The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Secure Email Gateway - Market Quadrant 2020 *

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

November 2020

TABLE OF CONTENTS

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.

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.

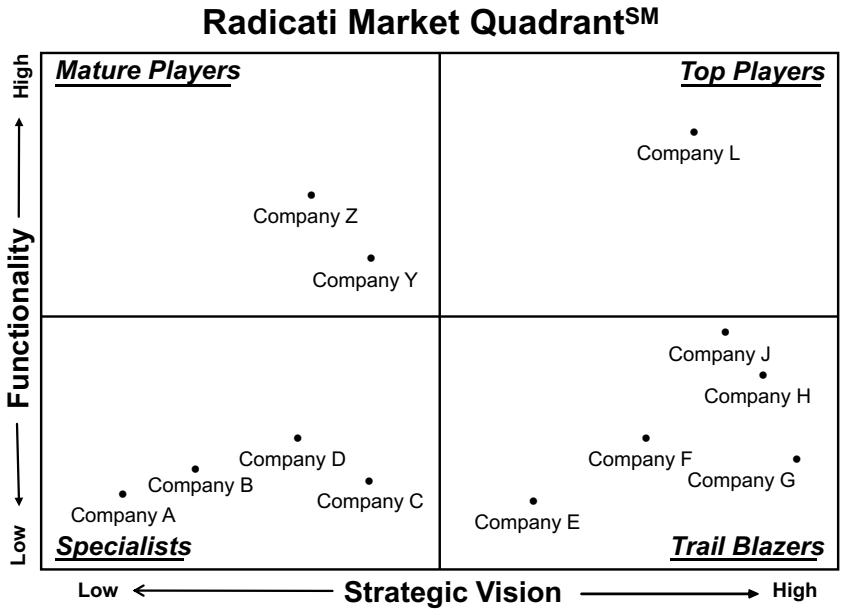

Figure 1: Sample Radicati Market Quadrant

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.

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 *Barracuda Networks, Cisco, Clearswift, Hornetsecurity, Microsoft, Mimecast, Proofpoint, Retarus, Sophos, Symantec, Trend Micro,* and *Trustwave*.

- 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.

- The Secure Email Gateway market continues to see strong growth as email remains a leading vector for malware attack and penetration. Organizations of all sizes are investing 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 become an increasingly important aspect of email security.

- Vendors of Secure Email Gateway solutions are increasingly integrating Data Loss Prevention (DLP), email encryption, Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR), Advanced Threat Prevention (ATP), Phishing Awareness Training solutions, and more into their offerings.

- Organizations of all sizes continue to invest in highly sophisticated email security solutions, as email remains a key vector for malicious attacks and compromise. The worldwide revenue for Secure Email Gateway solutions is expected to grow from nearly $3.2 billion in 2020, to over $5.5 billion by 2024.

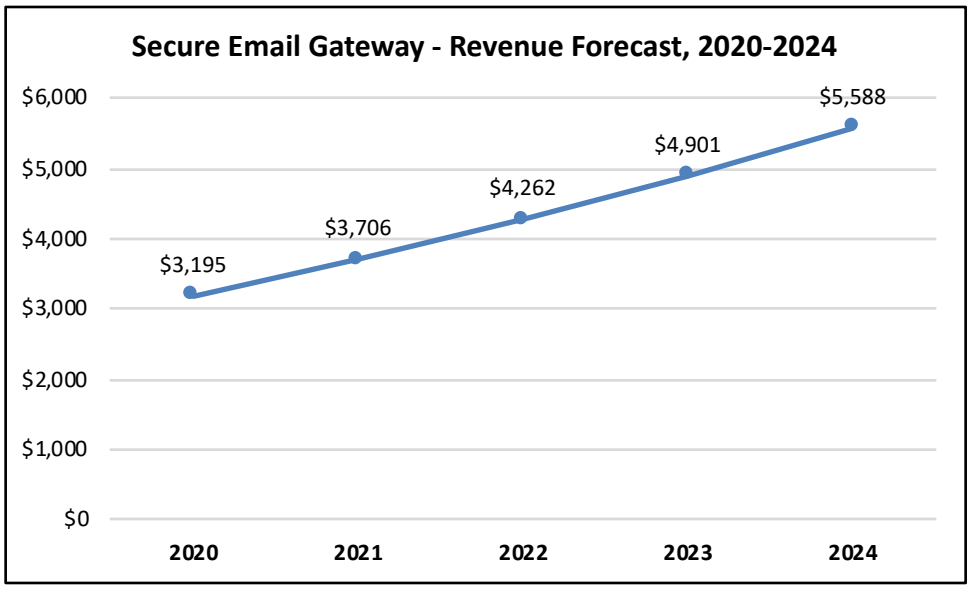

Figure 2: Secure Email Gateway Revenue Forecast, 2020 – 2024

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

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).

- ***Office365 API integration*** – the ability of the solution to integrate with Microsoft Office365 APIs.

- ***Business Entity Compromise (BEC)*** – the ability of a solution to detect BEC, as well as block BEC attempts before they occur and provide remediation capabilities. BEC is a form of cybercrime which uses email fraud to target one or more employees in an organization with spoofed emails that represent a trusted employee, customer, or entity and which request the victim to release payments, credentials, customer information or privileged information. It often relies on social engineering to cause the victim to transfer money or information to the fraudster.

- ***Account Takeover –*** is a form of BEC, where an account is appropriated for fraudulent reasons and starts generating fraudulent emails or is used for impersonation. The ability of the solution to detect and block account takeover attempts, as well as remediate the attack by removing all malicious emails sent by any compromised accounts.

- ***Phishing Awareness Training –*** does the vendor also provide phishing awareness training? Is it offered inline? Is it the vendor's own offering or is it available through partner(s)? Is it priced extra?

- ***Archiving and/or Email Continuity Services –*** does the vendor also provide email archiving and/or Email Continuity services? Is it the vendor's own offering or is it available through partners?

