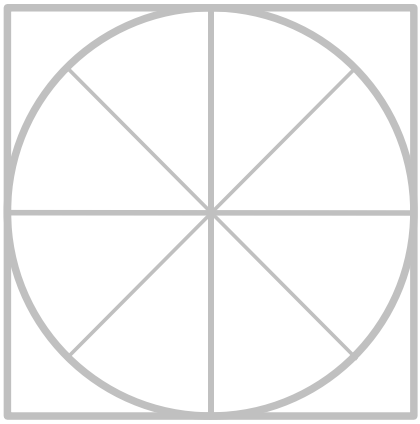
The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Secure Email - Market Quadrant 2023 *



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

March 2023

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.

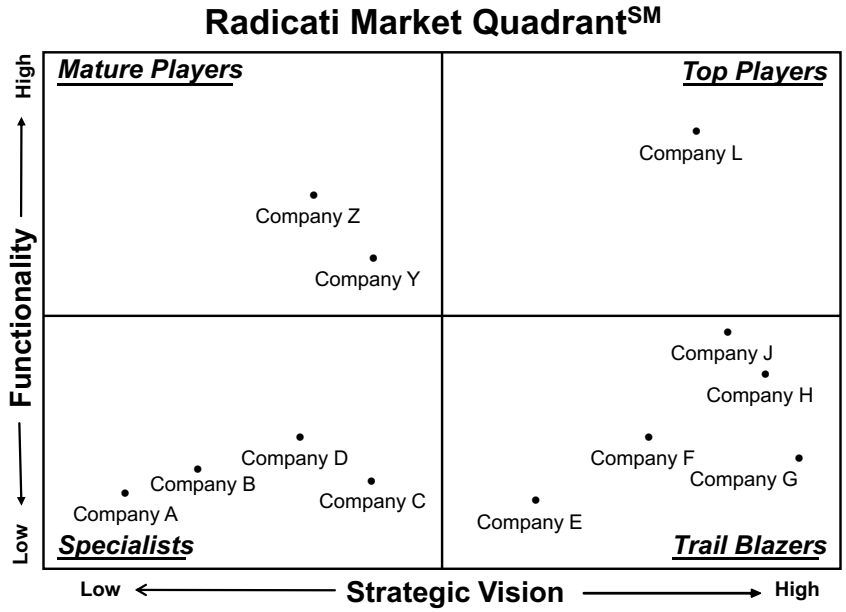


Figure 1: Sample Radicati Market Quadrant

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

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

- **Secure Email –** any software, appliance, or cloud-based service deployed at the mail server, SMTP gateway, or through API integration to filter out spam, viruses, detect and protect from phishing/spear-phishing attacks, and protect messaging traffic from all malware. Some of the leading players in this market are *Barracuda Networks, Cisco, Fortra's Clearswift, Hornetsecurity, Microsoft, Mimecast, Proofpoint, Retarus, Sophos, Symantec, Trend Micro,* and *Trustwave*.

- Some vendors of Secure Email 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 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 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 solutions is expected to grow from nearly $4.9 billion in 2023, to over $10.2 billion by 2027.

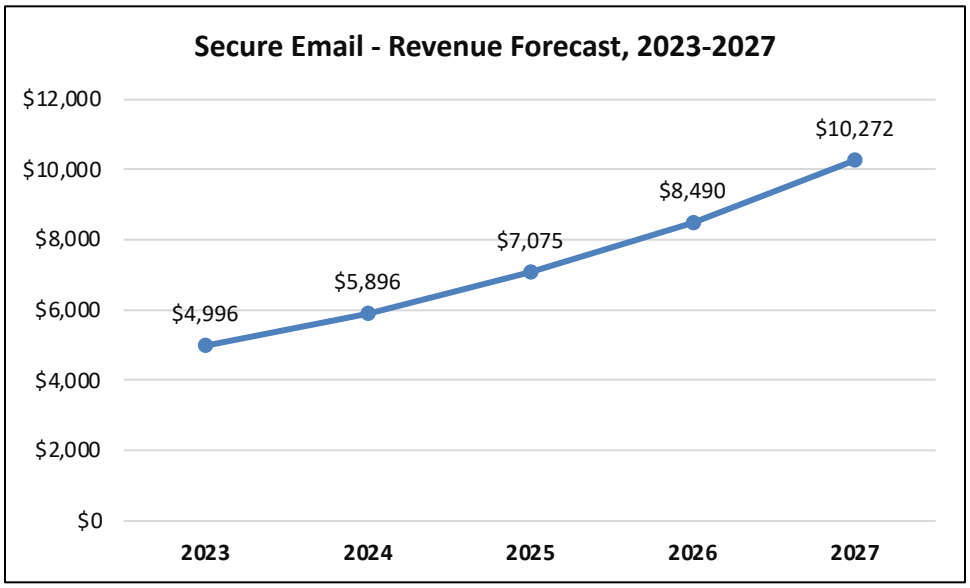


Figure 2: Secure Email Revenue Forecast, 2023 – 2027

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* 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

