seceon
SECURITY FOR EONS

Seceon aiSecurity Email360

AI-Driven Email Threat Protection

Secure Microsoft 365, Google Workspace, Zimbra, and SMTP with automated remediation and native Seceon APE correlation.

Product Overview

Seceon aiSecurity Email360 is an AI-powered email security platform that protects inbound and outbound mail against phishing, business email compromise (BEC), malware, data loss, and emerging content threats.

Mail is ingested via cloud API connectors (Microsoft Graph, Google Workspace), optional Zimbra paths, and/or an SMTP secure email gateway. Every message is analyzed through a staged orchestrator that combines authentication checks, URL reputation, attachment sandboxing, ML phishing/BEC models, NLP intent analysis, behavioral signals, DLP, and live threat-intelligence enrichment. A policy decision engine returns an allow / quarantine/block verdict, with optional automatic remediation back into the mailbox.

Security events stream into the Seceon APE collector plane so email threats correlate with endpoint, network, and identity signals across the Seceon OTM platform, ideal for enterprises and MSSPs that need one operational story, not another isolated inbox filter.



Highlights

- Multi-layered email threat protection for Microsoft 365, Google Workspace, Zimbra, and SMTP mail paths
- AI / ML detection for phishing, BEC / VIP fraud, malware, impersonation, and graymail
- Full analysis pipeline: authentication → URL → sandbox → NLP → DLP → threat intelligence → policy verdict
- Automated quarantine, trash, recall, and remediation with analyst workflows
- Native integration with Seceon APE / aiSIEM for correlation, MSSP multi-tenancy, and unified operations
- Outlook & Gmail Report Phish add-ins for user-driven feedback

Mail Path Coverage

Path	Capability
Microsoft 365	Graph sync, webhooks, mailbox remediation, pre-delivery / realtime protection
Google Workspace	Gmail sync and Pub/Sub ingestion
Zimbra	On-prem / hosted mailbox integration
SMTP Gateway (SEG)	Inbound MX / submission (ports 25 / 587) with verdict-before-delivery
API ingest	Programmatic submission for custom mail pipes
Third-party gateways	Proofpoint, Mimecast, INKY and PreVeil

Detection & Analysis Pipeline

Layer	What it does
Authentication	SPF, DKIM, DMARC, BIMI, MTA-STS (+ ARC merge)
URL Scanning	Batch URL reputation, redirects, and malicious-link scoring
Attachment Sandbox	Malware, macros, and suspicious payload analysis
Phishing ML	Heuristic + classifier models with explainable indicators
BEC / VIP Fraud	Wire-fraud, executive impersonation, and payment-diversion patterns plus vendor payment baselining, so altered invoices and wire diversions stand out
NLP Engine	Intent, entities, urgency, and social-engineering language
Behavioral Analysis	First-time senders, anomalies, and sender reputation signals
Supply-Chain Detection	Vendor / partner compromise patterns
DLP	Sensitive-data detection with direction-aware policy
Threat Intelligence	Domains, URLs, hashes, and IPs from master TI feeds + optional enrichers
Graymail	Newsletter / marketing classification and unsubscribe hygiene
Image / Media Analysis	QR codes inside images and PDFs are decoded and the hidden URLs inspected, logo impersonation, OCR; audio/video deepfake scoring
Advanced phishing	adversary-in-the-middle proxies, Turnstile cloaking, IDN homograph domains and prompt-injection content

Layer	What it does
Encryption / TLS Checks	Signature verification and TLS enforcement hooks
Decision Engine	Aggregates all scores into a clear verdict and action

Threat Intelligence

- 100+ commercial, open-source, government, ISAC, and dark-web sources, with signed nightly updates continuously synced into a master IOC store
- Hot Redis blocking sets for fast URL / domain / IP / hash matching at detection time
- Optional keyed enrichers (e.g. VirusTotal, AbuseIPDB, TAXII/STIX)
- Retention and feed controls to balance coverage vs. memory
- The same intelligence feeds aiSIEM correlation and aiXDR-PMax.

