SecurityGateway

SecurityGateway – Security Feature Overview

Anti-Spam, Data Leak Pevention, Compliance & More

Anti-spam, security and compliance for Microsoft Exchange Server, Microsoft 365 and other email platforms

Enterprise-Grade Email Security — On Your Terms

SecurityGateway

Executive Summary

Email remains the primary communication tool for businesses—and the primary target for cyberattacks. Organizations relying on Microsoft Exchange Server or Microsoft 365 often face increasing concerns around security complexity, data privacy, cost, and control.

SecurityGateway is a powerful, secure, and cost-effective secure email gateway that protects users on Microsoft 365, Microsoft Exchange and other email platforms from email-borne threats, giving organizations full control over their email security while delivering enterprise-grade protection against modern threats.

This white paper explores the security challenges businesses face today and how SecurityGateway provides a comprehensive, layered defense strategy without sacrificing control or flexibility.

1. Introduction

The Growing Email Security Challenge

Cyber threats targeting email systems have grown in both volume and sophistication. Phishing, ransomware, and business email compromise (BEC) attacks are now common tactics used by attackers to infiltrate organizations.

At the same time, businesses are increasingly concerned about:

- **Security** – Protecting sensitive communications from advanced threats
- **Control** – Avoiding dependence on third-party cloud providers
- **Compliance** – Meeting regulatory requirements such as GDPR and HIPAA
- **Data Sovereignty** – Keeping data within geographic and organizational boundaries

For organizations using Microsoft Exchange Server or Microsoft 365, SecurityGateway addresses these concerns by sitting in front of the mail server as a dedicated secure email gateway—providing full visibility, advanced threat filtering, and direct administrative control over every security decision.

2. The Email Threat Landscape

Email continues to be the most exploited attack vector due to its accessibility and the human factor involved.

Common Threats

- **Phishing & Spear Phishing** – Deceptive emails designed to steal credentials or sensitive data
- **Business Email Compromise (BEC)** – Impersonation attacks targeting financial transactions
- **Ransomware & Malware** – Malicious attachments or links that infect systems
- **Spoofing & Impersonation** – Forged sender identities designed to bypass trust mechanisms

Traditional, single-layer defenses are no longer sufficient. Modern email security requires a multi-layered approach that detects, blocks, and adapts to evolving threats.

3. SecurityGateway's Layered Security Approach

SecurityGateway uses a defense-in-depth strategy that combines multiple security technologies to protect against email-borne threats at every stage of the mail flow.

Key principles include:

- Multiple layers of independent protection — each layer operates regardless of others
- Real-time threat detection and adaptive filtering
- Policy-driven controls configured by your administrators
- Complete audit-level visibility into every filtering and delivery decision

SecurityGateway gives organizations the freedom to deploy and operate their security infrastructure as they choose—whether on-premise or in a private cloud environment.

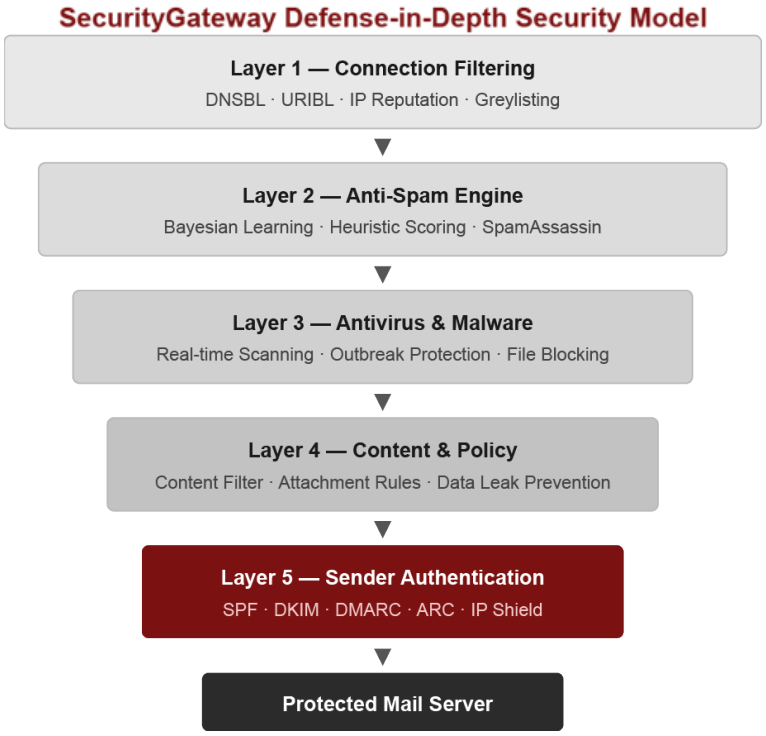


Figure 1 — SecurityGateway's five-layer defense-in-depth model, from connection filtering to authenticated delivery