- ***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.*

MARKET QUADRANT – SECURE EMAIL GATEWAY

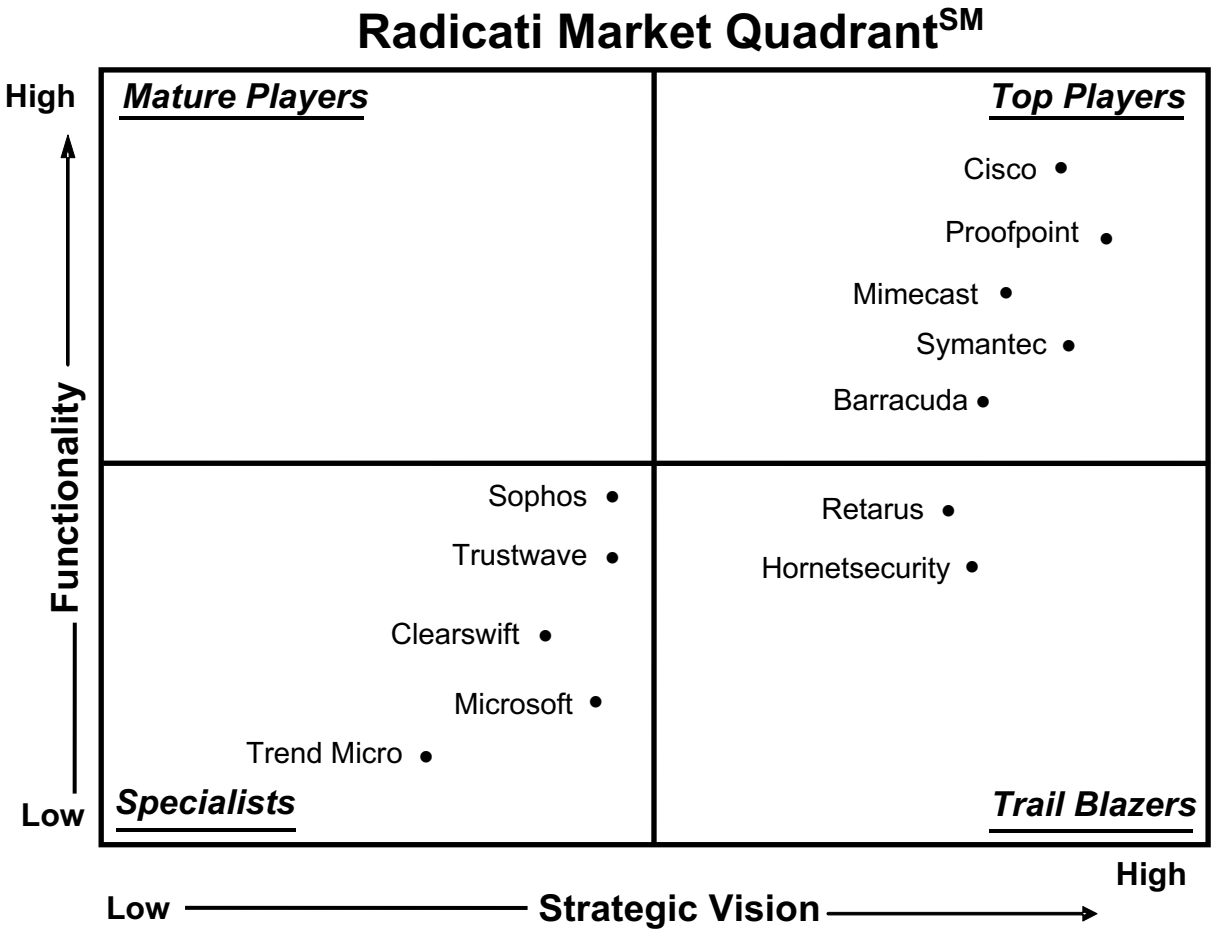

Figure 3: Secure Email Gateway Market Quadrant, 2020*

* Radicati Market Quadrant℠ is copyrighted November 2020 by The Radicati Group, Inc. This report has been licensed for distribution. Only licensee may post/distribute. 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.

KEY MARKET QUADRANT HIGHLIGHTS

- The **Top Players** in the market are *Cisco, Proofpoint, Mimecast, Symantec* and *Barracuda Networks.*
- The **Trail Blazers** quadrant includes *Retarus,* and *Hornetsecurity*.
- The **Specialists** quadrant includes *Sophos*, *Trustwave*, *Clearswift, Microsoft,* and *Trend Micro*.
- 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's security solutions are powered by the Cisco Talos Intelligence Group, made up of leading threat researchers. Cisco is publicly traded.

SOLUTIONS

Cisco Secure Email provides layered protection that defends against phishing, spoofing, business email compromise and loss of sensitive information. It is available in the following form-factors: Cloud Email Security (CES), Email Security Appliance (ESA), Virtual Email Security Appliance (ESAv), Security Management Platform (SMP), and Hybrid (Cloud and On-Premises). Cisco also offers Cisco Cloud Mailbox Defense, a cloud-native solution for Microsoft 365. All deployment options have feature parity.

Cisco Secure Email supports customers across all market 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 and allow customers to change the number of on-premises versus cloud users at any time during the term of their subscription. Cloud Mailbox Defense can be bundled with Cisco Secure Email to provide internal traffic analysis. It can also be deployed as a standalone offer for customers of Microsoft 365, starting at 25 seats.

Cisco's Secure Email solutions comprise the following capabilities:

- **Spam & Threat Filtering** – includes: *IP Reputation filtering***,** provided through SenderBase Reputation Filtering; *Sender Domain Reputation Filtering,* based on additional information about the domain of the sender and intelligence gathered by Talos; *Connection Controls,* based on the score determined during reputation filtering; *External Threat Feeds,* leverage the STIX over TAXII standard to consume customized third-party threat feeds; *Anti-Spam***,** "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; *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 that 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; *Phishing Defense,* augments sender authentication and business email compromise (BEC) detection capabilities, through machine learning and behavior analytics.

- **Anti-Spoofing** – includes: *DMARC, DKIM and SPF analysis*; *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 and performs specified actions to protect high-valued executive names; *Domain Protection,* automates the process of email authentication to prevent phishing, protect brands from fraud and maintain email governance.

- **Malware and Attachment Control** – offers multiple layers of protection to block hidden threats within attachments: *Mailbox Auto Remediation*, automatically removes malicious files from inboxes supporting Microsoft Exchange 2016 and 2019, Office365 and hybrid deployments; *Content Disarm and Regeneration (Safe Print)*, allows for attachments to be converted into a jpg and embedded in a PDF, while keeping the original in quarantine; *Antivirus***,** multi-layer signature-based antivirus protection is provided through Sophos and/or Intel (McAfee) antivirus engines; *Macro and FileType filtering***,** full inspection of PDF, OLE and Office file type attachments for macro or script presence; *Malicious URLs in documents*, extraction and scanning for malicious URLs inside PDF, OLE and Office file type attachments.