Response & Remediation

- Policy-driven allow / tag/quarantine / block actions
- Automated tenant-wide removal via Graph / Gmail APIs, with session revocation if a link was clicked
- Email recall and zero-hour style protection workflows
- Quarantine management with retention and cleanup jobs
- Analyst incident views, audit logging, and ML feedback loops
- End-user Report Phish from Outlook and Gmail add-ins

Security Operations & Platform

- Multi-tenant / MSSP-ready design with APE JWT auth and Postgres RLS
- Events published as formalized email_security records into Seceon APE
- Optional export to customer SIEMs (syslog, QRadar, Chronicle, Elasticsearch, Kafka)
- Notifications to Slack / Teams/email; ticketing hooks
- Remote Browser Isolation (RBI) proxy integrations for risky URL handling
- Unified experience through Seceon APE / SAPE console



Primary Use Cases

Use case	How aiSecurity Email360 helps
Stop credential-harvesting phishing	ML + URL + authentication + threat intelligence layers before and after delivery
Prevent BEC / invoice fraud	BEC models, NLP urgency/entity cues, and VIP patterns
Block malware & malicious attachments	Sandbox analysis with policy-based quarantine/block
Reduce graymail noise	Graymail detection and policy-based actions
Protect sensitive data in mail	DLP scanning with direction-aware enforcement
Pre-delivery defense on M365	Real-time / Graph pre-delivery protection path
Secure legacy or hybrid SMTP	SEG on ports 25/587 with verdict API
MSSP multi-customer email security	Tenant isolation + APE multi-tenant operations
Correlate email with broader attacks	APE / aiSIEM correlation across OTM products

Why Seceon aiSecurity Email360

Differentiator	Benefit
Depth, not a single filter	Full staged orchestrator from authentication through DLP and threat intelligence, rather than relying on a single ML score
Cloud API + SMTP in one product	Protect Microsoft 365, Google Workspace, and classic MX paths without needing two vendors
OTM Platform native	Email alerts join endpoint, network, and identity analytics in APE
MSSP-ready	Multi-tenant ACL, RLS, and APE-aligned operations
Actionable remediation	Quarantine, trash, recall, and policy automation, not alerts alone
User participation	Report-phish add-ins close the loop from inbox to SOC
Appliance-simple deploy	Docker/Ansible monolith package with a single setup.sh install
Proven accuracy	96% BEC detection with under 0.1% false positives

Deployment Snapshot

Item	Detail
Form factor	Single-node Linux appliance (Docker + Ansible)
Core stack	Kong · Monolith · Celery · SMTP gateway · Postgres · Redis · Kafka · SIEM processor
Install	./setup.sh -a with APE registration token
Auth	APE / SAPE JWT (no separate local login plane)
Network	HTTPS 443; SMTP 25 / 587 when SEG is used

Recommended host sizing (protected mailboxes)

Tier	Mailboxes	vCPU	RAM	Data disk
Medium	Up to 1,000	8	32 GB	500 GB
Large	Up to 5,000	16	64 GB	1 TB
X-Large	Up to 10,000	32	128 GB	2 TB

Ideal Buyers

- Mid-market and enterprise IT/security teams on Microsoft 365 or Google Workspace
- Organizations with SMTP / hybrid mail who need SEG + API defense together
- MSSPs delivering managed email security under Seceon OTM
- Customers who want email threats correlated with aiSIEM / aiXDR / identity in one platform

One-Line Pitch

Seceon aiEmail360 delivers AI-driven phishing, BEC, malware, and DLP protection across Microsoft 365, Google Workspace, and SMTP with automated remediation and native Seceon APE correlation for enterprise and MSSP operations.



Seceon aiSecurity Email360 continuously monitors email threats to detect phishing, BEC, malware, and data loss, prioritize risks, and automate remediation using AI/ML-driven analytics.

About Seceon

Seceon simplifies cybersecurity for MSPs, MSSPs, and IT teams by reducing risk and complexity. Our AI and ML-powered aiSIEM and aiXDR platform provides comprehensive threat detection and response. By integrating data from logs, identity management, networks, endpoints, clouds, and applications, we deliver real-time, accurate alerts and automated remediation. Trusted by over 850 partners, Seceon supports more than 9,800 clients with efficient, high-margin security services and continuous compliance.

Learn more about Seceon

Schedule a Demo www.seceon.com/contact-us/



© 2026 Seceon Inc. All rights reserved. aiSIEM and aiXDR are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.