MSecurity System™ Content, Threat, and Ransomware Protections

MSecurity System is a cloud solution that defends email users against advanced email borne threats, spam viruses, impersonation attempts, and malicious URLs attachments.

MSecurity System includes detection of phishing and fraudulent emails. Gateway services detect WannaCry as soon as it appears, without the need to additionally update the database.

With powerful antivirus filtering and email management, MSecurity delivers policy based layered protection to address email threats and prevents Personally Identifiable Information (PII) data leaks for large enterprises and SMEs.

Available with email continuity archiving featuring advance eDiscovery search for PII to Identify, Classify, Encrypt & Protect.

Gateway Services Benefits

- Traditional AV & Advanced Malware Detection
- Inbound/Outbound Email Security
- AntiVirus, Static and Dynamic
- AntiMalware Stream Scanning
- Viruses, Worms, Trojan Horses
- Content Filtering Keyword
- Framework for Regular Expression
- URL Protection/DDOS Mitigation
- File Attachment Sandboxing*
- Email Attachment Protection
- Human Analysis, Quarantining
- Permitted Sender Policy
- Domain Whitelisting
- Reporting Monitoring
- Centralize Management/ ADT Alerts
- Artifact Confidentiality
- Encryption Options
- Email Continuity 7-Day Spooling
- Web Portal Outlook Access
- Management Centralization

MSecurity System Features

Threat Protection provides multi-layer security, email continuity, and data leakage prevention. The system uses behavioral, heuristic, and sandboxing technologies to protect against zero-hour, targeted attacks and ransomware.

Email Data Loss Prevention (DLP) prevents the loss of intellectual property, customer data and other sensitive information through pre-defined filters (e.g., credit card, HIPAA, and Social Security Numbers). DLP provides offering summary or digest emails to end users.

Web Filtering protects email usage from URL phishing with near real time updated URL feeds of confirmed phishing.URL Masking and IP provide our partners and clients with reliable detection of the most sophisticated attacks. MTA design provides for URL, Spoofing, and Impersonation protection.

MSecurity System™ Content Protection and Compliance Email File Archiving

MSecurity System enables companies to search, scan, and save time identifying unprotected PII. Features such as PII Management and File Archive with SharePoint Integration enable tracking, mapping, and data ingesting to secured archiving services with user-based archiving.

Compliance File Archiving Integration
- Active Directory Federation Services (ADFS)
- Search archives of emails & files on Desktop & SharePoint UI
- Compliant Search Analytics includes Network Scanning & Mapping of PII
- Search and share analytics by site's' & shared folders
- Secured Access Control

PII Management for CCPA & GDPR Compliance

The MessageSolution Advanced eDiscovery Platform includes comprehensive features such as universal legal hold, configurable 3rd party Legal/Auditor access, data redaction, performs Fuzzy, Wildcard, Proximity & AI searches for comprehensive data collection.
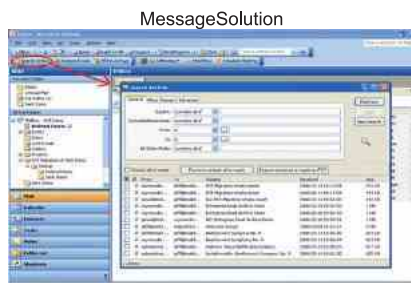
Support Public Cloud Networks

In addition to the MessageSolution Cloud Network, the solution also integrates with any private cloud networks and the following public clouds:

- Microsoft Azure
- IBM Cloud
- Google Cloud
- Amazon EC2

MessageSolution

Migrate to the Cloud

MessageSolution supports online and offline data import migration. Migrate historical data to the cloud-based archiving system from PST/NSF/GroupWise File, Public Folders, etc. MessageSolution also provides a stand-alone enterprise cross-platform email migration system to help organizations move from on-premise to hosted email services.

Global Online Implementation, Training & Support

New MessageSolution enterprise customer system deployment can be implemented for real-time, compliance archiving within half an hour.

All MessageSolution system implementations, training sessions and technical support sessions are done online via GoToMeeting or WebEx, making it more cost effective and always accessible.

Data Security in the Cloud

The greatest deterrent to cloud implementation is typically data security. Organizations worry about safety and accessibility of archived data.

To combat data security fears, MessageSolution offers SSL and AES encryption options. In addition, to maintain Soc II Type II certification, all MessageSolution data centers are bi-annually audited for physical and procedural safeguards.

The MessageSolution Platform also leverages multi-tiered access permissions to granularly manage internal data access permissions.

SOC 2 TYPE 2
AICPA SOC

Microsoft Azure • IBM Cloud • G Suite • amazon web services™