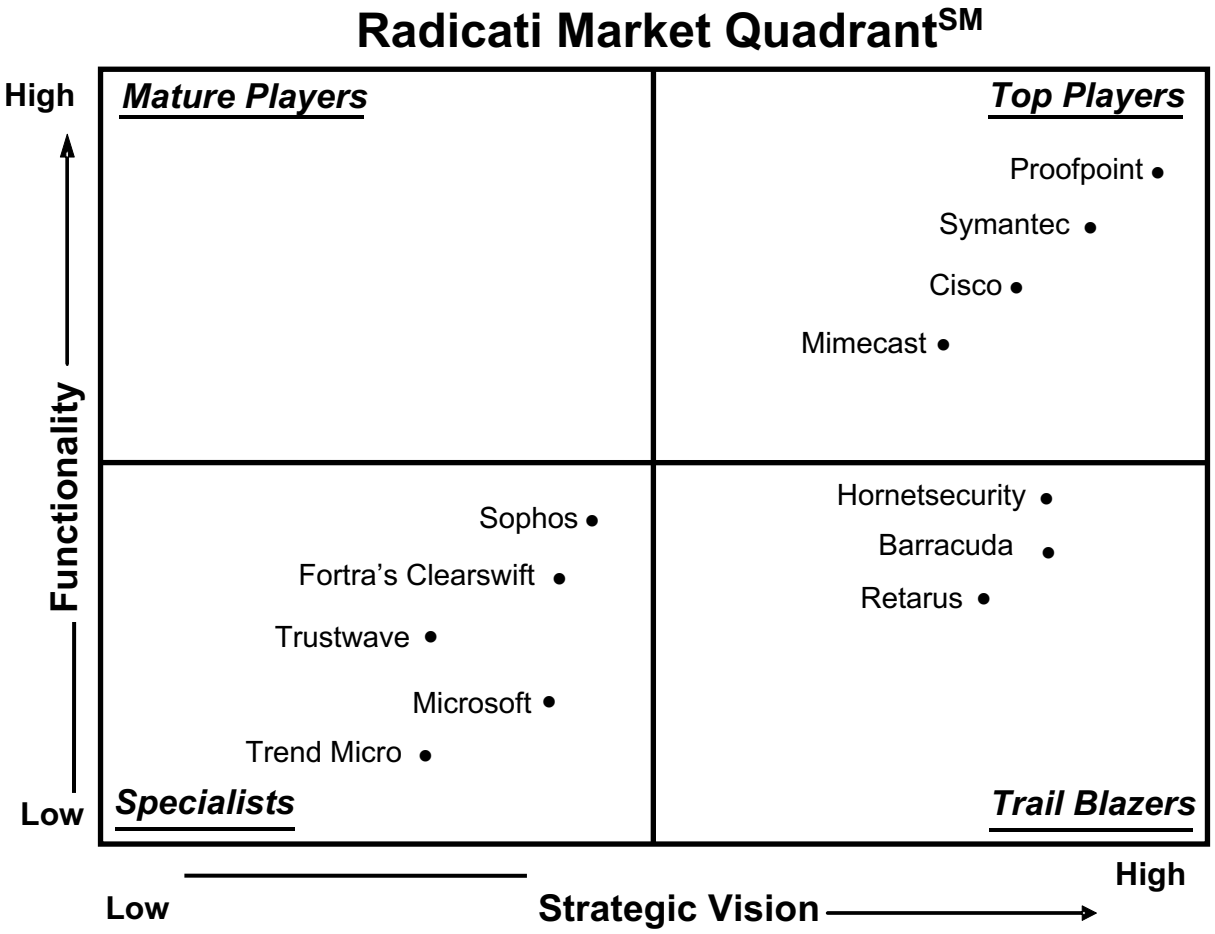


Figure 3: Secure Email Market Quadrant, 2023*

* Radicati Market Quadrant℠ is copyrighted March 2023 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 *Proofpoint, Symantec, Cisco, and Mimecast.*
- The **Trail Blazers** quadrant includes *Hornetsecurity, Barracuda,* and *Retarus*.
- The **Specialists** quadrant includes *Sophos*, *Fortra's Clearswift, Trustwave*, *Microsoft,* and *Trend Micro*.
- There are no **Mature Players** in this market at this time.

SECURE EMAIL - VENDOR ANALYSIS

TOP PLAYERS

PROOFPOINT

925 Maude Ave
Sunnyvale, CA 94089
www.proofpoint.com

Proofpoint delivers solutions for email security, data loss prevention, email authentication and monitoring, email encryption and archiving, social media protection, security awareness training, insider threat management and email archiving. In 2022, Proofpoint acquired several companies including Dathena, Intelisecure, and Illusive. Proofpoint is owned by investment firm Thoma Bravo.

SOLUTIONS

Proofpoint offers email security solutions as tiered bundles to stop phishing, business email compromise, malware and ransomware, and to identify and remediate compromised cloud accounts, and prevent data exfiltration. Proofpoint offers a wide choice of deployment options including cloud, dedicated appliance, virtual appliance, or a hybrid deployment. Proofpoint also offers an integrated cloud email security solution that allows companies to deploy using an inline API architecture without MX changes required.

Proofpoint Threat Protection – available as an integrated cloud email security or an on-premises or cloud-based gateway, prevents email-borne threats, including phishing, business email compromise (BEC) and ransomware/malware, with exhaustive search capabilities and visibility into all messages and threats. It offers the following capabilities:

- *URL and Attachment Sandboxing* – guards against phishing and ransomware attacks by analyzing all URLs and attachments in email and cloud-based applications. Analysis is done both statically and dynamically in Proofpoint's cloud-based sandbox, accurately identifying both widespread and highly targeted attacks. Suspicious URLs are proactively analyzed, re-written for additional analysis upon click and are sent to an isolated browsing session where content is accessed in read only mode to ensure that users are protected from 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 attacking them. Threat timeline and threat actor objective reports provide visibility into potential malware attacks by analyzing trends behind individual actors and threats.

- *AI/ML-Based Advanced Business Email Compromise (BEC) Defense* – Supernova (Proofpoint's next-gen AI-based detection engine), allows customers to uncover sophisticated email fraud and phishing attacks. AI/ML models analyze multiple aspects of email messages, such as header data, sender IP addresses, and the content of the email, including words/phrases commonly used in email fraud attacks. Behavioral models build unique user behavioral profiles which include an email recipient's halo of communication (e.g., who they communicate with and how often, as well as semantically what types of conversations they have). Any anomalies detected are combined with threat intelligence to detect and block complex social engineering attacks, including those which may utilize additional vectors such as phone calls. Granular details and forensics on BEC attacks are available to administrators in the management dashboard.

- *Actionable Insights* – 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.

- *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. The integrated security awareness training platform includes phishing simulations based on real-world threats, diverse training content across different security topics (e.g., passwords, internet and cloud, mobile devices, physical security, email) and a dashboard that provides at-a-glance view of program performance.

- *Email Authentication (DMARC)* – prevents fraudulent use of an organization's domain (spoofing) and protects the company brand from being used in fraudulent email attacks. This provides companies with more visibility into malicious lookalike domains or emails being sent using their domain, including third-party senders.

- *Automated 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. It also provides user feedback to help reinforce end user learning.

- *Account Compromise Detection* – monitors and detects account compromise from several sources, as well as detect suspicious behavior across cloud accounts. It also discovers and remediates identity vulnerabilities that can be used to move laterally or escalate privileges.

- *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.

- *Block Attacks through Personal Webmail* – Browser isolation integrations protect against inbound threats and data exfiltration originating from employee use of personal email accounts, such as Gmail or Outlook.com.

- *Outbound information protection* – provides controls for automated encryption and data loss prevention which protects against the loss of private or sensitive data including that associated with GDPR, HIPAA, PII or corporate email fraud.

- *Cloud Application Security Broker (CASB)* – offers visibility and control with a people-centric approach to protect users and safeguard sensitive data across both cloud and email

threats. It also helps discover shadow IT and govern the use of cloud and third-party OAuth apps.

