with other Fortinet security solutions 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 it address the complex deployment needs of a broad range of customers.

- FortiMail is an all-in-one solution offering which comprises advanced data protection features, such as DLP, Encryption and Archiving within its "core" threat prevention capabilities.

- 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.

- FortiMail would benefit from further improvements in its threat containment techniques, such as neutralization of active content in Office and PDF documents.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

BARRACUDA NETWORKS

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

Founded in 2003, Barracuda Networks operates in three distinct markets, including: content security; networking and application delivery; and data storage, protection and disaster recovery. Barracuda Networks is a publicly traded company.

SOLUTIONS

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

Barracuda Essentials – a fully cloud-based email security solution that combines several layers of protection for inbound and outbound email to secure against the most advanced email borne attacks, and email spooling to ensure business continuity.

Barracuda provides its own technology combined with open source technology to offer a multi-layered antispam protection approach that involves connection management including rate control, IP reputation including RBLs, sender and recipient authentication and content scanning policies including attachment filters, URL/image investigation, custom policies, and more.

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, attachment or using Barracuda's pre-defined filters.

Barracuda's email security solutions 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.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

Barracuda's Advanced Threat Detection (ATD) combines behavioral, heuristic, and sandboxing technologies to protect against zero hour and targeted attacks. ATD 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 their products in a central user interface.

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 email security solutions do not yet support DMARC, a capability which has become increasingly common with most secure email gateway vendors for combating phishing attacks.

- While Barracuda offers sandboxing, its Advanced Threat Prevention (ATP) capabilities are not as advanced as those of other vendors.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

SOPHOS

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

Sophos offers a variety of mid-market security solutions, including encryption, endpoint security, web, email, mobile and network security solutions are backed by SophosLabs, its global network of threat intelligence centers. The company is headquartered in Oxford, U.K., and is publicly traded on the London Stock Exchange.

SOLUTIONS

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

- **Sophos Email** – is a secure cloud email gateway designed to protect against spam, phishing, malware and data loss. It also enables customers to control of email security alongside endpoint, mobile, web, and wireless protection through Sophos Central's single interface.

- **Sophos Email Appliance** – is an all-in-one solution for email encryption, DLP, antispam and threat protection, providing advanced protection from spear phishing attacks. It can integrate with Sophos Sandstorm cloud sandbox for advanced threat protection. Sophos uses its own DLP engine and Content Control Lists which is available at no extra cost in its Email Appliance. Encryption also comes at no extra cost in Sophos Email Appliances.

Sophos uses its own technology for antivirus scanning. However, for antispam it uses a mix of its own plus third party technology were necessary. In addition, Sophos has data sharing agreements between threat protection labs that enhance its antivirus and antispam effectiveness.

The Sophos Central management console allows customer to manage multiple products alongside Sophos Email in the cloud. Sophos also provides integration between Sophos protected endpoints and its email solutions. Customers can enforce the same policy and required level of data protection for endpoints and at the gateway, which greatly eases administration.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

Sophos' plans to integrate its Email security solutions with its Synchronized Security approach to more efficiently stop malware distribution or data leakage in real-time.

STRENGTHS

- Sophos solutions integrate with Sophos Sandstorm, which provides cloud-based sandboxing complementing Sophos's traditional malware and threat detection technology to detect unknown threats designed to evade first-generation APT sandbox appliances.

- Sophos offers Time-of-Click protection to blocks malicious email URLs in order to protect against stealthy, delayed, spear phishing attacks. Whenever an email link is clicked, on any device, its URL reputation is checked against Sophos' cloud-hosted database.

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

- Sophos offers a central management interface which allows administrators to have complete control over all security features in one place, as well as offers integrated protection across other Sophos security offerings.

- Sophos email security solutions while feature-rich, are attractively priced for small and mid-size customers.

WEAKNESSES

- Sophos Email security solutions don't current integrate with its email archiving and email continuity offerings, however, Sophos plans to add this in the 2017 timeframe.

- Sophos currently offers encryption as a standard feature with its Email Security Appliance, but not as part of its email cloud offering. However, the company has this on its future roadmap.

- Sophos Synchronized Security offers sophisticated threat discovery, investigation, and response, however it does not yet integrate with its Email Security solutions. The company plans to add this capability in future releases.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

- Sophos's cloud-based and appliance-based email security solutions offer very different levels of functionality, customers should check carefully to determine which solution best fits their protection needs.

- Sophos Email security solutions are best suited for small and medium sized businesses, looking for ease of use and ease of administration.

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.

