Abnormal

The Essential Guide to Retiring the SEG

Legacy email gateways no longer fit the cloud and AI era

SEGs were built to block known threats at the perimeter. Modern attacks don't need malware, links, or spoofing to succeed.

SEG Blind Spots

Email remains the primary attack surface as today's attackers exploit trust, identity, and human behavior.

These threats are built to bypass the gateway.

Why Modern Attacks Get Through SEGs

No payloads	pass scanning
AI-written content	no linguistic anomalies
Legitimate sending infrastructure	pass authentication
Familiar communication patterns	no heuristic flags
Vendor impersonation	exploit trusted relationships

$2.8B

Lost to Business Email Compromise in 2024

Source: FBI IC3 Internet Crime Report 2024

68%

Of breaches stem from exploited human behavior

Source: Verizon DBIR 2025

$10.22M

Average cost of a breach in the U.S.

Source: IBM Cost of a Data Breach Report 2025

Static Filters vs. Modern Attacks

Traditional SEG Logic

- Relies on known-bad indicators
- Filters based on rules, signatures, and heuristics
- Focuses on payloads, spoofing, and obvious anomalies

Modern Attack Reality

- No payloads to scan
- AI-crafted content tailored to recipients
- Identity abuse and supply chain compromise
- Legitimate domains and accounts
- Behavioral manipulation instead of technical exploits
- Attack signals distributed across systems and channels

Static inspection can't keep up with dynamic threats exploiting human behavior.

Paying for Redundancy

Microsoft 365 and Google Workspace already stop commodity threats.

Third-party SEGs duplicate that coverage while adding cost, complexity, and operational drag.

Where SEG Costs Accumulate

- Licensing and maintenance fees
- SOC time spent triaging false positives
- Duplicate filtering efforts across SEG + native cloud tools
- Continuous rule tuning and policy updates
- Investigations of delayed or blocked legitimate mail
- Operational drag from maintaining parallel systems

A More Sustainable Model

Native cloud protection + behavioral detection

Baseline filtering stays native. Advanced threats are detected through identity and behavior, not content.

This model delivers stronger coverage with far less overhead.

Provides Baseline + Advanced Coverage

- Spam/malware (native)
- Behavioral + identity detection

Less Overhead

- No inline routing
- Minimal configuration
- Accelerated remediation

Life Beyond the SEG

Organizations that retire third-party SEGs see:

*Based on Abnormal customer data

95%

Reduction in SOC operational overhead*

42%

Reduction in email security licensing costs*

Built for Cloud Email. Designed for Human Risk.

Pairing native cloud protections with AI-native, behavior-based detection aligns email security with how today's attacks actually work.

Retiring the third-party SEG can help organizations simplify their security stack and reduce total cost of ownership.

Download The Essential Guide to Retiring the SEG for a complete migration blueprint.