STRENGTHS

- Proofpoint's unique process for identifying Very Attacked People (VAPs), enables security teams to understand their organization's human attack surface and implement a more effective security posture.

- Proofpoint's email security solution integrates with threat intelligence and forensics for information about malware, phishing, and email fraud, allowing security teams to better understand the threats, campaigns, and threat actors who carry out attacks.

- Proofpoint can protect against malicious URLs in attachments, and against 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 via prioritization, so administrators know which events to investigate.

- Automated remediation 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 best-in-breed secure email gateway and web security solutions, however, it does not offer endpoint protection. While Proofpoint does have partnerships with endpoint security vendors (e.g., CrowdStrike), customers wanting an integrated solution from a single vendor that combines secure email gateways and endpoint protection will need to look elsewhere.

- Customers indicate that while feature rich, Proofpoint Email Protection can be complex to install and maintain. However, Proofpoint does offer managed services for email security.

- Proofpoint's Threat Protection platform 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.

SYMANTEC

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

Symantec (a division of Broadcom Software) offers a wide range of security solutions (network, endpoint, information and identity) for the enterprise market. Symantec operates one of the largest civilian cyber intelligence networks, 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 two cloud based email security solutions, a messaging gateway solution and some feature add-ons as follows:

Symantec Email Security.cloud – a multi-tenant, cloud based email security service built to protect any combination of email deployments, including Microsoft Office 365, Google Workplace, 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 anti-spam services. This protection includes technologies, such as advanced heuristics, deep evaluation of links before email delivery, advanced phishing variant detection, and impersonation controls. It controls sensitive data and helps meet compliance and privacy requirements with built-in data loss prevention (DLP) and policy-based encryption policies. In addition, integration with the Symantec DLP solution enables more comprehensive DLP controls for protection of data across multiple channels.

Email Threat Detection, Response and Isolation (ETDRI) – is an enhanced email security service that extends Email Security.cloud's ability to detect targeted attacks, provide visibility into the attack landscape and therefore accelerate remediation. It also includes remote browser isolation capabilities to provide further protection against malicious weblinks and phishing attacks. 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. ETDRI 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. ETDRI 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 ETDRI, which allows customers to identify risky users and improve end user awareness through simulated phishing attacks. The license includes Symantec Email Threat Isolation, an integrated cloud based service that stops advanced email attacks by insulating users from spear phishing, credential theft, and ransomware attacks.

Symantec Email Fraud Protection – 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 Policy Based Encryption - Advanced – is an add-on that helps automatically safeguard the security and privacy of sensitive data sent through email allowing organizations to

deliver encrypted messages based on Symantec Data Protection policies using any of the available delivery methods; TLS, S/MINE, PGP, PDF (full message), PDF (attachments only), ZIP (attachments only), Office Native Encryption and the Secure Web Portal. The service enforces flexible rules in accordance with policies set in Email Security.cloud Data Protection. This hosted encryption solution allows organizations to protect sensitive information while removing the sometimes cumbersome task of managing digital certificates and encryption keys.

Symantec Messaging Gateway – 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, that takes data inputs from all Symantec's security products to provide protection intelligence across the portfolio (e.g. using file behavior on the endpoint to determine that files being sent by email are malicious).

STRENGTHS

- Symantec email security solutions are available as on-premises as well as cloud based solutions. Licensing options allow customers to combine these capabilities to also deploy hybrid scenarios. The solution includes support for air gapped (sensitive) networks by allowing off line signature and software updates.

- Symantec offers integrated threat isolation for corporate email, which helps prevent advanced email attacks such as spear phishing, credential phishing and ransomware. The threat isolation feature can also isolate suspicious attachments.

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

- 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 an integrated part of the Symantec Integrated Cyber Defense portfolio, the same portfolio that powers the Symantec Data-Centric Hybrid Cloud SASE strategy. This approach allows Symantec security solutions to better unify cloud and on-premises security.

- 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 through licensing bundles. 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 still needs to incorporate the ability to search and automatically remediate IOC's. The vendor is addressing this as part of its roadmap.

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, one of the largest commercial threat intelligence teams. Cisco is publicly traded.

SOLUTIONS

Cisco Secure Email (formerly Email Security Appliance and Cloud Email Security) provides layered protection that defends against phishing, spoofing, business email compromise and loss of sensitive information. It is available in several form-factors, including Cloud Gateway (SECG), Gateway (SEG), Virtual Secure Email Gateway (vSEG) for VMware and AWS, as well as a Hybrid (Cloud and On-Premises) solution. All gateway deployment options have feature parity.

In addition to the gateway offer, Cisco also offers **Secure Email Threat Defense** which integrates with Microsoft 365 through the Microsoft Graph API. It leverages advanced threat intelligence through Cisco Talos, uses artificial intelligence, machine learning, and natural language processing to detect advanced threats like BEC and account takeovers, and provides easy integration with other security tools through a RESTful API. Email Threat Defense offers a single interface for reporting, configuration and tracking. It provides full conversation and message trajectory views for full visibility into Microsoft 365 mailboxes to help protect against phishing, ransomware, and business email compromise. Secure Email is available in three licensing options:

- *Secure Email Essentials* – which delivers tools powered by Cisco Talos intelligence to quickly detect threats and quarantine suspicious messages.

  Secure Email Advantage – which includes all the features of Essentials plus enhanced data loss prevention (DLP). It allows administrators to create rules to prevent unauthorized data sharing and encrypt outbound messages.

- *Secure Email Premier* – includes all features of Advantage plus automated threat detection

and security awareness training.

Cisco's email security solutions comprise the following capabilities:

- *Spam & Threat Filtering* – Sender Reputation is the first layer of defense against all threats. It includes Sender IP Reputation filtering**,** and Sender Domain Reputation Filtering. IP Reputation provides dynamic protection against anomalous behaviors of the incoming IPs, hosts, domains, or senders based on intelligence gathered though honeypots and intelligence feeds. Content Scanning is performed by Context Adaptive Scanning Engine (CASE) and Talos Anti-spam Logic eNgine (TALN) engines, which leverage both heuristic and Bayesian scanning techniques to identify malicious characteristics of the email. Machine Learning techniques help identify calls for action or urgency of the email which are then fed into other BEC and Phishing models to strengthen verdicts for threat classification.