- **Malware Defense** – consists of four phases: *File Reputation*, a fingerprint of each file is captured as it traverses the gateway and sent to Cisco Secure Email Malware Defense's cloud-based intelligence network for a reputation verdict checked against zero-day exploits; *File Sandboxing*, when malware is detected, Malware Defense gleans precise details about a file's behavior; *File Retrospection*, deals malicious files that pass-through perimeter defenses, allowing customers to begin remediation quickly if a breach occurs; *File Remediation,* uses APIs to auto-remediate malware for mailboxes hosted in Microsoft 365, Exchange 2016 and Exchange 2019, and provides the added benefit of 'Search and Remediate' through message tracking for email administrators.

- **Threat Visibility and Investigation** – includes SecureX threat response integration, which provides investigative capabilities on threats based on URL, SHA values or domains and pivoting into Message Tracking data to simplify the investigation of threats. SecureX threat response is integrated throughout Cisco's portfolio, including: Secure Email, Umbrella, Cisco Secure Web, Malware Defense and NGFW.

- **Outbound Control** – includes *Data Loss Prevention (DLP)*, offered as a built-in engine that uses pre-tuned data structures along with optional settings to create policies; *Encryption*, leverages TLS and S/MIME. Full payload encryption is available through the Cisco Secure Email Encryption Service, which provides both push and pull encryption. CRES is available as part of the Cisco Outbound Essentials and Premium bundle.

- **Cisco Secure Awareness Training** – delivers phishing simulations and awareness training for end users.

STRENGTHS

- Cisco Secure Email leverages the threat detection capabilities of Talos, whose threat intelligence network gathers telemetry from the vast network of Cisco Security products.

- Cisco Secure Email is integrated with the Cisco Secure Endpoint console and with Cisco SecureX. This provides customers with tight control, visibility and automation from the network perimeter to the endpoint.

- Cisco Secure Email 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 buildouts (rather than multi-tenant offerings), which is often desirable for customers concerned about moving to cloud.

- Cisco offers a Microsoft 365 bundle aimed at the needs of budget-conscious small and medium businesses. Cloud Mailbox Defense also provides simplicity and affordability aimed at the needs of SMBs.

- Cisco has focused on product simplification, in recent years, to ease deployment complexity for customers across all sizes.

WEAKNESSES

- Cisco Secure Email solutions could benefit from an improved user interface. The vendor is addressing this as part of its roadmap.

- Customers indicate that the reporting functionality could be improved for greater ease of use. The vendor has this on its roadmap.

- While highly feature-rich, Cisco Secure Email solutions tend to be somewhat pricier than competing vendor solutions.

- Cisco SecureX supports integrations with the broader Cisco Security suite. However, additional work is needed to further enrich the integration of Cisco Secure Email solutions

with other components of Cisco's security portfolio. The vendor has this on its roadmap.

- Cisco does not currently offer email continuity services, which have become common with many vendors that offer email security solutions. The vendor has this on its roadmap.

PROOFPOINT

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

Proofpoint develops enterprise security solutions aimed at protecting people, data, and brands from advanced threats and compliance risks. The company delivers solutions for inbound email security, outbound data loss prevention, social media, digital risk, email encryption, compromised accounts, eDiscovery, security and awareness training, insider threat management and email archiving. Proofpoint is publicly traded.

SOLUTIONS

Proofpoint offers email security solutions as stand-alone products, as well as bundled with additional capabilities to stop phishing and business email compromise, identify and remediate compromised internal accounts and prevent data exfiltration. Proofpoint offers a wide choice of deployment options including cloud, dedicated appliance, virtual appliance or a hybrid deployment.

Proofpoint Email Security – available as an on-premises or cloud-based solution, serves to prevent email-borne threats, including phishing, business email compromise and malware , 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. URLs are re-written for post-delivery analysis upon click, as well as sent to an isolated browsing session to ensure that users are protected from suspicious URLs. End users can access the web content in read-only mode while the websites are analyzed to determine any malicious behavior. 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 scores all threats entering an organization and assigns an Attack Index score to every person in the organization. This helps identify Very Attacked People (VAPs) and enables a connection between email security and other adjacent controls, such as security awareness training, browser isolation and cloud application security.

- *Automate abuse mailbox analysis and remediation* – Closed Loop Email Analysis and Response (CLEAR) automates the analysis, identification and removal of malicious emails reported by end users through an abuse mailbox.

- *Threat Simulation & Security Awareness Training* – using VAP reporting, specific groups of users can be enrolled in training appropriate to the threats that they are being targeted with. This can also help assess end user vulnerability and puts in place corrective training to enhance the user's ability to identify and report threats.

- *Block email fraud/business email compromise* – 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, as well as detect suspicious behavior across cloud applications.

- *Block attacks through personal webmail* – protects against threats and data exfiltration, via employee use of personal email accounts, such as Gmail or Outlook.com through browser isolation integration.

- *Automated Response/mSOAR* – includes the ability to automatically remove potentially malicious email from an end user inbox, including forwarded messages. It also automates other remediation actions, such as blacklisting IP addresses, orchestrating workflow to quarantine an infected endpoint and requiring password resets.

- *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.

STRENGTHS

- Proofpoint's process for identifying Very Attacked People (VAPs), enables a more effective security posture to help protect organizations.

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

- Integration between sandboxing analysis and browser isolation offers an additional layer of security while allowing end users to access websites in a read-only mode.

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

- 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.

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

- Integration between threat intelligence and security awareness training allows organizations to customize training based on the actual threats targeting a user, and to use lures spotted "in-the-wild" for phishing simulation.

WEAKNESSES

- Proofpoint offers a best-in-breed secure email gateway solution, however, it does not offer endpoint protection or web security solutions. Proofpoint does have partnerships with security vendors that offer these solutions (e.g. Crowdstrike), however, customers wanting an integrated solution from a single vendor that combines secure email gateways, web security

and endpoint protection will need to look elsewhere.

