# ALSCO®

# EMAIL SECURE GATEWAY®:
## A CUTTING-EDGE AI-POWERED EMAIL SECURITY SOLUTION, BUILT ON 3 GROUNDBREAKING PATENTS BY ALSCO®

# INDRODUCTION:

Email remains the backbone of enterprise communication, facilitating collaboration, client interactions, and business transactions. However, it is also a primary target for cyber threats, including phishing, ransomware, credential theft, and brute-force attacks. These risks can lead to data breaches, financial losses, and operational disruptions, making robust email security essential for modern organizations.

**Email Secure Gateway®**, a flagship product by **ALSCO®**, addresses these challenges with advanced **Network Traffic Analysis (NTA)** and **AI-powered Self-Learning Technology**. It ensures real-time tracking of login attempts across **IMAP**, **POP3**, and **SMTP**, providing unmatched visibility into email activities. Integrated with **ALSCO® StorageBox**, it offers isolated, encrypted storage for attachments, safeguarding sensitive data from unauthorized access. Backed by three U.S. patents and officially registered as a trademark under **US Registration Number: 5992875, Email Secure Gateway®** delivers comprehensive protection, proactive threat detection, and compliance with global security standards. This document explores its key features, innovations, and benefits, showcasing its role as a cornerstone of enterprise email security.

# CORE EMAIL SECURITY CHALLENGES IN THE ENTERPRISE:

### Phishing Attacks and Credential Theft:
Cybercriminals use deceptive emails to steal sensitive information. Email Secure Gateway® detects and blocks phishing attempts, protecting employee credentials.

### Malware and Ransomware:
Emails often deliver malware or ransomware. Advanced scanning identifies and quarantines malicious attachments, preventing system compromise.

### Insider Threats and Unauthorized Access:
Unauthorized access can result in data leaks or intellectual property theft. Email Secure Gateway® provides detailed logs to detect and mitigate such threats.

### Lack of Visibility and Accountability:
Conventional systems often fail to track login attempts. Email Secure Gateway® offers comprehensive logging for proactive threat management.

### Email Spoofing and Impersonation Attacks:
Cybercriminals often forge sender addresses to impersonate trusted contacts or organizations, tricking users into revealing sensitive information or executing harmful actions. Email Secure Gateway® employs advanced sender authentication protocols (SPF, DKIM, and DMARC) to verify email origins, ensuring only legitimate messages reach user inboxes.

# COMPREHENSIVE SECURITY FEATURES:

**01**
### MULTI-LAYERED SECURITY WITH MX RECORDS
- **Eight MX Records:** Four IPv4 and four IPv6 addresses ensure maximum email deliverability and redundancy.
- **Distributed Infrastructure:** IP addresses are spread across multiple nodes to prevent service disruption during node failure.
- **Zero Downtime Assurance:** Even if one node fails, the remaining nodes ensure uninterrupted email service.

**02**
### QUEUE-BASED EMAIL DELIVERY ASSURANCE
- **Email Queuing:** In case of a server outage, all incoming emails are stored in a secure queue.
- **Encrypted Email Backup:** Emails remain encrypted in the queue until the hosting server is back online.
- **Zero Email Loss:** Guaranteed 100% delivery once the server is restored

**03**
### ADVANCED EMAIL ADMINISTRATION VIA SECURE PANEL
- **Secure Control Panel:** Email account creation, modification, and deletion are managed securely via a dedicated panel.
- **Two-Factor Authentication (2FA):** Adds an additional layer of access security.
- **IP Access Control:** Restricts control panel access to trusted IP addresses.

**04**
### SENDER AUTHENTICATION PROTOCOLS (SPF, DKIM, DMARC)
- **SPF (Sender Policy Framework):** Verifies sender IP addresses.
- **DKIM (DomainKeys Identified Mail):** Ensures message integrity and authenticity.
- **Enhanced Trustworthiness:** Guarantees emails are sent from legitimate sources.
- **DMARC (Domain-based Message Authentication, Reporting and Conformance):** Prevents email spoofing and phishing attempts.