- *Anti-Phishing and Malicious URL Detection* – Cisco offers deep inspection of URLs in four distinct phases during the scanning of messages. URL Reputation Service (URS) identifies known bad URLs which are filtered as part of the CASE 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"). Cloud URL Analysis (CUA) is triggered via Threat Outbreak Filters**,** which use crawling and static analysis techniques to determine if a threat exists in the URLs payload or code. URL Rewrite & Web Interaction Tracking allows 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. Cisco Secure Email Threat Defense augments sender authentication and business email compromise (BEC) detection capabilities, through machine learning and behavior analytics. Secure Awareness Training provides phishing simulations and awareness training.

- *Anti-Spoofing* – includes Sender Domain Reputation which can determine if a well-known brand is being spoofed in the sender's email without having to create long lists of domains to monitor. Inbound message verification relies on DMARC, DKIM and SPF analysis to determine the legitimacy and authenticity of the sender and potentially block messages from being delivered. 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 sending domain validation of their own domains to prevent phishing and protect brands from fraud.

- *Malware Defense* – is provided through three distinct services: Secure Malware Analytics, Virus Outbreak Filters, and Anti-Virus.

- *Attachment Claw-back and Filtering* – Mailbox Auto Remediation automatically removes malicious files from inboxes supporting Microsoft Exchange 2016 and 2019, Microsoft 365 and hybrid deployments. 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. 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.

- *Threat Visibility and Investigation* – offers 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 as well as DANE support to provide effective detection of DNS poisoning attacks with TLSA support. Full payload encryption is available through the Cisco Secure Email Encryption Service (SEES), which provides both push and pull encryption. SEES 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. It integrates with the Secure Email Gateway to create differentiated policies for the repeated clickers who "failed" the phishing simulations most frequently.

STRENGTHS

- Cisco email security leverages threat intelligence capabilities from Talos, as well as customer generated intelligence to provide protection against both large scale and targeted attacks.

- Cisco email security integrates with the Cisco Secure Endpoint and with Cisco SecureX. This provides customers with visibility, control and automation from the network perimeter to the

endpoint.

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

- Cisco has focused on product simplification, which eases deployment complexity for customers across all sizes.

WEAKNESSES

- Currently, Email Threat Defense is only aimed at Microsoft 365 environments. Support for other email platforms is on the vendor's roadmap.

- Customers indicate that some of the management interface and reporting functionality could be improved for greater ease of use.

- Features such as Email domain protection (e.g., DMARC authentication), Image analyzer (to scan for adult image content), and Intelligent multi-scan (which combines results of multiple anti-spam classifiers) are only available as add-ons to Cisco Secure Email plans, whereas they are typically part of the baseline offering in many competing solutions.

- Cisco does not currently offer its own email continuity services, however, it offers archiving in partnership with Theta Lake.

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 offers a choice of two email security solutions **Cloud Gateway**, a traditional cloud based secure email gateway, and **Cloud Integrated**, which does not require and MX record change and is aimed at protecting Microsoft 365 environments.

The solutions offer a common set of security features and deliver the same level of protection from BEC, phishing, malware, greymail and spam. Additionally both solutions methods offer advanced impersonation protection with dynamic banners to enable end-users to make smart choices about their email security. URL re-writing and Targeted Threat protection are also available to all customers across both solutions. Alongside email security, Mimecast also delivers a broader product range which includes awareness training, DMARC management services and information archiving. All capabilities are currently available to Cloud Gateway customers, and planned for roll out to the Cloud Integrated solution. The cloud gateway solution provides larger customers with a high degree of configurability to manage scenarios such as mixed cloud and on-premise deployment, as well as multi-geographical deployment with complex mail routing requirements.

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 open API architecture with out-of-the box integrations to help customers surface email intelligence, share threats bi-laterally with security enforcement points and automate/orchestrate actions with SIEM, SOAR

and EDR/XDR systems (e.g. Splunk, IBM QRadar, Microsoft, Crowdstrike, and others). The API also allows customers to ingest their own threat data into their Mimecast tenant.

Mimecast Targeted Threat Protection extends 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 which is integrated into the Mimecast platform, offers security awareness training. 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.

Mimecast Email Incident Response includes AI-powered automation tools that analyze, triage and prioritize potential threats, and email meta data is enriched by intelligence from the Mime|OS platform. User-reported threats are routed to Mimecast's security operations center where they are automatically analyzed, triaged and prioritized for analyst classification and remediation.

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. Mimecast also integrates with Netskope to offer organizations an omnichannel DLP solution engineered to fully manage and secure inbound and outbound email, blocking questionable email and sensitive content based on DLP tags.

STRENGTHS

- Mimecast offers strong solutions 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 strategy combines multiple email security services in a solution framework to meet the needs of organizations, ranging from SMBs to large enterprises.

- Mimecast's solution integrates with the customer's Active Directory (AD) and Google Workspace 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 Workspace information is also used to detect potential employee impersonations in inbound emails.

- Mimecast solutions are attractively priced and offer flexible purchasing models that fit with the budget needs of customers of all sizes.

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.

- While Mimecast provides email security, along with email continuity and information archiving, it does not satisfy customers who may be seeking to acquire email security and endpoint protection from a single vendor. However, Mimecast does provide out of the box integrations with third party endpoint security solutions (e.g., Crowdstrike, Microsoft Defender and others).

- Some customers we spoke with as part of this research indicated that reporting could be improved to offer greater granularity.

TRAIL BLAZERS

HORNETSECURITY

6425 Living Place
Suite 200
Pittsburgh, PA 15206
www.hornetsecurity.com

Hornetsecurity is a global security, backup, compliance and awareness training provider for Microsoft 365, securing companies and organizations of all sizes worldwide. Hornetsecurity is headquartered in Hanover, Germany with 12 regional offices and operates through an international network of channel partners, MSPs and 11 redundant, secured data centers. 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. Hornetsecurity also offers backup, replication, and recovery solutions, with a particular focus on Microsoft 365. In 2022, Hornetsecurity acquired IT-Seal, a security awareness training company, to provide customers with automated, needs-based awareness training, based on a patented spear phishing engine.

The company offers the following suite of services:

- **365 Total Protection** – offers protection for Microsoft 365 and Microsoft cloud services. It is available in four versions Business, Enterprise, Enterprise Backup, and Enterprise Compliance and Awareness.

    - The **Business edition** (Plan 1) comprises the following features:

- *Threat Detection* – multi-stage in-depth analysis and filter systems detect and block spam and virus threats.
- *Global S/MIME and PGP Encryption* – protects the entire email communication from being altered or read by third parties without authorization.