- Customers indicate that while feature rich, Proofpoint Email Protection can be complex to install and maintain.

- Proofpoint Email Protection tends to be somewhat more expensive than competing solutions. However, the Proofpoint Essentials solution, aimed at organizations with less than 1,000 users, is priced to address the SMB market.

- 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.

MIMECAST

1 Finsbury Avenue
London
EC2M 2PF
www.mimecast.com

Founded in 2003, Mimecast is a provider of cloud-based business services which comprise email security, archiving, email continuity, web security, security awareness training, and more. Mimecast is headquartered in London, UK, with North American headquarters in Lexington, MA and offices globally. Mimecast is a publicly traded company.

SOLUTIONS

Mimecast **Email Security with Targeted Threat Protection** is a core component of Mimecast's **Email Security 3.0** strategy. It enables protection against email attacks by addressing threats in three distinct zones: at the email perimeter, inside the network and the organization, and beyond the perimeter. It protects against malware, spam, advanced phishing, impersonations, and other emerging and targeted attacks, while preventing data leaks. Email Security 3.0 also encompasses awareness training and services to reduce the complexity of DMARC deployment and provide brand exploit protection. Mimecast also delivers email continuity, enterprise information protection (including archiving and data recovery) and web security. Mimecast services are all provided on their multi-tenant, cloud-based platform, Mime|OS, 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 and intelligence to provide anti-malware, anti-spam, and malicious URL filtering.

Mimecast offers a single integrated administration console for all services, 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 leading SIEM and SOAR systems (e.g. Splunk, IBM QRadar, and others) to enable data integrations and remedial responses from systems of the customer's choosing. The API also allows customers to ingest their own threat data into their Mimecast tenant.

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, employees, business partners, or well-known internet brands (combining both a Mimecast managed and customer customizable list of lookalike domains). 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. Ongoing checks are performed to identify malware that may already be inside the mail system and automatically remove it from mailboxes, as well as from the Mimecast Archive.

Browser Isolation is integrated with Email Security URL Protect to open potentially malicious URLs in a remote browser session. Web pages can be rendered read only to prevent credential and sensitive information phishing and zero-day malware is contained in the remote session. Users of Mimecast Web Security are provided a single policy across both services.

Mimecast's Awareness Training service (acquired from Ataata and integrated into the Mimecast platform) offers bite-sized security awareness training and cyber risk management content via videos which help combat information security breaches caused by employee mistakes. Customers can convert the phishing attacks that their users have clicked on (users are protected via rewritten URLs) into phishing campaigns to test the rest of their users. The results from 'bad' URL clicks and phishing campaigns are integrated into Mimecast SAFE Score's user risk score which also measures statistics such as sentiment, engagement with training modules and answers to assessments.

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's Email Security 3.0 strategy combines multiple email security services in a solution framework to meet the email security needs of organizations, ranging from SMBs to large enterprises.

- 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 email security is entirely cloud-based, which may not suit organizations that are still reluctant to rely entirely on cloud-based security systems.

- Mimecast provides email security, along with email continuity, 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 endpoint protection from a single vendor.

- Customers we spoke to as part of this research, indicated that the DLP functionality could be improved through better filtering and reduced false positives.

SYMANTEC, A DIVISION OF BROADCOM

1320 Ridder Park Drive
San Jose, California 95131
United States
www.broadcom.com

Symantec offers a wide range of security solutions for the enterprise market. Symantec operates the largest civilian cyber intelligence network, allowing it to see and protect against the most advanced threats. Symantec is an operating division of Broadcom. Broadcom 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 on-premises email systems, such as Microsoft Exchange. Symantec Email Security.cloud blocks targeted attacks, spear phishing, ransomware, viruses and malware, business email compromise (BEC) attacks, email fraud, spam, and bulk mail with anti-malware and antispam services. This protection includes technologies, such as advanced heuristics, deep evaluation of links before email delivery, advanced phishing variant detection, and impersonation controls. 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.

Email Threat Detection and Response (ETDR) – is a service that can be added to detect targeted attacks while providing visibility into the attack landscape to accelerate remediation. It

uses cloud-based sandboxing and payload detonation to identify and stop complex 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. ETDR also provides detailed data on targeted attacks that attempt to enter an organization via email, as determined by Symantec research analysts. In addition Targeted Attack Analytics provides information on email campaigns, helping organizations build protection around high risk users. Analytics data can easily be exported to third-party Security Incident and Event Management (SIEM) solutions, Symantec Endpoint Detection and Response, Symantec Integrated Cyber Defense Exchange, Symantec Information Centric Analytics, and other security tools. Additionally, ETDR includes auto-remediation capabilities to claw back emails from O365 inboxes that are detected as malicious post-delivery. Symantec also offers Phishing Readiness services as part of ETDR, which allows customers to identify risky users and improve end user awareness through 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 is available as either a cloud-based service or an on-premises appliance.

Symantec Email Fraud Protection – is an add-on service that helps organizations automate implementation of sender authentication controls such as SPF, DKIM, and DMARC. The service builds and manages a global whitelist of trusted third-party senders by cataloging thousands of third-party email services and automatically updating this list with any configuration changes.

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. Symantec also provides a license bundle that includes both Symantec Message Gateway and Email Security.cloud. Messaging Gateway integrates with Symantec Content Analysis, an advanced content filtering and malware analysis platform, to provide advanced threat protection.

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 integrated threat isolation for corporate email, which helps prevent advanced email attacks such as spear phishing, credential phishing and ransomware.

- Symantec's Email Fraud Protection service helps customers implement and automate sender authentication controls such as SPF, DKIM, and DMARC.

- 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 accelerates response to targeted, advanced email attacks with deep visibility as well as powerful remediation capabilities. In addition, integration with SIEM/SOAR 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.

- 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

- Symantec has been working to bring together and harmonize its portfolio of email security solutions across Email Security.cloud and Messaging Gateway. Customers choosing a hybrid deployment, however, can expect differences in administration procedures across the different solutions.

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

- While Symantec offers blacklisting of Indicators of Compromise (IOC), and Auto Remediation to delete an email from the users' inbox which is later found to be malicious, it currently lacks the ability to search and automatically remediate IOCs. The vendor is addressing this as part of its roadmap.

BARRACUDA NETWORKS

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

Founded in 2003, Barracuda Networks provides email protection, content, network and application security, and data protection services to business organizations. Barracuda Networks is privately held by Thoma Bravo.