SOLUTIONS

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

The Gateway protects customers from new and existing malware using a combination of dual antivirus engines from Sophos and/or Kaspersky. Both 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 active code in html, Office, PDF and OpenOffice and optionally remove them, allowing a safe document to be delivered to the recipient.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

Antispam detection is provided by a layered solution utilizing IP reputation, greylisting, anti-spoofing, RBL, SPF, DKIM, sender validation and spam signatures and offers 99%+ spam detection with reliability.

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 3rd party technologies and allows the Clearswift solution to modify the data, for example redacting and sanitizing of 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.

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). Sanitization can also remove potentially embarrassing change tracking comments which may carry data which could represent a data leak.

Structural Sanitization works on active code carrying files such as HTML, Office, PDF and OpenOffice. These file can carry VBA, ActiveX, Javascript and OLE objects which could be used to launch an attack on a message recipient. The Gateway can detect and/or strip the active code from the file and deliver a safe version.

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 approach with can be used in both push and pull modes.

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

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

STRENGTHS

- Clearswift's SECURE email gateway is available in a variety of form factors to help meet diverse customer needs.

- Clearswift offers Adaptive Redaction features in all its Gateway product. 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'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 just license additional DLP features as required on-top of the base hygiene product).

WEAKNESSES

- Clearswift solutions would benefit from integration with sandboxing solutions.

- Clearswift does not currently offer URL sanitation or DMARC support. However, the vendor has this on their roadmap for future releases.

- Clearswift currently lacks the ability to scan internal Office365 traffic, but does scan Office 365 traffic that crosses the organizational boundary.

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

Copyright © November 2016, 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 Office 365. 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:

- **BAE Systems' Zero Day Protection** – uses a combination of static and dynamic analysis to catch advanced malware. It relies on proprietary live browser analysis technology and instrumented application methods to isolate and defeat attempted attacks that traditional sandbox scanning may miss. Zero Day Prevention also includes click-time protection which provides real-time detection and blocking capabilities to protect against malicious links.

- **BAE Systems Insider Threat Prevention** – solution 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 check for DMARC authentication checks which may indicate potential Business Email Compromise. This automatic policy enforcement protects against disgruntled employees, as well as accidental leakage as a result of a genuine mistake by those who are not aware of data privacy requirements. Insider Threat Prevention also includes industry-specific policy packs to help customers in highly regulated markets with the compliance of GLBA, HIPAA, and PCI DSS for best-in-class policy management and hardened protection against information loss.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

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

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

- **BAE Systems' Email Compliance Archiving** – provides tamper-proof compliance arching and eDiscovery capabilities to retrieve messages.

- **BAE Systems' 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 Zero Day Protection, Insider Thread Prevention, and Web Security.

STRENGTHS

- BAE Systems offers a full suite of cloud-based email security solutions that provide complete control over inbound and outbound corporate messaging.

- BAE Systems leverages what it calls "Instrumentation", which allows it to spot events leading up to an exploit as opposed to sandboxing which relies merely on observing behavior once a payload is deployed. This offers stronger defense against sandbox-aware malware.

- 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.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

- BAE Systems offers policy-based email encryption 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 3rd 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 entirely on cloud-based security.
- BAE Systems' EPS does not provide any form of Directory Harvest Attack (DHA) detection, or Denial of Service (DoS) detection which are commonly provided by most competing secure email gateway solutions.
- BAE Systems Threat Analytics does not provide sandboxing, relying instead mainly on heuristics to detect complex threats.
- Customers have indicated that administrative reporting features are rather basic.

SONICWALL

5455 Great America Parkway
Santa Clara, CA 95054
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 part of Dell Software Group from 2012 to 2016, In June 2016, Dell sold SonicWALL to private equity firm Francisco Partners and Elliott Management.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

SOLUTIONS

SonicWALL Email Security offers solutions that deliver protection from spam, phishing and viruses, in the following form factors:

- *Hosted Email Security* – delivers cloud-based protection from inbound and outbound threats – including spam, phishing, zombie attacks and malware.
- *Email Security Appliances* – safeguard inbound and outbound email on a single, or cluster of, system(s). 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* – receives 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 onto 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 offers DLP through a policy & compliance engine that can be used to protect sensitive records from being emailed outside the organization, including Record ID matching, policy dictionaries, and more.

Email Encryption is integrated in the products, and is available as a separately licensed component.

STRENGTHS

- SonicWALL Email Security offers robust, longstanding expertise with email security and management technologies, including: antivirus, antispam, phishing, policy and compliance, encryption, and sandboxing in a variety of form factors that fit a diverse set of customer

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

needs.