**05**
### ENCRYPTED FILE ATTACHMENT PROTECTION
- **Isolated Encrypted Storage:** Attachments are scanned & stored securely in isolated environments.
- **Content Scanning:** Ensures all files are scanned before reaching user inboxes.
- **ZIP/RAR/PDF Threat Detection:** Prevents unauthorized or malicious encrypted files from being delivered.

## 06

### LOAD BALANCING FOR SERVER RESOURCE OPTIMIZATION

- **Automatic Load Balancing:** Incoming emails are distributed evenly across multiple nodes.
- **Resource Optimization:** Prevents server crashes caused by high CPU or RAM utilization.
- **Scalability:** Efficiently handles thousands of simultaneous email requests without latency.

## 07

### BANDWIDTH PROTECTION FROM EMAIL FLOODING ATTACKS

- **Spam & Flood Protection:** Prevents malicious spam floods designed to exhaust network bandwidth.
- **Proactive Filtering:** Filters out large volumes of malicious traffic before reaching the primary server.
- **Continuous Service Availability:** Ensures bandwidth is preserved for legitimate communications.

## 08

### COMPREHENSIVE EMAIL LOG MANAGEMENT

- **Detailed Email Logs:** Tracks all incoming & outgoing emails with timestamps and user information.
- **Failed Login Alerts:** Detects unauthorized login attempts and potential brute-force attacks.
- **Centralized Reporting:** Administrators can review logs for auditing and security purposes.

## 09

### REPUTATION-BASED IP MANAGEMENT

- **Global IP Reputation:** Emails are routed through globally recognized IP addresses.
- **IP Blacklist Prevention:** Ensures outgoing emails aren't blocked due to poor IP reputation.
- **Enhanced Deliverability:** Eliminates the risk of emails being marked as spam due to bad IP scores.

## 10

### MACRO-BASED MALWARE PROTECTION

- **MS Office Macro Security:** Blocks malicious macros in Word, PowerPoint, Excel, and Access files.
- **Automatic Scanning:** Detects and neutralizes macro-based threats in real-time.
- **Zero Day Protection:** Prevents execution of potentially dangerous macros embedded in attachments.

## 11

### ADVANCED EMAIL ARCHIVING

- **30-Day Archiving:** Deleted or lost emails can be retrieved within 30 days.
- **Advanced Search:** Search archived emails using sender, recipient, date, and subject filters.
- **Instant Recovery:** Emails are restored directly into inboxes with a single click.

## 12

### BRUTE-FORCE ATTACK PREVENTION

- **Login Attempt Monitoring:** Tracks repeated failed login attempts & blocks suspicious IP addresses.
- **Real-Time Alerts:** Administrators are notified of potential brute-force attacks.
- **IP Lockout:** Temporarily restricts access from offending IP addresses.

## 13

### DANGEROUS FILE-TYPE FILTERING

- **Malicious File Blocking:** Automatically blocks high-risk file types like .bat, .cmd, .dll, and .com.
- **Prevent Command Execution:** Eliminates risks from files that can execute harmful scripts.
- **Centralized Threat Reporting:** Administrators are alerted when such files are detected.

## 14

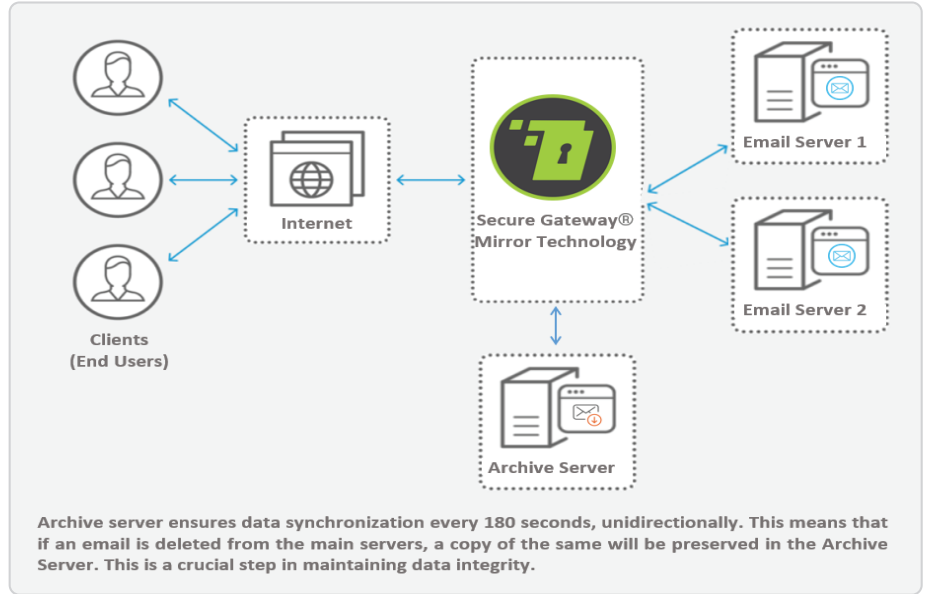### TWO-FACTOR AUTHENTICATION (2FA)

