EMAIL SECURITY

CENSORNET EMAIL SECURITY IS A CLOUD-BASED EMAIL SECURITY AND BACKUP SERVICE THAT SCANS BOTH INBOUND AND OUTBOUND EMAIL FOR VIRUSES, PHISHING THREATS, CONTENT VIOLATIONS AND SPAM.

By doing this in the cloud it removes the processing and bandwidth burden on the local email server and also provides a layer of resilience in case of local mail server failures. It can, if required, backup unlimited email for up to seven years for complete peace of mind and can also provide an emergency inbox in the event of local mail server failure, which means employees are not left without email capability due to unexpected failure.

At the core of CensorNet Email Security is a sophisticated rules engine that allows the IT administrator to customize exactly how email flows in and out of the organization. The rules engine can inspect all aspects of email, including content, attachments, size, headers, recipients to name but a few and take appropriate action, such as quarantine, re-route, notify, reject and more.

KEY FEATURES

SECURITY

Incorporates multi-layers of security and provides inbound and outbound email protection across the whole organization by removing email-borne malware threats and spam before the email is delivered to your mail server – thus improving bandwidth and increasing mail server resources.

MANAGEMENT

Backs up email for regulatory compliance for up to seven years and enables email access even if the local mail server has failed.

REPORTING

Provides complete visibility on inbound and outbound messages for your domain(s). Audit allows for examination of the exact reason an email was delivered or rejected, including the conversation with the remote email server. Chart and table reports can be generated based on the rules triggered and actions taken for all inbound and outbound email.

DEPLOYMENT

Zero upfront investment in hardware or software required. Quick and easy deployment by redirecting domain MX records to CensorNet Email Security cloud.

CENSORNET

EMAIL SECURITY

KEY BENEFITS

INCREASE SECURITY

Prevents accidental access to malware by removing infected email messages and attachments before they reach your network. Blocks phishing emails that appear genuine and redirects to quarantine.

PREVENT DATA LOSS

Notifies instantly or blocks email messages that match content rules relating to confidential or sensitive information.

INCREASE UP-TIME

Ensures business continuity in the case of local email server failure by allowing employees to use the CensorNet Email Security portal to read, reply, and compose emails.

IMPROVE BANDWIDTH

Blocking spam in the cloud means only clean email messages are delivered to the local network, reducing the amount of bandwidth and resources required on mail servers.

RAPID RETURN ON INVESTMENT

Preventing malware outbreaks and reducing spam messages deliver an instant return on investment.

LOW TOTAL COST OF OWNERSHIP

A simple licensing model based on the number of mailboxes to manage, easy deployment, and no hardware or software licensing requirements.

REDUCE LEGAL RISK EXPOSURE

Use the SecureMail feature to send messages that are never stored on the recipient's computer and are accessed through an encrypted portal. Use the rules engine to block email containing sensitive content and optionally backup all inbound and outbound email for later review.

SECURITY

Real-time Anti-Malware Scanning	Incorporate multiple layers of security such as online threat detection, reputation and heuristics to block viruses in email attachments
Anti-spam Filtering	Real-time anti-spam and anti-phishing protection for inbound and outbound email removes spam, potentially harmful emails, time wasting messages and bogus messages.
Directory Harvest Attack Prevention	Drop email that is destined for invalid or fake email addresses before it reaches your mail server.
Outbound Protection	In the event of a spam outbreak on your network, CensorNet Email Security can protect outbound email volumes to help contain the problem.

CENSORNET

EMAIL SECURITY

Safe & Deny Lists	Create company-wide or personal (per user) Safe & Deny lists
Rules Engine	Over 20 conditional triggers to control email delivery. Messages can be filtered based on size, keywords, spam score, time, source, destination, attachments and more.
Dictionary Filtering	Create an unlimited number of "dictionaries" which may contain text strings such as email addresses or keywords. The dictionaries can then be used as part of the Rules engine to trigger various events.
TLS	Enforce TLS security for encrypted email transactions. Restrict communication with other email servers that do not honor TLS.
Queuing	As CensorNet Email Security is your primary and secondary MX in the event that your local email server fails, email will be queued for up to 7 days until your server is back online again. Once online, the mail will be delivered as normal.

MANAGEMENT

Web User Interface	Easy to use web-based portal provides a simple administration interface.
Delegated Administration	Create multiple administrators with different levels of access to the administration interface.
Quarantine Digest	The Digest email lists all messages in the users quarantine and allows the user to preview, release or block the messages, without needing to login to the portal. This reduces IT administration and allows the user to manage their personal Safe lists easily.
Active Directory/ Exchange Integration	Synchronize mailboxes from Exchange with the CensorNet Email Security portal. Synchronize Active Directory groups and apply rules based on group membership if required. Remote pull or remote push options available.
Disclaimers	Append an HTML and/or plain text disclaimer on all outbound email. Set different disclaimers for different domains.
Email Backup	Optionally backup all inbound and outbound email. The backup option includes unlimited storage and the backup can be stored from 3 days to 7 years.
Emergency Inbox	Optional web-based email client within the CensorNet Email Security portal that allows users to read, compose and reply to messages within the portal.

CENSORNET

REPORTING

Detailed Audit	Provide complete visibility on inbound and outbound messages for your domain(s). The email audit allows for examination of the exact reason an email was delivered or rejected, including the conversation with the remote email server.
Action & Rule Reports	Chart and table reports based on the rules triggered and actions taken for all inbound and outbound email.
Top Talkers Report	Understand which users are sending and receiving the most email.
Event Viewer	All actions and events are logged in the Event Viewer allowing the administrator to see exactly what user has performed a certain action within the portal.

DEPLOYMENT

Quick and Easy Deployment	Redirect domain MX records to CensorNet Email Security cloud. CensorNet Email Security will then forward clean messages to the local email server.

UNIFIED SECURITY SERVICE

A 360-degree view across web, email and cloud applications at a single glance.

CLOUD APPLICATION SECURITY

Secure adoption of cloud services and applications in your organization.

MULTI-FACTOR AUTHENTICATION

Keep your systems and data safe with multi-factor authentication.

WEB SECURITY

WEB SECURITY

CLOUD APPLICATION SECURITY

UNIFIED SECURITY SERVICE

EMAIL SECURITY

MULTI-FACTOR AUTHENTICATION

IDENTITY

WEB SECURITY

Provide a safe Internet experience for all the people within your organization.

EMAIL SECURITY

A cloud based solution to keep your organization safe from email threats.

IDENTITY

Single shared identity store fully AD integrated.

WANT TO LEARN MORE?

VISIT OUR WEBSITE