4. Core Security Features

4.1 Advanced Spam & Phishing Protection

SecurityGateway includes powerful filtering technologies to stop unwanted and malicious email before it reaches your mail server. Multiple independent layers act as a pipeline, each removing a different category of threat:

- Bayesian and heuristic spam filtering — learns from your organization's mail patterns
- DNS Block Lists (DNSBL) and URI Block Lists (URIBL) — block known malicious senders and URLs
- Anti-phishing and anti-spoofing detection
- Custom filtering rules and policies
- Greylisting — temporarily defers connections from unknown senders; spambots that do not retry are discarded automatically

Working together, these stages dramatically reduce inbox threat rates while keeping false positives low so that legitimate mail flows uninterrupted.

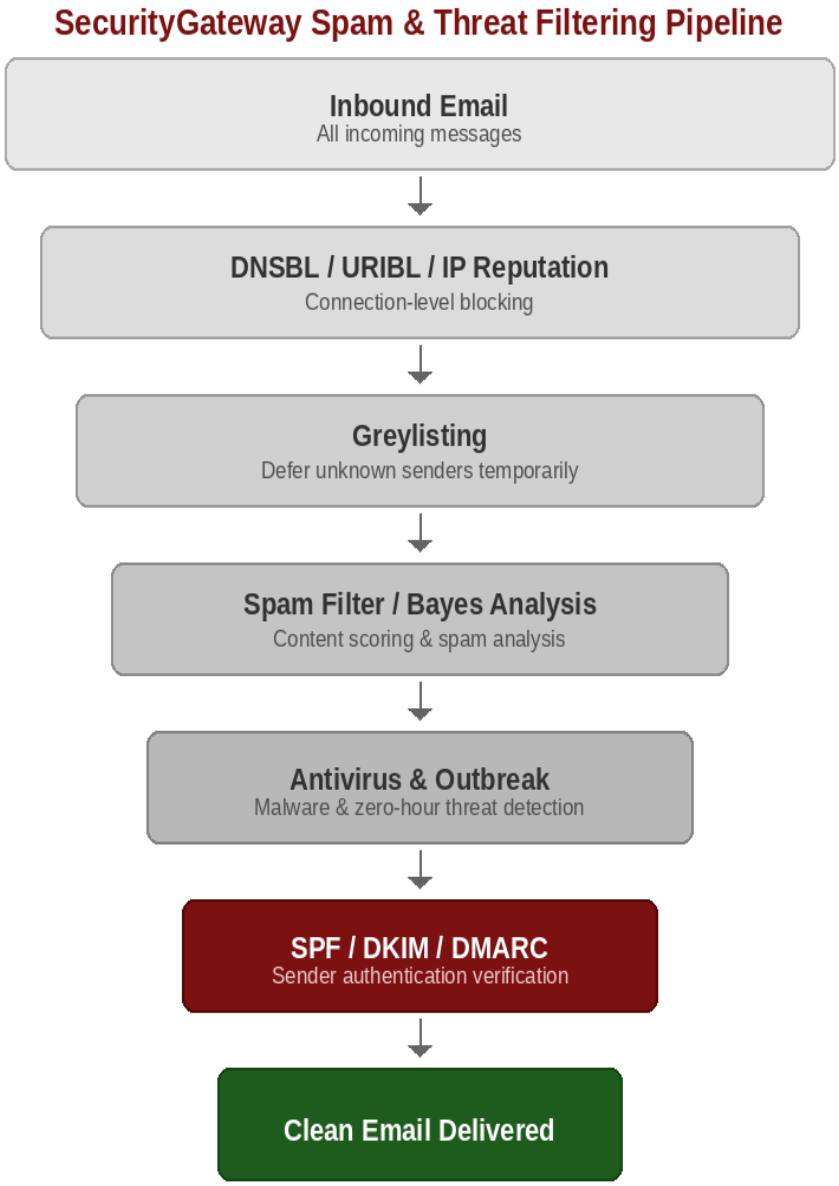


Figure 2 — Inbound email passes through six independent filtering stages before delivery

4.2 Antivirus & Malware Defense

SecurityGateway incorporates server-level antivirus and anti-malware scanning across all message traffic—both inbound and outbound—before messages are delivered.