SOLUTIONS

Barracuda offers email protection solutions 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 under the umbrella of **Total Email Protection**:

- **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

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** – combines artificial intelligence, deep integration with Microsoft Office 365, and brand protection into comprehensive cloud-based solution that guards against spear phishing, business email compromise and account takeover. Sentinel's API based architecture uses an AI engine to study historical communications patterns. This allows it to identify anomalies in messages, as well as find and block social engineering attacks in real time. Sentinel can also stop phishing attacks used to harvest credentials that lead to account takeover. It can also identify accounts that are already compromised and alert IT.

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

- **Barracuda Forensics and Incident Response** – automates response and remediation of email attacks. Automated incident response allows IT to quickly identify the nature and scope of an attack, and immediately eliminate malicious emails by removing them directly from the users' inboxes. Analytic capabilities provide insight into delivered mail which helps identify malicious messages in users inboxes.

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.

STRENGTHS

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

- Barracuda provides extensive protection to detect and block spear phishing, business email compromise, account takeover, and other targeted attacks. Barracuda solutions provide attack detection, as well as automated incident response to quickly remediate email attacks that may have gotten through.

- Barracuda supports automated incident response through its Forensics and Incident Response tool, which allows IT to automate response to email attacks and automatically remediate malicious messages post-delivery.

- Barracuda Real-Time Protection offers strong protection to stop rapidly propagating threats, and correlates threat intelligence across email and web gateways.

- API integration with Office 365 provides visibility into internal and historical data to help protect against spear phishing and account takeover.

- Barracuda PhishLine offers extensive tools and techniques for user security awareness training, helping to embed training in everyday user activities.

- Barracuda also provides a full suite of cloud archiving and backup solutions that integrate with Microsoft Office365, OneDrive for Business and SharePoint.

WEAKNESSES

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

- Barracuda offers encryption capabilities but these are not currently integrated with SIEM/SOAR tools. The vendor has this on its roadmap.

- Customers indicate that management of Barracuda content filters can be somewhat complex.

- Barracuda's management interface for Sentinel and Essentials could be improved through greater data visualization and an improved UI. The vendor has this on its roadmap.

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

TRAIL BLAZERS

RETARUS

Aschauer Straße 30
81549 Munich, Germany

Retarus, founded in 1992, provides an enterprise cloud platform for communications, secure email and business integration that helps connect business-critical processes between companies worldwide. Retarus is based in Germany, with offices in the US, and worldwide. The company is privately held.

SOLUTIONS

Retarus **Secure Email Platform** is a cloud-based solution that protects business communications while ensuring deliverability, compliance, ease of use, control and transparency. The solution provides advanced threat protection at the gateway level, as well as post-delivery protection. Retarus Email Security integrates with SIEM systems, as well as email infrastructures, including:

Microsoft 365, Google G Suite, Microsoft Exchange, Domino, and others. Key features of Retarus Email Security include:

- *Spam, Phishing 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 analysis as well as other intelligent filter, pattern, and identification rules that are updated continuously. Phishing detection includes checking URLs against multiple external databases from specialized vendors (e.g. Spamhaus, and others).

- *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 handling allows recipients to receive large attachments despite size limitations defined by their mail server. For outbound email communication, Retarus offers additional services for transmission of both high volume and transactional emails (e.g. CRM systems such as Salesforce). An Attachment Blocker prevents the delivery of files attached to incoming emails when these match customer defined criteria, for instance 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-suite executives). Individual names of employees may also be added to a so-called “Targeted Members Blacklist” in order to avoid friendly name spoofing.

- *Sandboxing* – in-depth analysis of specific file attachments including AI/ML algorithms and heuristics in order to identify “zero day attacks”. Sandboxing functionality, based on technology from Palo Alto Networks, is hosted and managed in Retarus data centers to ensure data protection and compliance. Emails identified as infected are either deleted or quarantined, and a notification is sent to the intended recipient.

- *Time-of-Click Protection* – defends against malicious links by rewriting email URLs. The 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 of the current traffic situation. An Email 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* – Automated Directory Synchronization automatically reconciles customer addresses with Microsoft (Exchange, Active Directory, Azure Active Directory for Office 365), HCL Domino/Notes, 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* – Retarus offers a managed Email Encryption key management service and supports standard encryption formats (e.g. PGP, SMIME, OpenPGP). In order to ensure that intended recipients are able to read emails without installing certificates on their own email client, Retarus 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 the recipient inside a password-protected PDF, or ZIP document.

- *Patient Zero Detection & Real-Time Response* – provides early recognition and alerting of previously unknown malware and phishing URLs ("patient zero") through a patented technology. The technology uses digital fingerprinting (i.e. a hash of meta data and URL/attachments) to back-track, detect and automatically clawback any threats in emails that have already been delivered.

- *Forensic SIEM Integration* – delivers forensic data for ingestion into third-party SIEM solutions.

- *Email Continuity* – is an email recovery solution for emergency scenarios (e.g. complete email outage), which allows users to receive and send emails via an alternative webmail platform.

- *Email traffic management* – Retarus offers a "*Transactional Email*" service in order to separate high-volume outbound traffic (i.e. bulk mailings from CRM or other outbound messaging solutions) from business email traffic. Retarus Transactional Email Services

provide advanced mechanisms to send emails directly from applications with higher deliverability rates, detailed tracking and secure document handling options.

- *Retarus Policy Engine* – supports address rewriting, user-based routing and other functions that allow deep customization of individual email policies.

- *Predelivery Logic* – is a rule-based service which analyzes and optimizes emails in the Retarus Enterprise Cloud, before they are forwarded to the company's internal infrastructure. It makes it possible for companies to create company-specific rules to check, organize, route or adjust all of their email traffic. If intrusive emails are received primarily from a specific region or country, automatic measures, such as quarantining, can be put in place to deal with messages based on origin (e.g. Geo IP).

STRENGTHS

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

- 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.

- Retarus offers email continuity services, which are a value added for customers.

- As a European company, based in Germany, Retarus offers cloud services that are fully GDPR compliant without the need of additional data export mechanisms.

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

- While Retarus provides basic integration with Microsoft Azure directory services, this could be enhanced to provide more granular policy controls.