- SonicWALL leverages its GRID Network, a dedicated malware research team developing new spam signatures and detection techniques, based on data collected from SonicWALL's appliances.

- SonicWALL Email security supports DMARC, DKIM, and SPF message handling and reporting.

WEAKNESSES

- SonicWALL plans to release refreshed, new hardware for its appliance based solutions.

- SonicWALL needs to achieve tighter integration with sandboxing technologies across its product portfolio.

- SonicWALL needs to add improved email archiving and continuity capabilities.

- SonicWALL DLP capabilities are rather basic when compared with other vendors in this space.

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 home users. 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.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

SOLUTIONS

Trend Micro's **InterScan** suite is a comprehensive line of security solutions for enterprises that offer antivirus, antispam, anti-spyware, and anti-phishing, along with compliance and content filtering features. InterScan solutions are available in a number of different form factors and packages, including:

- **InterScan Messaging Security Virtual Appliance –** protects against spam, viruses, spyware, phishing, blended attacks and data loss. Supports VMware ESX or ESXi.

- **InterScan Messaging Security Software Appliance** – same protection as virtual appliance for bare metal installation with tuned, security-hardened OS.

- **InterScan Messaging Security Suite** – offered as a software solution, provides protection against viruses, spam and botnets, phishing, spyware, blended attacks, data loss and content filtering capabilities. SaaS pre-filter and Data Privacy and Encryption module are not available in this implementation.

- **Hosted Email Security –** is a SaaS solution that protects organizations against spam, viruses, spyware and phishing. It comes with content filtering capabilities.

- **Hosted Email Encryption** – is an add-on to Hosted Email Security service with advanced encryption capabilities.

- **ScanMail Suite for Microsoft Exch**ange – offers mail server security for Microsoft Exchange to protect internal and external email against spam, phishing, ransomware, and targeted attacks, with optional integrated data loss prevention (DLP) functionality.

- **ScanMail Suite for IBM Domino** – secures internal and external email as a native IBM Domino server application to stop spam, phishing, ransomware, and targeted attacks.

- **Cloud App Security for Office 365** – offers threat and data protection for Microsoft Office 365 email, SharePoint Online, and OneDrive for Business.

- **Hybrid SaaS Email Security** – combining virtual appliance and software appliance deployments.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

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.
- 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 solutions don't seem to be updated as frequently as those of its competitors.
- DLP is available but only at an extra cost.
- Trend Micro sells email security in a variety of packages, but does not integrate its email security offerings fully with Advanced Threat Prevention (ATP) for advanced real-time malware analysis and threat correlation.

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. Customers can add **Exchange Online Advanced**

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

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 also adds protection against "zero-day" attachments and harmful URL link, through real-time behavioral analysis and sandboxing.

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.

Message Encryption – allows recipients of encrypted messages to enter a simple one-time passcode to read it. 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 natively, free of charge with most Microsoft Office 365 plans. Where an additional fee is required it is usually very small.

- Microsoft has been investing heavily to address growing concerns over 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 manage 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 best-of-breed security vendors.

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited

- 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 © November 2016, 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**
- **Instant Messaging**
- **Unified Communications**
- **Identity Management**
- **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, and is headquartered in Palo Alto, CA, with offices in London, UK.

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 © November 2016, 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, 2016-2020	Jul. 2016	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2016-2020	Jul. 2016	$3,000.00
Email Market, 2016-2020	Jun. 2016	$3,000.00
Cloud Business Email Market, 2016-2020	Jun. 2016	$3,000.00
Advanced Threat Protection Market, 2016-2020	Mar. 2016	$3,000.00
Enterprise Mobility Management Market, 2016-2020	Mar. 2016	$3,000.00
Information Archiving Market, 2016-2020	Mar. 2016	$3,000.00
US Email Statistics Report, 2016-2020	Mar. 2016	$3,000.00
Email Statistics Report, 2016-2020	Mar. 2016	$3,000.00
Instant Messaging Market, 2016-2020	Feb. 2016	$3,000.00
Instant Messaging Growth Forecast, 2016-2020	Feb. 2016	$3,000.00
Social Networking Growth Forecast, 2016-2020	Feb. 2016	$3,000.00
Mobile Growth Forecast, 2016-2020	Jan. 2016	$3,000.00
eDiscovery Market, 2015-2020	Dec. 2015	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Instant Messaging Market, 2017-2021	Feb. 2017	$3,000.00
Email Statistics Report, 2017-2021	Feb. 2017	$3,000.00

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

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

Copyright © November 2016, The Radicati Group, Inc. Reproduction Prohibited