- Real-time scanning of all email attachments
- Detection of known and emerging threats using multiple AV engines
- Blocking of suspicious or dangerous file types
- Detection & quarantine of potentially malicious QR codes
- Detection of potentially malicious macros in Microsoft Office documents
- Outbound scanning to prevent internal spread of malware

Outbreak Protection (Zero-Hour™ detection) — stops new threats before signature updates are available using pattern-based analysis

Threats are contained at the gateway before they can reach users or propagate to internal infrastructure.

4.3 Email Authentication & Integrity

SecurityGateway enforces all three major email authentication standards to validate sender identity and block spoofing attempts. Each plays a distinct role in SecurityGateway's anti-impersonation framework:

- **SPF (Sender Policy Framework)** — Confirms that the connecting server's IP address is listed among the domain's authorized sending hosts
- **DKIM (DomainKeys Identified Mail)** — Attaches a digital signature to outgoing messages so receiving servers can verify message integrity and the sending domain
- **DMARC (Domain-based Message Authentication, Reporting & Conformance)** — Ties SPF and DKIM outcomes together under a domain-wide enforcement policy and routes aggregate authentication reports back to domain owners

These mechanisms protect your domain reputation and ensure message authenticity. SecurityGateway also supports ARC (Authenticated Received Chain), which preserves authentication results for legitimately forwarded messages.

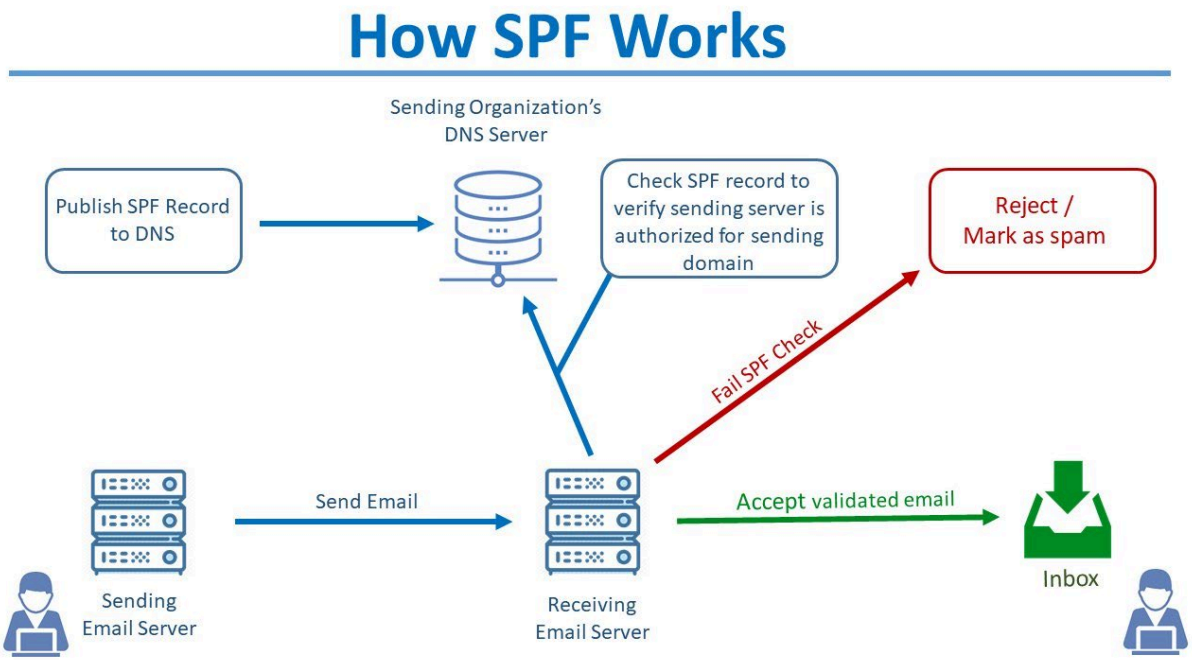


Figure 3a — How SPF works: the receiving server checks the sender's DNS record to confirm the sending IP is authorized for that domain

