E. EMAIL
Censornet Email Security (EMS)

Protection from known, unknown and emerging email threats.

Email Security (EMS) from Censornet provides comprehensive protection from traditional email threats including spam, viruses, large-scale phishing attacks and malicious URLs.

EMS also includes a unique combination of advanced innovative technologies to address modern targeted and sophisticated email threats including impersonation attacks (business email compromise or CEO fraud) and unknown malware.

Traditional pattern, message attribute and characteristic matching are complemented with algorithmic analysis for ultimate threat detection without impacting accuracy.

Behavioural analysis alone includes over 10,000 algorithms analysing more than 130 variables extracted from each email message.

Multiple signature and behaviour-based antivirus engines offer protection from all forms of malware including zero day variants.

- 99.999% spam detec   tion with near zer o false positives
- 100% virus protection

At the core of EMS is a sophisticated policy engine that allows the IT administrator to customize exactly how email flows in and out of the organization. The engine can inspect all aspects of email, including size, content, attachments,headers, sender recipients and take appropriate action, such as deliver, quarantine, company quarantine, re-route, notify, reject.

EMS is both an advanced email security solution and a full cloud-based email routing engine with fully featured company and personal quarantines for message management. Deep categorization – distinguishing between professional marketing and suspect mass email campaign messages for example – enables flexible policies that deta precisely how different types of messages are processed and tagged.

EMS is fully managed by and delivered through the Censornet Platform that also includes Web Security, Cloud Application Security and Multi-Factor Authentication. The Censornet Platform provides a single web interface for central policy configuration and management, as well as data visualization and reporting.

EMAIL SECURITY

- 100% cloud based and easy to deploy with a simple MX record change

- Incorporates multiple technologies to ensure enterprise class threat detection ra tes with very high accuracy

- Full analysis of Inbound email with optional Outbound email analysis using unlimited keyword lists

- Multiple traditional signature and behaviour based AV engines including static sandboxing of file attachments

- Censornet LinkScan™ provides time of click protection from malicious URLs in emails with the option to scan links at time of delivery

For email administrators detailed message tracking is invaluable in being able to quickly view exactly why an email was delivered or rejected, including email headers and the full conversation with the remote email server.

ADD-ON SERVICES

Email Backup	Email Archiving	Email Continuity	Secure Email
Stores copies of messages for up to 7 years with full text search.	Provides a fully compliant archive with unlimited storage for an unlimited time.	Provides users with an 'Emergency Inbox' accessed via the browser if the primary email server fails.	Provides a simple solution to sending encrypted emails to specific recipients.