- The **Enterprise edition** (Plan 2) adds:
  - *Forensic Analyses* + AI – 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* – 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.
  - *Email continuity* – provides a stand-by system that can be activated within seconds, enabling employees to continue to communicate smoothly in the event of an infrastructure failure.
  - *Email archiving* – stores emails in a revision-proof and legally compliant manner in secure Hornetsecurity data centers.

- The **Enterprise Backup edition** (Plan 3) adds data loss prevention (DLP) functionality through:
  - *Automatic backup of M365 data* – backs up M365 user and group mailboxes, Teams Chats, SharePoint document libraries, OneDrive business accounts, with various restore options for quick and easy recovery.

- *Endpoint backup* – backs up files on users' roaming and on-premises endpoints such as laptops and desktop computers.

- The **Enterprise Compliance and Awareness edition** (Plan 4) adds phishing attack simulations, security awareness service, an employee security index; permission management, alerts and auditing, as follows:
  - *Next-Gen Security Awareness Training Service* – serves to train employees using spear phishing simulations and AI-powered training.
  - *365 Permission Manager* – allows administrators to more easily manage Microsoft 365 permissions, enforce compliance policies, and monitor violations. It also helps administrators monitor compliance states and audit policy violations, which helps organizations maintain compliance with internal and external regulations and policies.

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

- **Spam and Malware Protection** – offers detection of 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 (Secure Links), rewriting, sandboxing, and Malicious Document Decryption to safeguard IT infrastructures against advanced threats like Emotet, CEO fraud, Ransomware or scanning of malicious content hidden in QR codes.

- **Email Continuity Service** – supports uninterrupted email 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.

- **Security Awareness Training** – can also be purchased as a standalone service.

- **365 Permission Manager** – is a Governance, Risk & Compliance (GRC) Software tool that allows users gain a full overview of their M365 file permissions across SharePoint Online, OneDrive, Microsoft Teams, and Microsoft 365 Groups.

Hornetsecurity also offers a **Mailbox Migration Tool**, which helps partners transfer customer mailboxes from on-premises to the Microsoft 365 cloud.

STRENGTHS

- Hornetsecurity's 365 Total Protection offers email security, backup, and compliance in an easy-to-use package and an attractive price point aimed at Microsoft 365 customers of all sizes.

- Hornetsecurity's automated training service, based on a patented spear phishing engine is simple to use, and offers individually customized, needs-based training to users.

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

- Coupled with the email protection, Hornetsecurity also offers data loss prevention capabilities for Microsoft 365 and Windows endpoints, providing a single vendor solution managed through a single pane of glass.

- 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.

WEAKNESSES

- Hornetsecurity 365 Total Protection is aimed at Microsoft 365 customers, rather than being email platform agnostic.

- While Hornetsecurity is currently well known in Europe, so far it has been less visible 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 offers basic DLP features integrated with its solutions, however customers with advanced DLP requirement may wish to look at adding best-of-breed DLP solutions.

BARRACUDA NETWORKS

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

Barracuda Networks, founded in 2003, provides email protection, content, network and application security, and data protection services to business organizations. Barracuda Networks is a privately held company, owned by investment firm Kohlberg Kravis Roberts & Co (KKR).

SOLUTIONS

Barracuda offers email protection solutions through flexible deployment options which include cloud-hosted, hardware appliances, virtual appliances, and public cloud instances (e.g., AWS, Azure, vCloud Air). Barracuda offers these solutions through three (Software-as-a-Service) SaaS plans *Advanced, Premium,* and *Premium Plus.*

- **Barracuda Email Protection Advanced –** protects users from email threats with a secure email gateway combined with artificial intelligence. Capabilities include:

  - *Spam and Malware Protection* **–** identifies and blocks spam, viruses, and malware delivered via email messages.

  - *Attachment Protection* **–** combines behavioral, heuristic, and sandboxing technologies to protect against zero-hour and targeted attacks. A sandbox environment is used to detonate and observe the behavior of suspicious attachments.

  - *Link Protection* **–** automatically rewrites URLs so that Barracuda can sandbox the request at click time to block malicious links.

  - *Email Continuity* **–** in the event of a mail server or service outage or loss of connectivity, an emergency mailbox lets users continue to send and receive emails.

  - *Phishing and Impersonation Protection* **–** automatically detects and prevents impersonation, business email compromise, and other targeted attacks. Barracuda's AI engine learns each organization's unique communication patterns and leverages these

patterns to identify anomalies and prevent socially engineered attacks in real time.

- *Account Takeover Protection* – stops phishing attacks used to harvest credentials for account takeover. AI detects anomalous email behavior and alerts IT, then finds and removes all fraudulent emails sent from compromised accounts.

- *Automatic Remediation* – all user-reported messages are automatically scanned for malicious URLs or attachments. When a threat is detected, all matching emails are automatically moved from users' mailboxes into their junk folders.

- *Email Encryption* – secures email by encrypting it during transport to the Barracuda Message Center, encrypting it at rest for storage in the cloud, and providing secure retrieval by recipients through HTTPS web access.

- *Data Loss Prevention* – supports the creation and enforcement of content policies to prevent sensitive data, from being sent by email. Policies can automatically encrypt, quarantine, or block certain outbound emails based on their content, sender, or recipient.

- **Barracuda Email Protection Premium** – includes all features in Advanced, plus automated post-delivery email incident response. Capabilities include:

  - *Threat Hunting and Response* – helps quickly identify and remediate post-delivery threats by automating investigative workflows and enabling direct removal of malicious emails.

  - *Automated Workflows* – supports building of custom playbooks to completely automate the incident response process.

  - *Domain Fraud Protection* – prevent email domain fraud with DMARC reporting and analysis. Barracuda provides granular visibility and analysis of DMARC reports to help minimize false positives, protect legitimate email, and prevent spoofing.

  - *Web Security* – protects users from accessing malicious web content with advanced DNS and URL filtering.

- *SIEM/SOAR/XDR Integration* – helps orchestrate incident response cross-product with RESTful API (beta) and Syslog integrations.

- **Barracuda Email Protection Premium Plus –** includes all features in Premium, plus protection for Microsoft 365 with user training, data protection, email archiving, and zero trust access. Capabilities include:

  - *Zero Trust Access for Microsoft 365* – reduces exposure to lateral attacks on Microsoft 365 applications and helps mitigate breach risks for remote employees and contractors.

  - *Attack Simulation* – simulated phishing attacks are constantly updated to reflect the most recent and most common threats.

  - *Security Awareness Training* – offers advanced, automated education technology that includes simulation-based training, continuous testing, reporting for administrators, and active incident-response awareness.

