

K-12 Email Security Vendor Scorecard

Compare evidence, operating fit, and complete annual cost

Score every vendor with the same scenarios. Use 0 for unavailable, 1 for claimed, 2 for demonstrated, 3 for pilot verified, and 4 for accepted with evidence.

Protection coverage

REQUIREMENT	WEIGHT	SCORE 0-4	EVIDENCE / NOTES
SPF, DKIM, DMARC, ARC, alignment, and forwarding context			
Display-name, protected-person, reply-domain, and lookalike impersonation			
Links, redirects, shortened URLs, newly observed domains, and QR codes			
Documents, archives, scripts, images, executables, and encrypted-content boundaries			
Inbound, internal, and outbound scope stated precisely			
False-positive controls with reason, owner, scope, and expiration			

Investigation and response

REQUIREMENT	WEIGHT	SCORE 0-4	EVIDENCE / NOTES
Human-readable verdict evidence			
Search by sender, recipient, subject, message ID, URL, file, and campaign			
Quarantine review and safe release			
Related-message discovery and provider-side action			
Role-based authorization and confirmation for consequential changes			
Durable activity, decision, and delivery receipts			

Implementation and service

REQUIREMENT	WEIGHT	SCORE 0–4	EVIDENCE / NOTES
Documented mail-flow design, pilot, acceptance tests, rollback, and cutover owner			
Monitoring, escalation, after-hours handling, and incident communication			
Training by role and usable support documentation			
Provider-action reconciliation, retry behavior, and failure visibility			
Export and exit plan for data, routing, integrations, and DNS			

Privacy and access

REQUIREMENT	WEIGHT	SCORE 0–4	EVIDENCE / NOTES
Data fields, location, encryption, retention, deletion, and subprocessors			
Tenant separation and support-access boundaries			
Identity lifecycle, SSO, administrator roles, and emergency access			
Audit export and customer-visible activity history			

Commercial terms

REQUIREMENT	WEIGHT	SCORE 0–4	EVIDENCE / NOTES
Staff, students, shared mailboxes, groups, aliases, and guests			
Message volume, storage, retention, API use, and response actions			
Implementation, migration, training, support, and premium modules			
Minimum, renewal, increases, discounts, termination, and growth			