- Retarus does not currently support DMARC. However, the vendor has this its near term roadmap.

- Retarus does not currently offer user phishing awareness training. However, the vendor is working to address this through partners.

- While well known in Europe, Retarus currently lacks visibility in the North American market.

HORNETSECURITY

Am Listholze 78
30177 Hannover, Germany
www.hornetsecurity.com

Hornetsecurity is a German cloud email security provider, which offers solutions to protect IT infrastructures, digital communication and data exchange for organizations of all sizes. Hornetsecurity is present globally in 12 locations, and operates in more than 30 countries through its international distribution network. The company is privately held.

SOLUTIONS

Hornetsecurity offers cloud based security solutions aimed at addressing all areas of email security, including spam and virus filters, legally compliant archiving, encryption, as well as defense against CEO fraud and ransomware.

The company offers the following suite of services:

- **365 Total Protection** – offers comprehensive protection for Microsoft 365 and Microsoft cloud services. It is available in two versions Business and Enterprise. The Business version comprises the following features:

  - *Threat Detection* – multi-stage in-depth analysis and filter systems detect and block spam and viruses threats.

  - *Global S/MIME and PGP Encryption* – protects the entire email communication from being altered or read by third parties without authorization.

  The Enterprise version adds:

  - *Forensic Analyses* + AI – relies on artificial intelligence and machine learning to detect and avert threats, fraud attempts and digital identity theft at an early stage. It delivers an Intention Recognition System, Fraud Attempt Analysis, Identity Spoofing Recognition, Spy-Out Detection, Feign Facts Identification and Targeted Attack Detection.

  - *URL Malware Control* – protects against targeted and blended attacks and digital espionage and notifies of any direct attacks.

  - *ATP-Sandboxing* – (available with the Enterprise edition) offers protection against targeted and blended attacks. It serves to detect malware in email attachments and automatically alert IT security teams of a potential threat.

  - *GDPR + GoBD* – email archiving is done automatically, when emails are sent/received in accordance with GDPR requirements. Different retention periods can be specified based on applicable data protection regulations. Private emails can be marked by the user and individual users can be excluded from the archiving procedure. In-house email communication can also be archived.

  - *Global Security Dashboard* – centralizes all the functions and results of 365 Total Protection and offers a complete overview of the company security. A range of information and statistics information is displayed on the Dashboard based on the selected service levels.

- **365 Total Encryption** – is a paid for add-on service to 365 Total Protection. It encrypts the entire content of the enterprise email communications in Microsoft 365, providing protection against all forms of espionage and hackers. All incoming email messages are fully encrypted before they reach the Microsoft cloud. Emails already stored in a Microsoft 365 mailbox are also encrypted once 365 Total Encryption is activated.

In addition, Hornetsecurity offers the following services as stand-alone solutions:

- **Spam and Malware Protection** – offers high detection rates for spam and viruses. The Spam Filtering Service effectively protects mail servers against DDoS attacks and phishing emails.

- **Advanced Threat Protection –** offers a broad set of defense mechanisms that include freezing, URL scanning, rewriting, sandboxing, and Malicious Document Decryption to safeguard IT infrastructures against advanced threats like Emotet, CEO fraud or Ransomware.

- **Email Continuity Service** – supports uninterrupted mail services through an alternative email solution (POP3/IMAP mailbox or webmail access). All archived emails are securely stored in encrypted databases in certified and secured data centers.

- **Email Archiving** – ensures that all incoming and outgoing emails are automatically stored in their original form in Hornetsecurity's data centers immediately upon arrival and dispatch. Emails cannot be edited or deleted before the set retention period has expired.

STRENGTHS

- All Hornetsecurity services are cloud-based, which delivers all the advantages of cloud to customers.

- Hornetsecurity offers a comprehensive set of services aimed at all aspects of email security, at an attractive price point for organizations of all sizes.

- Hornetsecurity offers a SIEM Connector, which automatically receives and imports e-mail log entries from the Hornetsecurity Cloud and provides an interface to SIEM services from Hornetsecurity's 365 Total Protection and Spam Filter Service solutions.

- Hornetsecurity offers Email Authentication as a standard solution, with a self-service module in the control panel, which allows admins to easily configure the service.

- Hornetsecurity offers 24/7 support service worldwide.

WEAKNESSES

- While Hornetsecurity is currently well known in Europe, it has so far been less present in the North American market. The company is working to address this.

- Hornetsecurity offers strong email protection, however, it does not offer endpoint security which may disappoint customers looking to source both from a single vendor.

- Hornetsecurity currently does not offer Phishing Awareness Training, however, this is on the vendor's roadmap.

SPECIALISTS

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 for email, network, next-gen endpoint and server protection with EDR, mobile device protection, encryption, wireless, a range of public cloud security solutions including cloud security posture management, and a human-led Managed Threat Response team. In March 2020, Thoma Bravo completed the acquisition of Sophos.

SOLUTIONS

Sophos Email uses a combination of detection methods and machine learning, to protect against malware, spam, phishing impersonation attacks, and data loss. Sophos Email is available in conjunction with a full portfolio of security solutions managed through a single cloud management console. Sophos Email relies on advanced machine learning capabilities which utilize the Sophos-owned deep learning neural network and global threat intelligence from Sophos Labs. This enables Sophos Email to detect both known and unknown malware without having to rely on signatures. The product can identify sophisticated Business Entity Compromise (BEC) attempts through analysis of message body content and subject line to identify conversations with suspicious content.

Sophos Email delivers the following key capabilities:

- *Impersonation Protection* – Sophos Email relies on a variety of technology methods, including machine learning, to identify impersonation attempts using VIP identities in order to commit fraud or other illegal activity. Utilizing the Sophos-owned deep learning neural network, Sophos advanced ML capabilities can analyze message body content and subject lines to identify conversations with suspicious content, specifically in relation to tone and wording which may be used to identify unusual requests from a sender.

- *Advanced Threat Protection* – SophosLabs advanced threat detection technology including Sophos Sandstorm, deploys sophisticated machine learning technology to detect new and emerging suspicious payloads containing threats, malware, and unwanted applications, as well as high-level threats embedded in documents, including ransomware. Sophos Sandstorm detonates these files in series of virtual machines, simulating a real end user environment where behavior can be monitored, delivering safe documents, not just PDFs.