  - *Cloud Archiving* – a cloud-based, indexed archive that supports granular retention policies, extensive search, role-based auditing/permissions, legal hold, and export.

  - *Cloud-to-Cloud Backup* – data protection and cloud backup for Microsoft 365 data, including Exchange Online mailboxes, SharePoint Online, OneDrive for Business, and Teams.

  - *Data Inspector* – automatically scans OneDrive for Business and SharePoint data for sensitive information and malicious files containing malware.

STRENGTHS

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

- Barracuda provides 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 Incident Response tool, which gives IT control on responding to unique use cases and eliminates manual and repetitive tasks.

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

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

- Barracuda Security Awareness Training offers extensive tools and techniques for user security awareness training, helping to embed training in everyday user activities, and integrates natively with Incident Response to make just-in-time training possible for VIPs and very-targeted employees.

WEAKNESSES

- Barracuda offers native DLP capabilities with its email security solutions, however these do not currently integrate with any third-party tools. Customers with advanced compliance needs should check carefully whether the features offered fit their data loss protection requirements.

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

- While Barracuda's management interface for Impersonation Protection and Email Gateway Defense has been improved through greater data visualization and an improved UI, the vendor still has a number of improvements relating to this on its roadmap.

RETARUS

Aschauer Strasse 30
81549 Munich, Germany

Retarus, founded in 1992, enables efficient and secure business communication for companies worldwide via enterprise-level cloud solutions. Retarus is based in Germany, with offices in Europe, the USA, and APAC. The company is privately held.

SOLUTIONS

The Retarus **Secure Email Platform** is a comprehensive cloud-based solution aimed at large and mid-size organizations to help protect against sophisticated threats, including business email compromise and identity theft, phishing, ransomware attacks, social engineering, and others. Retarus is highly available with built-in redundancy via multiple data centers. Retarus offers a fully European option for GDPR sensitive customers.

Key email security features of the Retarus Secure Email Platform include:

- *Essential Protection* – provides a layer of protection using antivirus and antispam engines to offer end-to-end protection from phishing and spoofing, as well as inbound traffic management. Retarus supports and validates SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) as well as DMARC (Domain-based Message Authentication, Reporting and Conformance).

- *Advanced Threat Protection* – delivers increased security aimed at addressing new complex threats involving social engineering and targeted attacks. It delivers a comprehensive set of features for anti-phishing, antivirus, antispam, CXO Fraud protection (BEC), as well as malware detection through multi-vendor data sources and Retarus' own technology.

- *Sandboxing* – offers in-depth analysis of specific file attachments, including AI/ML algorithms and heuristics to identify "zero-day attacks". It is based on technology from Palo Alto Networks, hosted and managed in Retarus data centers to ensure data protection and compliance.

- *Post-Delivery Protection* – is a patented and self-developed Retarus technology which allows early recognition and alerting of previously unknown malware and phishing URLs. It uses

digital fingerprinting (i.e., a hash of metadata and URL/attachments) to back-track, detect and automatically claw back any threats in emails that have already been delivered.

- *Retarus Enterprise Administration Services Portal (Retarus EAS Portal)* – provides administrators with transparency and detailed message tracking on a message-level. Reporting can be integrated with SIEM, M/SOAR and training solutions.

- *Quarantine portal* – is an easy-to-use tool which helps educate users about the potential risk posed by each message blocked, including a secure preview mode for all quarantined emails. Threats are displayed distinctly from messages that were filtered out due to self-configured rules. The user interface is available in eleven languages.

In addition, Retarus provides the following email compliance features:

- *Archiving* – offers tamper-proof compliance archive (retention) for business email in real-time, for both internal and external messages and their attachments. Including access and change logging as well as fast search.

- *Encryption* – key-based encryption is provided via S/MIME, PGP and OpenPGP at the gateway level. Additional password-based encryption is available via the Secure Webmailer service which allows to include recipients without an encryption solution in place.

- *DLP* – checks emails addressed to external recipients systematically against pre-defined criteria and helps prevent loss of internal and confidential information. Specific rules regarding permitted recipients can be defined at the mailbox level, an integrated attachment blocker can also prevent the sending of specified files or file formats.

Retarus also offers a rich range of additional infrastructure services which include:

Predelivery Logic – allows companies to consolidate and protect their email environments by organizing, editing, and routing messages based on custom security rules.

Email Continuity – offers cloud-based webmail backup providing ready-to-use, pre-provisioned inboxes and access to the company address book. It is designed to be intuitive and mobile-friendly.

Transactional Email – is as an additional service for the delivery of high-volume emails generated by business applications (e.g., CRM systems). The service includes advanced mechanisms for improved deliverability rates, enhanced security, detailed tracking and secure document handling options.

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 message tracking, 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 with headquarters in Germany, Retarus offers cloud services that are fully GDPR compliant.

WEAKNESSES

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

- Retarus offers email encryption through its Retarus Email Encryption module. However, this an extra cost item.

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

- Retarus does not currently offer user phishing awareness training, which is becoming popular with many competing solutions. The vendor is working to address this through its partner

network.

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

SPECIALISTS

SOPHOS

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

Sophos offers IT security solutions for businesses, which include endpoint, encryption, email, next-generation firewall (NGFW), mobile security and unified threat management. All solutions are managed through Sophos Central, a cloud-based management platform, backed by Sophos X-Ops, its global threat intelligence network. Sophos is owned by private equity firm Thoma Bravo and headquartered in Oxford, U.K.

SOLUTIONS

Sophos Email uses a combination of detection methods and machine learning, to protect against malware, spam, phishing impersonation attacks, and data loss. It 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 from Sophos Labs, which enables it to detect both known and unknown malware without having to rely on signatures. The product can also identify sophisticated Business Email Compromise (BEC) attacks through message body content and subject line analysis to identify conversations with suspicious content. Sophos Email works with Microsoft Exchange Online, Microsoft Office 365, Google Workspace, and any other email solution.

Sophos Email is managed through Sophos Central, a single SaaS-based console for all Sophos products. Sophos Email security solutions are deployed in the cloud, and support both cloud-based and on-premises email services. There are two deployment options:

- Sophos Mailflow – integrates directly with Microsoft 365 using the Microsoft Exchange Connector Services to scan the emails.

- Sophos Gateway – integrates with email solutions via an MX Record update to route email traffic through the Sophos Email gateway.

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 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 integrated cloud-based management console that enables organizations to manage a layered defense including email, network security, next-generation endpoint and server protection with XDR, mobile device protection, encryption, wireless, a range of public cloud security solutions including cloud security posture management, and a human-led Managed Detection and Response team.