KEY FEATURES

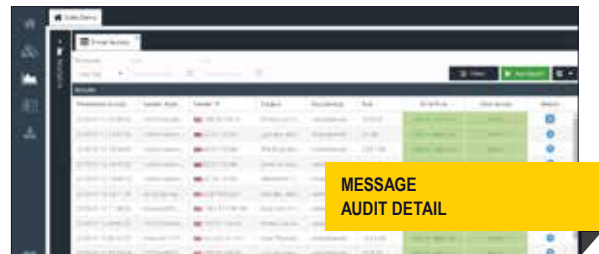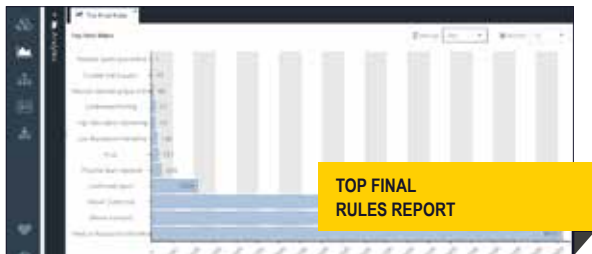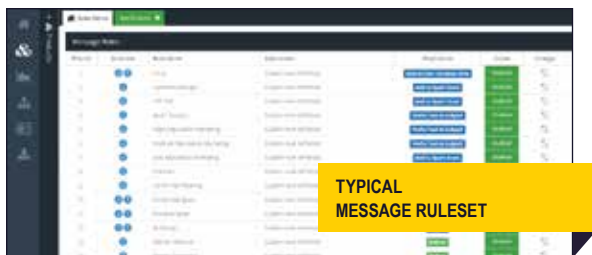|	
Anti-spam	• Multiple engines use a combination of technologies to detect spam as well as more sophisticated targeted phishing and impersonation attacks.
Anti-malware	• Multiple traditional signature and behavior based antivirus engines for detection of malware.
Censornet LinkScan™	• LinkScan rewrites URLs in email messages and provides point of click protection using multiple reputation services. • Options to autoredirect, click continue, block on threat and show/hide target URL. • Option to scan links at time of message delivery as well as at time of click.
Safe & Deny Lists	• Create company-wide and/or individual user Safe & Deny lists.
TLS / Opportunistic TLS	• Enforce TLS encryption and restrict communication with other email servers that do not support the TLS protocol. • Option to enable opportunistic TLS with fall back to plain text if TLS is not supported by the receiving mail server.
Email Authentication	• Support for SPF, DKIM and DMARC.
Executive Tracking List	• Use details synced from Active Directory to automatically detect users' real names within header and envelope address fields to protect against impersonation attacks / CEO fraud.
Nearby (cousin) Domains	• Compares sender domain to legitimate domain names to identify nearby domains (that vary from the actual domain name by one or two characters). • Protects against impersonation attacks / CEO fraud.
Subject Tags and Headers	• Add tags such as [EXTERNAL] or [MARKETING] to message subject lines. • Add HTML or plain text headers to inbound messages alerting users to potential risks.
File Attachments	• MIME type checking of file attachments with ability to block dangerous file types. • Detect password protected archives.
Keyword Lists	• Create unlimited keyword lists. Use rules to analyze messages and take action based on confidential or sensitive content.
Sending Limit Monitoring	• Automatic protection from attempts to send large volumes of messages outbound to prevent domain blacklisting.
Mail Queuing	• Email is automatically queued for 7 days in the event of a failure or outage of the primary email service/server(s).
Directory Harvest Attack (DHA) Prevention	• Drop email that is destined for invalid or fake email addresses.

MANAGEMENT

Policy Engine	• Over 20 conditional triggers to control email delivery and filter messages based on size, keywords, spam score, time, source, destination, attachment size, headers, AD attributes and more.
User Synchronization	• Active Directory synchronization service ensures changes are replicated. Apply rules based on AD group membership if required.
Web Interface	• Fully managed by and delivered through the Censornet Platform.
Delegated Administration	• Allows creation of multiple administrators with different levels of access to the Censornet Platform.
Quarantine	• Option to move messages to Company and User quarantines.

Quarantine Digest	• Digest emails list all messages within the user's quarantine and allow messages to be previewed, released or blocked. Interaction with the digest allows the user to manage their individual Safe & Deny lists. Users can set the frequency and days on which digest emails are received.
Disclaimers	• Append an HTML and/or plain text disclaimer to all outbound email. Set different disclaimers for different domains.

REPORTING

Real-time Visibility	• Charts provide detailed visibility of inbound and outbound mail flow as well as rules triggered, and actions taken. Ability to drill down from high level graphs and charts to detailed reports.
Report Builder	• Administrators can define their own reports based on available field names and criteria. Reports can be saved and then exported. Audit reports can be searched using criteria including time, user, sender address, subject, sender IP, recipient, direction, final action, rule name. Marking reports as 'Favourite' adds them to a quick access area.
Scheduling and Alerting	• Link reports to schedules and optionally only receive a report when there is content (alert mode). Alert on rules, actions, content etc.
Top Trend Reports	• A selection of pre-defined trend reports with chart and table data. Trend reports can be exported to PDF and e-mailed to recipients.
Multiple Views	• Analyze and report by time, user, sender address, subject, sender IP, recipient, direction, final action, rule name.
Detailed Audit (Message Tracking)	• Detailed view of analysis of individual messages with the exact reason an email was delivered or rejected. Includes email headers and full conversation with the remote email server.
Log Retention & Auto-archiving	• Email Security log data is archived automatically after 90 days and available to download from the Censornet Platform for a period of a further 12 months. Longer retention periods are available.

TYPICAL
MESSAGE RULESET

RULE
CREATION

TOP FINAL
RULES REPORT

MESSAGE
AUDIT DETAIL

DEPLOYMENT

Quick and Easy Deployment	• Redirect domain MX records to the Censornet EMS cloud.
Email Service Provider Support	• Works with all email service providers. Deliver email to different providers based on user AD Group membership – supporting hybrid environments using Exchange on premise with O365 Exchange Online or Gmail.