- *Single Management Console* – Sophos Email is part of Sophos Central, a single cloud security platform that enables organizations to manage a layered defense including email, network security, next-generation endpoint and server protection with EDR, mobile device protection, encryption, wireless, a range of public cloud security solutions including cloud security posture management, and a human-led Managed Threat Response team.

STRENGTHS

- Sophos Advanced Threat reporting provides deep visibility into email attachments detonated in the Sophos cloud sandbox, with a breakdown of threat verdicts based on machine learning analysis, file reputation scores, VirusTotal results and Mitre ATT&CK Matrix tactics.

- 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 Email integrates with the Sophos Phish Threat service to provide phishing simulations and security awareness training in the same console. The Sophos Central console allows customers to link Sophos Email and Phish Threat to identify risky user behavior and enroll users directly into targeted security awareness training.

- Sophos Central offers a single cloud security platform to manage a layered defense which includes email, network security, next-gen endpoint and server protection with EDR, and more.

WEAKNESSES

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

- Sophos email security does not yet offer as tight integration with Microsoft Office365 as solutions from other vendors. The vendor has this on its roadmap.

- Customers indicated that Sophos reporting through Sophos Central, while easy to use and comprehensive, could offer greater reporting granularity.

- Sophos email security solutions are a best fit for organizations with small to medium sized IT teams, where management simplicity is a key purchase driver.

TRUSTWAVE

70 West Madison St, Suite 600
Chicago, IL 60602
www.trustwave.com

Trustwave is a cybersecurity and managed security services provider focused on threat detection and response. It offers a comprehensive portfolio of managed security services, consulting services, and email security and data protection technology. Trustwave is the global security arm of Singtel, with customers in 96 countries.

SOLUTIONS

Trustwave **Secure Email Gateway (SEG)** delivers a complete range of email security and management features, based around robust business email compromise (BEC) protection and a flexible policy engine. SEG threat protection is backed by the dedicated SpiderLabs team focused on email security research. The solution is available either through an on premise, or a cloud-based delivery platform. The SEG Cloud platform is located globally to meet the needs of customers in their geographic locations.

Trustwave SEG 10.0 addresses email and cyber security threats through a single platform that offers advanced protection leveraging proprietary threat intelligence and research, policy configuration and in-depth data security and compliance management.

Trustwave SEG's on premise option, is an SMTP gateway solution that can be deployed with any internal or cloud-based company email system and provides an organization with the layered security solution it needs to manage email content, fight advanced threats such as phishing, ransomware, and business email compromise (BEC), eliminate spam, and transparently enforce email acceptable use policy and any other regulatory compliance requirements. Trustwave SEG also goes beyond email security to provide a flexible and capable policy engine which provides a robust business operations tool with diverse use cases. The platform is accessible through an administrative interface, which provides auditing capabilities to manage configuration change processes and provide complete auditability.

SEG Cloud is the SaaS based solution, which is deployed by redirecting SMTP traffic and filtering email at the Internet level before it reaches the network, delivering always-on, inbound and outbound email protection. Administrators can log into the Trustwave SEG console and

manage all users and account settings from a single, secure platform. The SEG Cloud platform supports automated onboarding processes which facilitate adoption by SMB customers.

Trustwave SEG also provides a **Service Provider Edition** to meet the needs of organizations with multitenant requirements, designed to be hosted in the data centers of Service or Solution Providers.

Trustwave also offers a number of features that are available as bundled offerings, or optional add-ons to SEG, as follows:

- **SEG Email Archiving Module** – is available to any SEG customer. It is a cloud-based archiving module that offers variable retention policies, full eDiscovery console, continuity capability, and easy to use options for customers wanting to import existing archive data into the service, as well as options to export data out of the service.

- **SEG Email Encryption Module** – services allow customers of SEG, both the on premise and SaaS versions, to send sensitive emails or confidential documents to recipients securely, without requiring the recipient to download or install any additional software. SEG can be used to intelligently scan email for confidential information, based on customer-defined policies, as well as encrypt sensitive messages.

- **SEG Blended Threat Module** – uses multiple validation methods, including real-time behavioral analysis and content inspection as well as information from several industry standard sources, to identify and block sites that serve suspicious or malicious code. Since validation is performed in real time by a cloud service when a link is clicked, it is highly effective in catching and neutralizing new exploits for all users on any device from any location. This module comes standard in SEG Cloud.

- **SEG Image Analyzer Module** – is a specialized image scanning and classification solution designed to automatically scan and sort images entering the organization via email into either an “offensive and pornographic” category or a “normal and acceptable” category. This feature can help protect employees, customers, and suppliers from exposure to inappropriate or illegal content, can help reduce legal liability, and provides a better understanding of how the email system is conforming with acceptable use policies.

- **Supported Antivirus Software** – Trustwave SEG supports several third-party antivirus scanners to scan for virus or malware laden email. These antivirus solutions from Sophos, McAfee, Kaspersky, and Bitdefender. Trustwave SEG also fully supports a Yara-based malware engine that offers additional capabilities to detect malicious attachments.

STRENGTHS

- Trustwave SEG provides support for Azure Information Protection and Rights Management Services (RMS) this enables clients to enforce outbound email policy on Azure RMS encrypted email for Office 365. SEG also provides the ability to decrypt email and enforce all RMS outbound policy controls before re-encrypting the email and sending it.

- Trustwave SEG has a dedicated BEC engine that helps identify low volume, highly-targeted spear-phishing attacks. The engine is regularly updated with intelligence from Trustwave's SpiderLabs dedicated email security research team, and Trustwave's threat intelligence Fusion platform.

- Trustwave's SEG platform, including BEC, malware and phishing protection, integrate with its Managed Threat Detection and Response Fusion platform.

- Trustwave offers a business workflow tool, which is an email management toolbox with advanced routing, autoresponders, header rewriting and external commands that help customers integrate their business processes to improve business workflow.

- Trustwave SEG offers easy, automated onboarding and is attractively priced for organizations and service providers of all sizes.

WEAKNESSES

- While Trustwave SEG currently offers many pre-configured reporting options, it would benefit from an increased level of reporting granularity and deeper customization options. The vendor is aware of this and has it on its development roadmap.

- Trustwave offers traditional security training education but does not offer the automated phishing awareness training and simulation that has become common in many competing offerings.

