On the Surface

- No additional hardware or software required to achieve 99.9%+ spam and malware filtering effectiveness
- Initiate service by changing MX Record to point to the Email Security service
- Automated daily configuration check to ensure optimized protection
- Office 365-compatible
- Outbound filtering included
- Full security management for administrators through a consolidated portal with Two-Factor Authentication (2FA)
- Integrated Mobile First web design for the Dashboard and Impersonation Protection sections
- Modern dashboard that spotlights phishing and malware threats

venza® msp

Functional Benefit

Impersonation Protection Technology

- Flags the message with a customizable indicator "Suspected Impersonation" or quarantines the message
- Verifies source against email addresses provided for key display names
- Checks incoming display names against the associated email addresses

Quarantine – categorized by Spam, Malware, Released Mail and Trash

- Searchable by date range, from/to, subject, country, attachment
- Retention period from 14 to 30 days, depending on domain settings
- Easily release valid messages to inbox
- Safely view and analyze captured emails, including the ability to show raw messages, view header information, check against RBLs, check the IP address, download message for further analysis and more
- Quarantined Alerts – A smart filter that analyzes your email history to ensure a potentially valid message doesn't become quarantined without your knowledge

Daily Quarantined Message Report

- Provides listing of all quarantined mail with an option to hide known sources of junk from your quarantined list with the Declutter feature
- Configurable by end-user
- Selectable receipt interval (from none up to multiple times daily)
- Sent to each end-user's inbox
- Allows message viewing/analysis and release directly from within the report

Domain Statistics Report

- Sent weekly to administrator and any other chosen recipient(s)
- Contains domain-specific statistics, including allowed list requests, message type counts, spam categories, spam and virus frequency by email address and more

Outbound service that scans and filters outgoing messages for spam and malware

Integrated Lightweight Directory Access Protocol (LDAP)

- Allows your active directory to be automatically synced on a set schedule with Email Security, ensuring your spam and malware service is always available to your current user base
- Promotes active directory health, which is beneficial to system efficiency
- Eliminates effort on part of administrator to keep up with company turnover in regards to active directory
- Works with multiple server types and can schedule automatic imports in intervals from 1- to 24-hour increments
- Does not transfer password information

Convenient Scan options

- Certain file extensions, link extensions and document macros can be globally blocked from reaching your network
- Messages from unknown sources or with unknown URLs can undergo more stringent analysis before being delivered to your network

Customizable mail rules

- Easily configured and set through a simplified interface
- Processed and applied based on conditional criteria set by administrator
- Includes conditions, such as recipient, sender, subject, body, headers, country and more with multiple parameter types to ensure valid and effective rule processing
- Contains many actions if conditions are met, including hold, allow, delete, bounce, copy, forward and more

Disclaimer feature allows administrator to assign a set statement on all inbound and outbound messages

Log search function for administrators

- Provides an efficient method for administrator to easily trace a message path through the network
- Viewable and searchable in the Customer Portal up to 14 days and 2,500 messages
- Inbound and outbound messages included
- Logs color-coded according to filtering result for ease of review
- Quickly export up to 50,000 messages to CSV for offline analysis
- Utilizes real-time country-to-IP mapping
- Ability for administrator to view logs according to time zone of specific user

Bulk Add Users to quickly and easily add up to 100 users at a time

Delivery Queue

- Shows status of any message(s) that has not been accepted by your mail server
- Provides the ability to reject or release any problem message, as well as greater visibility to troubleshoot mail server issues on either end of the delivery

Export Email Addresses

- Easily export all email addresses associated with the domain into a CSV file
- Useful to verify completeness after import process
- Lists all types, whether as Public Folder, Resource, User, Alias, etc.

Filtering Expertise

Contains several customizable filter settings to give more granularity in regards to the effectiveness and efficiency towards your domain(s)

- Allowed Lists can be easily submitted by end-users and managed by administrator
- Bulk Add filters can simplify adding multiple email or IP addresses, domains, file names, text or specific countries to allowed or blocked list

- Also can individually add allowed or blocked email or IP addresses, domains, filenames, text or specific countries
- Quick summary of domain filter settings is also available to the admin, as well as CSV settings export

Tiered filter permissions easily configured and managed by admin

- Four tiers: Domain Blocked List, User's Blocked List, Domain Allowed List, User's Allowed List
- User permissions may be set to supersede domain permissions if necessary and approved by administrator

Open, Closed, and Controlled Domain mode options, based on specific needs

Open mode

- Accepts mail for all users, regardless of whether or not they exist on user list for the domain
- Supported with a 14-day quarantine retention period
- New mode that provides admins with more user alias management flexibility

Closed mode

- Holds email received from unknown addresses and keeps from entering the system if not on user list for the domain
- Supported with a 30-day quarantine retention period if Closed mode is set to delete messages from invalid users
- New mode that provides admins with more user alias management flexibilty

Over sixty different filtering tests, including:

- Bulkmailer (gray mail) – allows mail received as a bulk mail campaign to be sorted into a more convenient folder than the inbox
- Spearphishing – one of the industry's first tests, designed to avoid Business Email Compromise (BEC) by utilizing AppRiver's proprietary detection technology.
- Additional content tests designed to identify scams, adult phrases, header issues, bounced messages, encoded subjects, byte signature scanning, forged mailers and/or routes, client side scripts in HTML, redirects, suspicious URLs, maximum invalid users, no legitimate content, phishing, all forms of message obfuscation, spam phrases, tracking bugs and more
- Sender Policy Framework (SPF) verification – set to either hard or soft rules
- DomainKeys Identified Mail (DKIM) protocol verification – checks the DKIM signature with a public key
- Domain-Based Message Authentication Reporting & Conformance (DMARC) verification – checks SPF and DKIM authentication and alignment
- Additional sender verification checks including ISP, return path domain, HELO, reverse DNS, forged domains and more
- Profiles that check for specific regional dialects and characters

- Weight checks that can be dialed up or down to filter more or less aggressively

Situational Awareness

Domain-level statistics provided for previous 30 days to assist with identifying issues before they become trends

- Message count
- Message size
- Message type
- Countries (of message origin)
- Recent users on domain
- Export quarantine logs to CSV file

Behind the Curtain

- Phish Finder Advanced Threat Intelligence that identifies and addresses brand-spoofing, phishing attacks
- Proprietary technology that is highly effective against conversation hijacking
- Utilizes five anti-virus engines (two proprietary)
- Reaches beyond typical machine-learning algorithms with real-time dynamic behavioral analysis, automation, sandboxing and link detonation
- Increases effectiveness with more than 8 million rules written by technicians, who monitor and proactively adjust Email Security defenses 24 hours a day, 365 days a year against emerging threats
- Continuously engages with several threat intelligence feeds (including our own) to help improve situational awareness
- Uses integrated blocked list feeds, both proprietary and 3rd party

Email Security is a cloud-based Anti-phishing and malware filter that's designed to keep your inbox clean and your network safe. A simple MX Record change routes your mail through the Email Security servers before it ever reaches your network, which ensures that the mail that reaches your network doesn't pose a threat. While our solution contains numerous adjustable settings, it is designed to work efficiently and optimally with little or no interaction from administrators. Please consult our team with any questions you may have about Email Security and your specific situation.

venza® msp