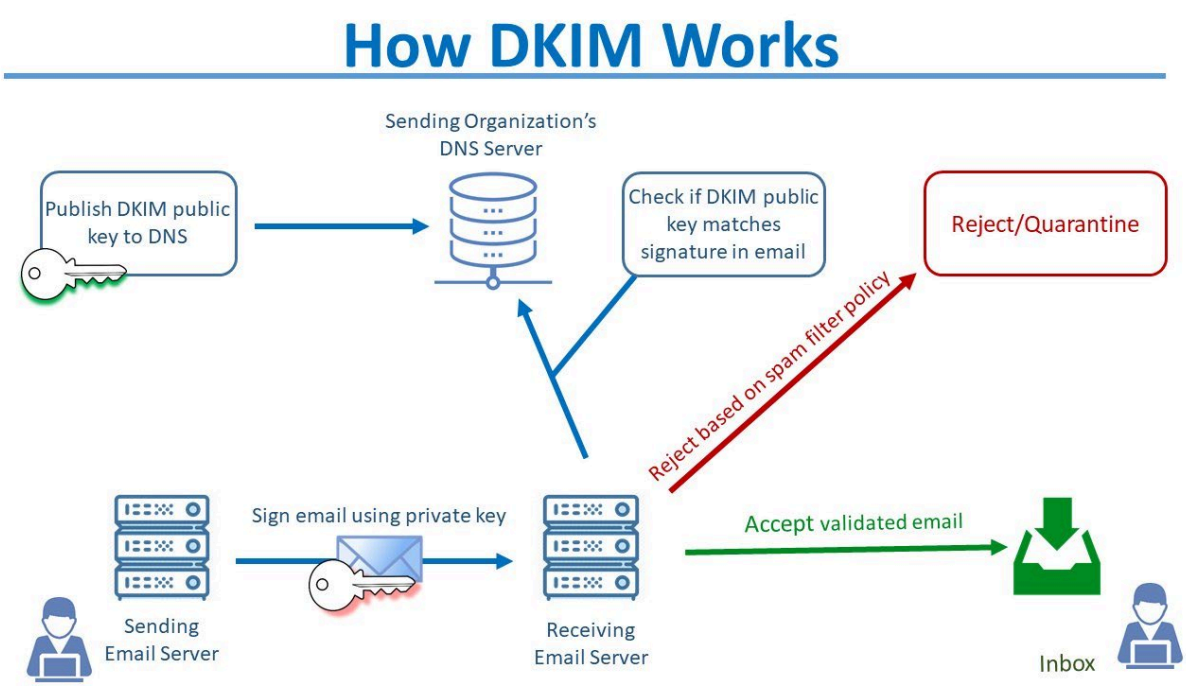


Figure 3b — How DKIM works: the sending server signs each email with a private key; the receiving server verifies it against the public key in DNS