- *Cybersecurity Awareness Training* – Sophos Synchronized Security connects Sophos Email with Sophos Phish Threat, its phishing attack simulation and security awareness training solution. It can identify users that have been blocked or warned from visiting high risk profile websites, and seamlessly enroll them into targeted phishing simulations and training.

STRENGTHS

- Sophos Email's Advanced Threat Report 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 Managed Detection and Response (MDR) provides fully managed service, delivered by Sophos experts who detect and respond to cyberattacks targeting a customer's email accounts, servers, networks, cloud workloads and computers.

- Sophos Email integrates with the Sophos Phish Threat service to provide phishing simulations and security awareness training in the same console.

- Sophos Central offers a single integrated cloud-based management console to manage a layered defense which includes email, network security, next-generation endpoint and server protection with XDR.

WEAKNESSES

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

- Sophos offers phishing awareness training integrated into Sophos Central, however this requires a separate license.

- 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.

FORTRA'S CLEARSWIFT

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

Fortra is a cybersecurity software company which offers solutions for detecting, inspecting, and securing critical data over email, web, and the cloud. In 2019, Clearswift was acquired by HelpSystems, a U.S.-based company, and after a rebrand is now known as Fortra. Clearswift solutions are part of Fortra's Digital Risk and Email Protection group. Fortra is owned by private equity firms TA Associates, Charlesbank, HGGC and Harvest Partners.

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 antivirus engines from Sophos or Avira, as well as a hosted Sandbox from Sophos. 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's active code detection mechanisms that identify, 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.

Anti-spam 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 where URLs are checked against multiple real-time phishing and malicious URL feeds. It also applies heuristics to detect phishing exploits. URLs can be rewritten to redirect to browser isolation solutions to provide additional "time-of-click" protection.

The Gateway scans messages of any language in either direction based upon a granular policy. There is a policy engine that performs message and attachment decomposition and 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. This functionality is known as Adaptive Redaction and covers three areas: data redaction, document sanitization, and structural sanitization.

Data redaction permits the modification of multiple formats, including text, HTML, PDF, Office, and OpenOffice, and allows textual modification by replacing keywords and phrases with asterisks "*". For credit card information, all but the last 4 digits are replaced. Data redaction can also be performed on document footers/headers, watermarks, and tracking comments. As well as providing DLP, the bi-directional scanning also protects against unwanted incoming data acquisition, the receipt of which can cause issues for compliance with GDPR. Redaction of text in images is also available through optical character recognition (OCR). In this case the redacted text is "black-boxed" from the image (rather than a separate object being overlayed), to ensure it cannot be recovered.

Document sanitization allows for document properties such as author, subject, status, etc. to be removed. Other important information, such as data classification labels, can be whitelisted so they are excluded from the sanitization process. Sanitization can also remove potentially embarrassing change tracking comments which may carry data that could lead to a data breach. Anti-steganography is available to ensure that hidden data cannot be exfiltrated and hidden malware cannot enter the organization.

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 mail, 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 encryption types. 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 and on-premises solutions. An optional digital rights management (DRM) solution is also available.

The Gateway can be peered with other email gateways to form a "cluster" for scalability and availability purposes, and with Microsoft Exchange or Microsoft 365, to provide additional internal email inspection and DLP functionality, or with web gateways to provide a consistent policy across multiple communication platforms.

STRENGTHS

- Fortra's wider data security portfolio allows customers to also obtain secure file transfer, data classification, and digital rights management products from the same provider. Integration of these products into a centralized console is underway.

- The solution integrates with the Clearswift Secure Web Gateway to help combat increasingly sophisticated threats, such as Dynamic malware on URLs.

- The solution can scan internal email traffic as well as traffic that crosses the organizational boundary. This includes both on-premises Exchange installations, as well as Microsoft 365.

- Clearswift's Secure Email Gateway forms the basis of a channel DLP solution when coupled with Clearswift Secure Web Gateway, customers looking for an Endpoint or Network-based DLP solution can add Fortra's Digital Guardian.

- Clearswift offers Adaptive Redaction features in all its gateway products. This includes image redaction and anti-steganography features. Comprehensive Adaptive Redaction is a differentiator which is generally not available in competing products.

- Clearswift offers phishing awareness training through Fortra's Terranova Security training suite.

WEAKNESSES

- Fortra offers an impressive set of solutions through its Clearswift Secure Email Gateway, Agari Phishing Defense, PhishLabs, and Terranova phishing awareness training. However the vendor is still working to offer a fully integrated experience and a consolidated user interface across all solutions. The vendor has this on its 2023 roadmap.

- Clearswift Secure Email Gateway would benefit from more support for customized threat feeds. The vendor is working to add threat feeds from other areas of the Fortra product portfolio (e.g., Agari, PhishLabs and Core Impact) to improve efficacy.

- Reporting could be improved, through more granularity and greater customization. The vendor has this on their roadmap through the development of a new product portal.

- Clearswift's Secure Email Gateway would also benefit from improved SOAR capabilities as more customers are interested in automating policy definition and updating threat resources using their own feeds.

- Although Clearswift offers strong email security solutions, and the acquisition by Fortra has extended exposure to Fortra' customers in North America, the vendor is still less visible than other competing vendors in the secure email gateway market.

TRUSTWAVE

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

Trustwave Holdings is a cybersecurity security provider of managed detection and response (MDR), managed security services (MSS), database security, and email security. Trustwave Holdings is a standalone business unit and independent subsidiary of Singtel Group Enterprise.

SOLUTIONS

Trustwave **MailMarshal** delivers a range of email security and management features, based around business email compromise (BEC) protection and a flexible policy engine. MailMarshal threat protection is backed by the dedicated SpiderLabs team focused on email security research. The solution can be deployed on-premises, in the cloud, or as a hybrid cloud solution. The MailMarshal Cloud platform is located globally to meet the needs of customers in their geographic locations.

Trustwave MailMarshal 10.0.3 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. The latest version includes an improved Management Console with enhanced email inspection and reporting.

Trustwave **MailMarshal On Premises**, 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. The solution also goes beyond email security to provide a flexible policy engine which can be used as an 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.

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

Customers can combine the on-premises and cloud solution into hybrid scenarios. Trustwave MailMarshal 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 several features that are available as bundled offerings, or optional add-ons to MailMarshal, as follows:

- **Email Archiving** – is available to any MailMarshal 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.