- **Enhanced Login Security:** Users must verify their identity with a code sent to their phone.
- **Time-Sensitive Codes:** Each code is valid for 120 seconds, adding an extra layer of security.
- **Phishing & Keylogger Protect:** Prevents unauthorized access even if credentials are compromised.

# ILLUSTRATIVE WORKFLOW DIAGRAMS:
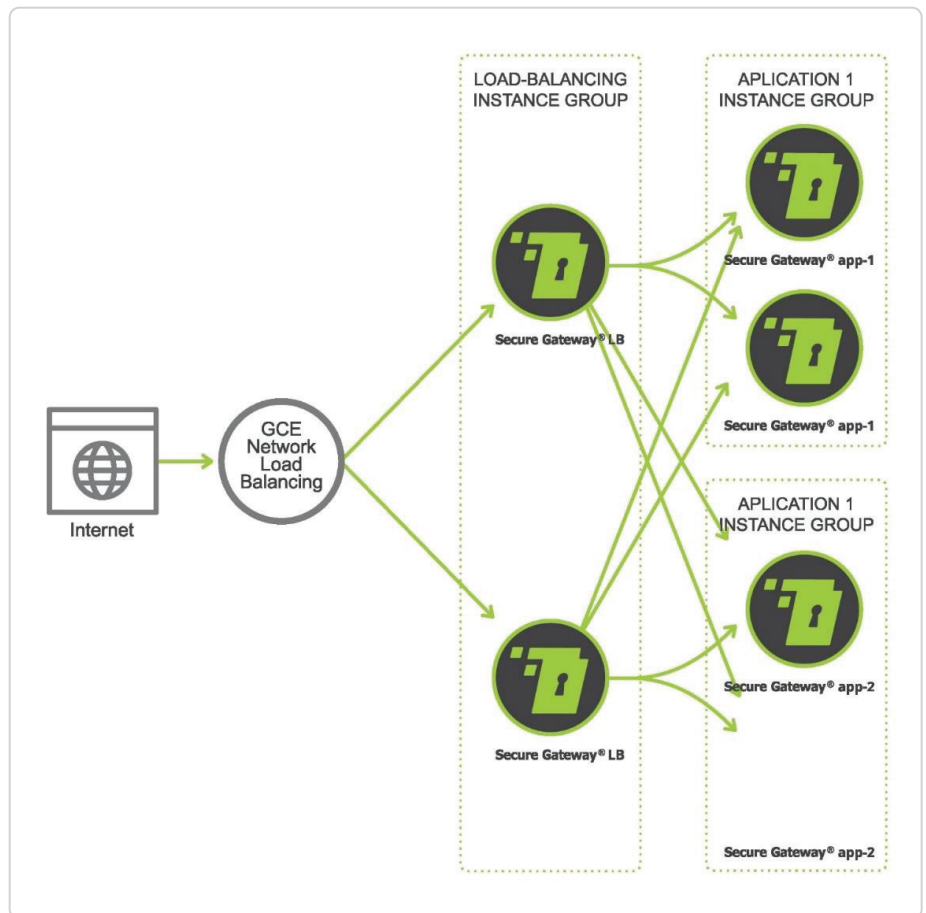
## 01

**Mirror Node Email Protection:**
Visual representation of how email traffic is filtered using a mirrored setup.



Archive server ensures data synchronization every 180 seconds, unidirectionally. This means that if an email is deleted from the main servers, a copy of the same will be preserved in the Archive Server. This is a crucial step in maintaining data integrity.