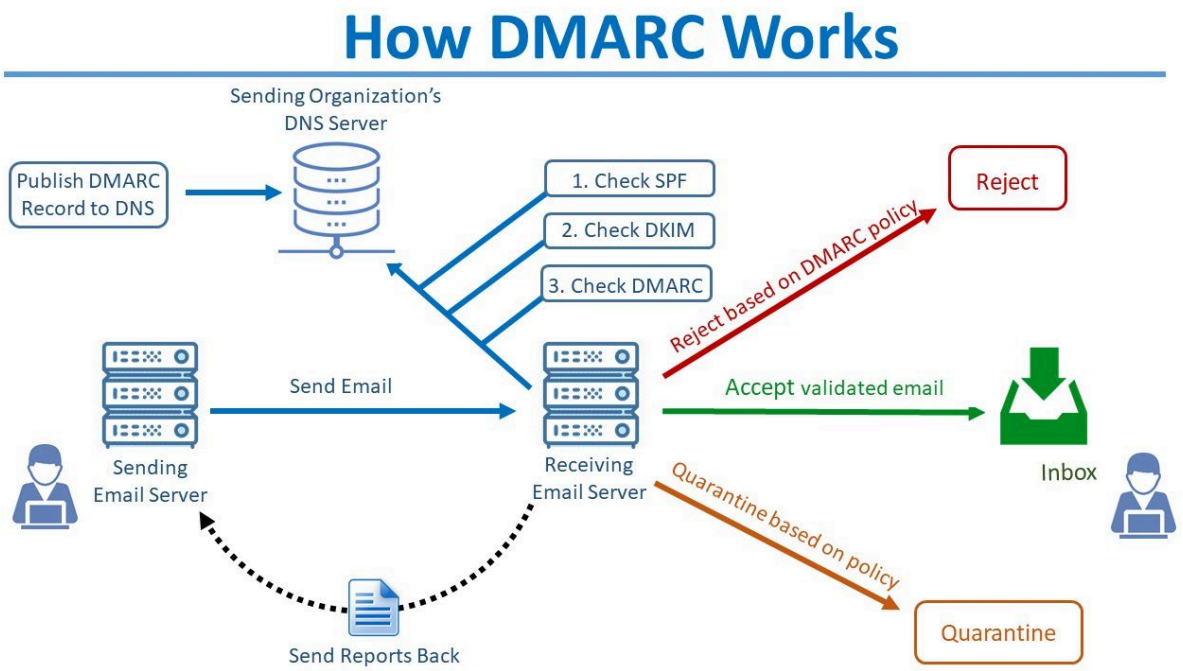
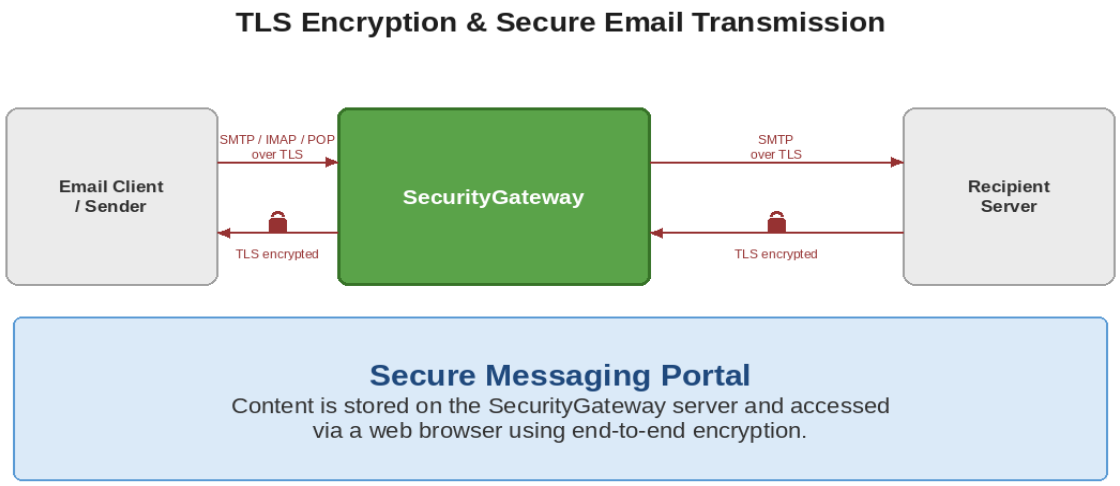


Figure 3c — How DMARC works: combines SPF and DKIM results to enforce a domain policy (none / quarantine / reject) and send aggregate reports back to the sending domain

4.4 Encryption & Secure Communication

Encrypting communications in transit is a basic requirement for any serious security policy. SecurityGateway delivers several encryption layers:

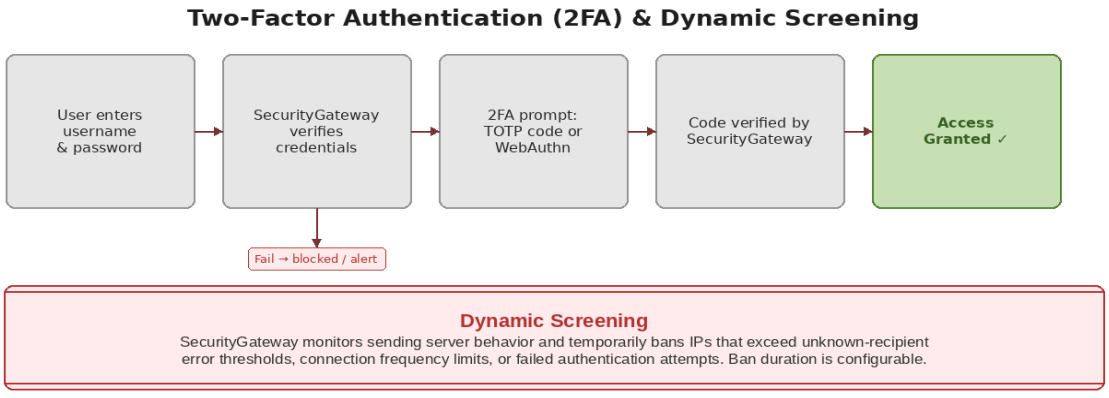
- **TLS (Transport Layer Security)** — Secures the SMTP session between the sending server and SecurityGateway, and between SecurityGateway and downstream mail servers
- **RequireTLS & MTA-STS** — Policy enforcement for secure server-to-server delivery paths
- **Secure Messaging Portal –** Messages are stored on the SecurityGateway server and accessed via a web browser using end-to-end encryption



4.5 Access Control & Account Security

SecurityGateway puts administrators in full command of access policies, with tools to lock down connections and reduce the risk of account compromise:

- IP allow/deny lists and connection filtering — associates domains with authorized IP addresses to prevent connection-level spoofing
- Account lockout policies — automatically lock accounts after repeated failed login attempts
- Authentication controls — enforce SMTP AUTH so only credentialed users can send mail
- Role-based administrative access — Domain-level or global delegation of admin permissions
- Dynamic Screening — Monitors sending server behavior to detect suspicious patterns—banning IPs that exceed connection frequency limits, trigger unknown-recipient errors, or fail authentication too many times; bans are temporary and configurable



SecurityGateway

5. Administrative Control & Visibility

SecurityGateway's administrative capabilities stand out as one of its strongest advantages. Administrators have access to:

- Centralized management console with a comprehensive administration interface
- Color-coded message logs and full SMTP transcripts that create a complete, searchable record of all mail activity
- Customizable security policies — rules, filters, and thresholds all under your control
- Alerts and reporting tools to surface threats and anomalies quickly

This depth of visibility enables IT teams to identify and act on threats quickly, and to maintain authoritative oversight over the entire email environment—a level of transparency that shared cloud platforms simply cannot match.

6. Compliance & Data Governance

SecurityGateway is built to support regulatory and internal compliance obligations without routing data through a third-party cloud provider:

- Integrated email archiving with data retention policies and legal hold
- Full support for GDPR, HIPAA, and other regulatory frameworks
- Policy enforcement and data leak prevention (DLP) — content filters can flag or quarantine sensitive content
- Audit-ready logging and reporting for compliance investigations

In contrast to cloud-based alternatives, SecurityGateway keeps organizations in direct control of where data lives and how it is retained—enabling full data residency compliance on their own infrastructure.

7. Data Sovereignty & Deployment Flexibility

Organizations with strict data privacy requirements benefit from SecurityGateway's range of deployment options:

- On-premise deployment — full control over physical hardware and data location
- Private cloud hosting — SecurityGateway Private Cloud delivers the full server experience managed by MDaemon Technologies experts
- MSP / multi-tenant deployments — flexible SaaS licensing for service providers
- Data stored within your own infrastructure or chosen geographic region — essential for regulated industries and government bodies

This flexibility is especially valuable in regulated sectors such as healthcare, legal services, financial services, and government, where data must remain within defined boundaries.

Positioned upstream of the mail server, SecurityGateway intercepts threats at the network edge—well before they can reach internal infrastructure.

SecurityGateway

Key Differentiators

- Gateway-level threat interception eliminates risk upstream, before messages ever reach user inboxes.
- Multi-stage filtering delivers sustained reductions in spam, phishing, and malware across all mail traffic.
- DLP policy enforcement prevents sensitive content from leaving the organization via email without authorization.
- Built-in archiving supports regulatory compliance obligations and provides a reliable recovery path after service disruptions.
- A unified management interface delivers full-spectrum visibility and control across all mail flow activity.

For more information visit **mdaemon.com**

MDaemon® technologies