- While Trustwave offers strong BEC capabilities, it does not provide account takeover detection features.

- Trustwave does not offer Microsoft Office365 API integration.

- Trustwave lacks market visibility. The vendor is working to address this.

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 2019, Clearswift was acquired by HelpSystems a Minnesota based company, and forms part of HelpSystem's Data Security Group.

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 triple antivirus engines from Sophos, Kaspersky and/or Avira. 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 multiple formats, including 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%+ spam detection using two scanning engines. 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. URLs can also be rewritten to redirect to browser isolation solutions to provide additional time-of-click protection.

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, in-real time, to ensure policy compliance, for example redacting and sanitizing content. This functionality is known as Adaptive Redaction and covers three key areas; data redaction, document sanitization, and structural sanitization.

Data Redaction permits the modification of multiple formats, including 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. Redaction of text in images is also available, with the redacted text being black-boxed out of the image (rather than a separate object being overlayed), to ensure that it cannot be recovered.

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 Boldon James, both HelpSystems companies). Sanitization can also remove potentially embarrassing change tracking comments which may carry data which could represent a data leak. Anti-steganography is available to ensure that hidden data cannot be exfiltrated and hidden malware downloads cannot be infiltrated.

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 approach with can be used in both push and pull modes. Portal options are available for both cloud-based or on-premises solutions. An option for integration into an enterprise digital rights management solution (eDRM) is also available.

The Gateway can be peered together with other email gateways to form a "Cluster" for scalability and availability purposes, and 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 offers Adaptive Redaction features in all its Gateway products. This was recently enhanced with image redaction and anti-steganography features. Comprehensive Adaptive Redaction is a differentiator which is generally not available 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.

- HelpSystems' wider data security portfolio allows customers to also obtain Large File Transfer and Data Classification products from the same provider. Integration of these products into a centralized console is underway.

- 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 needed.

WEAKNESSES

- Clearswift solutions would benefit from integration with sandboxing solutions. This is on the vendor's roadmap.

- Clearswift Secure email gateway would benefit from more support for customized threat feeds. This is on the vendor's roadmap.

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

- Clearswift does not currently support a number of key features, such as Office365 API integration, account takeover detection, phishing awareness training, which have become commonplace with many competing solutions.

- Although Clearswift offers strong email security solutions, the vendor currently lacks market visibility particularly in North America. The acquisition by HelpSystems is intended to address this.

MICROSOFT

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

Microsoft develops products and services for businesses and consumers, and delivers an extensive portfolio of solutions which include 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 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 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 Threat 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 links, through real-time behavioral analysis and sandboxing. It supports spoofing intelligence to detect and block outbound or inbound spoofing attempts. Messages identified 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 available in 2 plans: Plan 1 includes configuration, protection and detection capabilities, Plan 2 adds automation, investigation, remediation, and user education capabilities. ATP Plan 1 is included free of charge in Microsoft 365 Business Premium. APT Plan 2 is included in Office 365 Enterprise E5, Office 365 Education A5, and Microsoft 365 E5 plans. Both plans can also be added 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 need to enter a simple one-time passcode to read the message and can send encrypted replies. Office 365 Message Encryption combines email encryption and rights management capabilities, powered by Azure Information Protection. 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.

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 include 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, to protect against ransomware and advanced attacks. The email solutions integrate with Trend Micro Apex Central for central management and threat sharing with other security layers to improve visibility and overall protection. Email security solutions also integrate with Trend Micro's XDR (Extended detection and response) managed service which offers correlated detection and response across email, endpoints, servers, cloud workloads, and networks. Trend Micro email security solutions are available as cloud or on-premises solutions in different packages, as follows:

Cloud-based Solutions:

- **Email Security** – is a cloud-based 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. It is available in two bundles: Standard, and Advanced.

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

- **Cloud App Security** – is a Trend Micro's Cloud Access Security Broker (CASB) solution that secures email and cloud sharing in Office 365, Gmail, Box, Dropbox, and Google Drive. It relies on artificial intelligence and machine learning to uncover ransomware, Business Email Compromise (BEC), and other 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 HCL Domino (formerly IBM Domino)** – offers malware and spam protection as a native 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 Server (now Teams)** – on-premises software to protect 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 email security solutions in all form factors and a variety of different packages to fit the needs of customers of all sizes.
- Trend Micro's email security solutions integrate with its endpoint and web security solutions to offer stronger enterprise-wide protection.
- 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 sells email security in a variety of packages, but not all its email security solutions integrate fully with its Advanced Threat Prevention (ATP) solutions for real-time threat correlation.
- Trend Micro offers basic, policy-based DLP, but only at an extra cost.
- Trend Micro email solutions track URL usage, but do not support preventive actions such as url replacement or quarantining.
- Customers indicate that administration and policy setup for Trend Micro email security solutions is somewhat lacking and could be improved, particularly for hybrid gateway scenarios.
- Trend Micro's email security portfolio shows signs of aging and does not appear to be updated as frequently as those of its competitors.

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.

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, 2020-2024	May 2020	$3,000.00
Email Market, 2020-2024	Apr. 2020	$3,000.00
Cloud Business Email Market, 2020-2024	Apr. 2020	$3,000.00
Unified Endpoint Management Market, 2020-2024	Apr. 2020	$3,000.00
Corporate Web Security Market, 2020-2024	Apr. 2020	$3,000.00
Microsoft Office 365, Exchange and Outlook Market Analysis, 2020-2024	Apr. 2020	$3,000.00
Advanced Persistent Threat (APT) Market, 2020-2024	Apr. 2020	$3,000.00
Information Archiving Market, 2020-2024	Apr. 2020	$3,000.00
Email Statistics Report, 2020-2024	Mar. 2020	$3,000.00
Social Networking Statistics Report, 2020-2024	Feb. 2020	$3,000.00
Instant Messaging Statistics Report, 2020-2024	Jan. 2020	$3,000.00
Mobile Statistics Report, 2020-2024	Jan. 2020	$3,000.00
Cloud Access Security Broker (CASB) Market, 2019-2023	Nov. 2019	$3,000.00
Enterprise DLP Market, 2019-2023	Nov. 2019	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Secure Email Gateways Market, 2020-2024	Nov. 2020	$3,000.00
Endpoint Security Market, 2020-2024	Nov. 2020	$3,000.00

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

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