## 02

**Load Balancing Model:**
Demonstrates how email traffic is evenly distributed across multiple nodes.

## 03

**Centralized Log Monitoring:**
Shows real-time access tracking and security reporting.



## 04

**8 MX Records Infrastructure:**
Highlights redundancy and failover mechanisms in multi-node setups.



## 05

**Threat Prevention Workflow:**
Illustrates the steps of detecting and blocking spam, viruses, and malicious attachments before they reach the server.
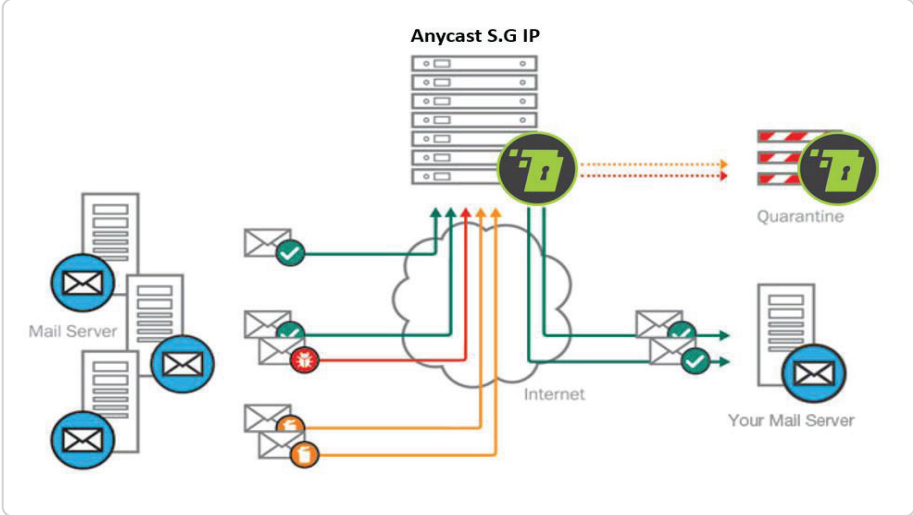
# TRADEMARK AND CERTIFICATION:

## E-Mail Secure Gateway® – A Mark of Trust and Innovation

At ALSCO®, we take immense pride in the E-Mail Secure Gateway®, a name officially recognized and protected by the United States Patent and Trademark Office (USPTO) under Registration No. 5,992,875. This certification serves as a testament to our unwavering commitment to innovation, security, and excellence in enterprise email protection.

## United States of America
### United States Patent and Trademark Office

### E-MAIL SECURE GATEWAY

**Reg. No. 5,992,875**

**Registered Feb. 18, 2020**

**Int. Cl.: 42**

**Service Mark**

**Supplemental Register**

ALSCO Software LLC (DELAWARE LIMITED LIABILITY COMPANY)
#300
3200 Greenfield Road
Dearborn, MICHIGAN 48120

CLASS 42: Internet security software services, namely, providing temporary use of non-downloadable computer virus protection software; computer services, namely, on-line scanning, detecting, quarantining and eliminating of malware; maintenance of computer software relating to computer security and prevention of computer risks

FIRST USE 11-7-2019; IN COMMERCE 11-7-2019

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT STYLE, SIZE OR COLOR

SER. NO. 88-437,538, FILED P.R. 05-20-2019; AM. S.R. 11-08-2019

Director of the United States
Patent and Trademark Office

# WHY THIS TRADEMARK MATTERS FOR YOU:

**Authenticity and Trust:** The trademark assures our clients of the authenticity and reliability of the E-Mail Secure Gateway® solution.

**Legal Protection:** It prevents unauthorized use, ensuring our clients benefit from a legally protected cybersecurity solution.

**Commitment to Excellence:** Backed by official certification, this mark underscores our dedication to leading the industry with patented, innovative technologies.

## CONCLUSION:

Email Secure Gateway® by ALSCO® is a comprehensive, AI-powered email security solution that safeguards enterprises against cyber threats while ensuring transparency, compliance, and reliability. Its integration with ALSCO® StorageBox provides secure storage for attachments, while advanced features such as two-factor authentication, threat detection, and detailed auditing ensure the highest level of email security for businesses across industries.