- **Advanced Email Encryption** – services allow customers of MailMarshal, 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. MailMarshal can be used to intelligently scan email for confidential information, based on customer-defined policies, as well as encrypt sensitive messages.

- **Malware Analysis Sandbox** – proactively prevents advanced malware and provides a safe environment in which to execute and observe malicious code or to encourage threats into exposing themselves. It helps reduce the amount of time between infection and remediation, mitigates the risk of breaches, and detects zero day or unknown attacks.

- **Advanced Threat Protection** – 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. It is a standard module in MailMarshal Cloud.

- **Image Analyzer** – 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 MailMarshal supports several third-party antivirus scanners to scan for virus or malware laden email, these include solutions from Sophos, McAfee, Kaspersky, and Bitdefender. Trustwave MailMarshal also fully supports a Yara-based malware engine that offers additional capabilities to detect malicious attachments. Sophos is included in all MailMarshal On Premises and Cloud bundles.

- **MailMarshal Internal SMTP Toolkit (MIST)** – is a Microsoft Windows-based SMTP Toolkit that can handle complex SMTP routing and internal operational business needs via a scalable software solution. It addresses the needs of businesses may have moved to the cloud but still need to maintain systems that transmit email for operational purposes, or need to exchange emails directly with third party providers that integrate with business applications.

STRENGTHS

- Trustwave MailMarshal 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 Microsoft 365. MailMarshal also provides the ability to decrypt email and enforce all RMS outbound policy controls before re-encrypting the email and sending it.

- Trustwave MailMarshal 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 dedicated SpiderLabs team, and Trustwave's threat intelligence Fusion platform.

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

WEAKNESSES

- While Trustwave MailMarshal has improved its reporting features, however, more improvement in this area with greater granularity and deeper customization options would still be beneficial.

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

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

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

MICROSOFT

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

Microsoft offers products and services for businesses and consumers, through a portfolio of solutions for office productivity, messaging, collaboration, and more.

SOLUTIONS

Microsoft Exchange Online Protection (EOP) is Microsoft's email security solution which is an integral part of Microsoft Office 365. It helps protect against spam and malware and includes 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 **Microsoft Defender for Office 365** (formerly Office 365 Advanced Threat Protection), **Data Loss Prevention (DLP)**, and **Office 365 Message Encryption** for a more fully featured security solution.

- **Microsoft Defender for Office 365** – is a cloud-based email filtering solution that provides protection against phishing, malware, and spam attacks. It offers near real-time protection

against high-volume spam campaigns, with DKIM and DMARC support. It also adds protection against "zero-day" attachments and harmful URL links, through real-time behavioral analysis and sandboxing. It can be deployed as an add-on to on-premises Microsoft Exchange Server deployments, Microsoft Exchange Online cloud mailboxes, or hybrid environments. It is available in 2 plans.

Microsoft Defender for Office 365 Plan 1 provides the following capabilities:

- *Safe Links* – provides time-of-click verification of URLs in email messages and Office files.

- *Safe Attachments* – provides zero-day protection against unknown malware and viruses. Suspicious messages and attachments are routed to a special environment where machine learning and analysis techniques are used to detect malicious intent. If no suspicious activity is detected, the message is released for delivery to the mailbox.

- *ATP for SharePoint, OneDrive and Microsoft Teams* – can be turned on to help detect and block malicious files in team sites and document libraries.

- *Anti-phishing protection* – detects attempts to impersonate user and internal or custom domains. It applies machine learning to block phishing attacks.

- *Advanced reporting dashboard* – provides real time threat detection reports with recommendations and alerts to imminent threats.

Plan 2 adds the following capabilities:

- *Threat investigation and response tools* – which include Threat Trackers to deliver intelligence on prevailing cybersecurity issues; Threat Explorer for real-time reporting detection; Automated Investigation and Response (AIR) to support automated investigation and response to well-known threats; Attack Simulation training, and cross-domain XDR capabilities.

Microsoft Defender for Office 365 Plan 1 is included in Microsoft 365 Business Premium. Microsoft Defender for Office 365 Plan 2 is included in Office 365 E5, Office 365 A5, and Microsoft 365 E5. Both Plan 1 and Plan 2 are also each available as an add-on to certain

subscriptions. A *Safe Documents* feature, which allows viewing of documents in a protected state, is only available with the Microsoft 365 E5 plan, or Microsoft 365 E5 Security licenses.

- **Purview Data Loss Prevention (DLP)** – Microsoft 365 E3 includes DLP protection for SharePoint Online, OneDrive and Exchange Online. It also includes protection for files shared through Teams because Teams uses SharePoint Online and OneDrive to share files. DLP protection in Teams Chat requires an E5 license. The Microsoft Purview Compliance Center (formerly Microsoft Compliance Center) provides a central policy management console that allows administrators to manage DLP policies across different services. The DLP on-premises scanner extends DLP protection to on-premises file shares and SharePoint document libraries.

- **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 Microsoft Defender for Office 365, 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 Microsoft Defender for Office 365 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 often difficult for customers to understand exactly what security features they are getting with what plans.

- Microsoft offers a rich ecosystem of security solutions, however, integrating all components correctly and maintaining them fully integrated throughout Microsoft's continuous upgrade cycle can be daunting for many organizations.

- As a purely cloud-based solution, Microsoft Defender for Office 365, is not applicable to customers with purely on-premises deployments or air-gapped networks.

- 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 email 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 security solutions for organizations, service providers, and consumers. Trend Micro's cloud-based Smart Protection Network brings together threat reporting and analysis based on a worldwide threat assessment infrastructure. Trend Micro is publicly traded.

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 Vision One 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 365, Google Workspace, and other hosted and on-premises email solutions. It offers Business Email Compromise (BEC) protection and offers flexible user profile definitions. It is available in two bundles: Standard, and Advanced (which adds sandboxing, AI-based fraud/BED detection, and email continuity).

- **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 Microsoft 365, Google Workspace, Salesforce, Box, and Dropbox. 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 IBM Domino** – offers malware and spam protection as a native Domino server application.

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

- **IM Security for Microsoft for Business Server** – on-premises software to protect Microsoft Skype for Business Servers from malware, web threats, content violations and data loss.

Trend Micro offers a range 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 (cloud and on-premises) in 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 DLP functionality, 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**
- **Social Media**
- **Instant Messaging**
- **Archiving & Compliance**
- **Wireless & Mobile**

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:

- Strategic Business Planning
- Management Advice
- Product Advice
- TCO/ROI Analysis
- Investment Advice
- Due Diligence

MARKET RESEARCH PUBLICATIONS

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

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