seceon

DATA SHEET

Seceon® aiEmailSec™ empowers organizations to secure their email infrastructure with powerful, flexible, and a best-in-class solution. It defends against spear phishing, impersonation, business email compromise, and catches even the latest wave of deep sea phishing attacks that use clever tricks to hide from both trained users and conventional email filters.

aiEmailSec for Office 365 | Exchange | G Suite

Key Benefits:

- All incoming mail is automatically checked against over two dozen computer vision and text analysis models that "see" the message and therefore even very convincing forgeries get blocked.
- Malicious mail can be automatically quarantined, while questionable mail can be delivered with a clear, prominent warning that your users will understand.
- Protects against both spear phishing and brand forgery attacks.
- Deploys organization-wide in 1-2 hours.
- Works with any mail client, on any device.
- "Report Phish" link in the mail sends the mail to your SOC.
- Analytics dashboard gives IT/Security total visibility, supporting time-bounded queries.
- Includes state-of-the-art spam and anti-malware protection.
- HTML sanitization blocks XSS, JavaScript, CSS attacks
- Real-time analysis engine does not slow down mail delivery.

Email is a popular medium for the attackers to get into an enterprise network in order to breach valuable data. It is an entry vector within an organization to spread malware, phishing attacks by deceiving the recipients. Email security describes various techniques for keeping sensitive information in email secure against unauthorized access, loss, or compromise and is necessary for both individual and business email accounts. **Seceon® aiEmailSec** is a mail protection gateway that uses sophisticated AI, machine learning and computer vision algorithms to block deep sea phishing attacks and can automatically scan both internal and external email to identify & flag phishing emails. Moreover, aiEmailSec can either quarantine the mail or deliver it with disabled links and a user-friendly warning.

aiEmailSec has three levels of classification.

Clean/unusual/malicious model means that malicious emails can be quarantined while merely suspicious or unusual mails can be delivered with a user-friendly banner to each email explaining what, if anything, is wrong with the email.

aiEmailSec detects zero-day brand forgeries.

Uses computer vision algorithms to recognize brand-indicative imagery, HTML, text, colors, etc. It can spot logo-like text where there is only text and no image.

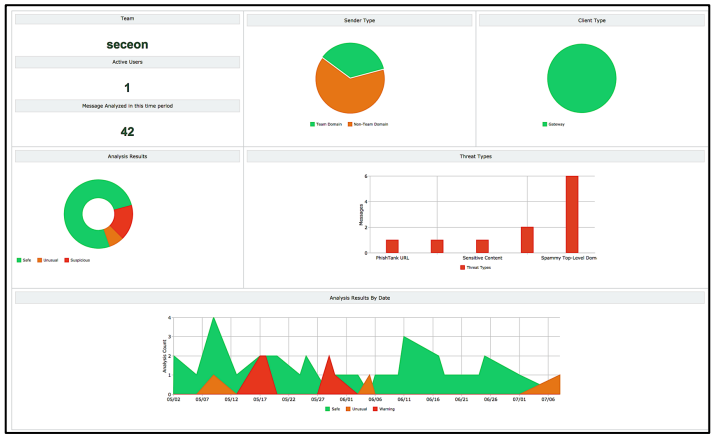
aiEmailSec catches zero day spear phishing attacks.

Social graph-based sender profiling and sender anomaly detection algorithms spot these "Business Email Compromise" (BEC) attacks. These emails often lack URLs or attachments, so they elude detection by most mail protection systems.

aiEmailSec is easy to deploy and fully scalable.

Some newer anti-phishing solutions rely on EWS or REST API access to the Exchange tenant. This method scales poorly, adds latency to mail delivery, creates security concerns (since the service requires admin access to the Exchange tenant), and doesn't integrate with Exchange Mail Flow Rules for quarantining malicious emails. In contrast, aiEmailSec deploys inline, integrated with Exchange, as part of the normal mail flow. This means it supports quick deployment, staged roll-out to users by groups, and the ability to quarantine, folder, or drop malicious email using standard Exchange controls.

The aiEmailSec Dashboard



The dashboard gives admins comprehensive statistics on recent attacks and prevention rates. For example:

- Which employees were most targeted with spear phishing over the last month?
- How many phishing attacks did we block this week?
- What are the top 50 domains responsible for brand forgery attempts targeting our users?

What Makes It Different?

FEATURE	DESCRIPTION
Internal & External email	The platform can be configured to scan both internal and external email.
Real Time Threat Detection	aiEmailSec supports policy-based URL rewriting to prevent users from clicking through malicious links. The malicious link check occurs both at message delivery time and in real-time when the user clicks through, meaning click-throughs are protected with up to-the-minute threat information.
Deep Link Inspection	Alongside looking up URLs in known threat feeds, aiEmailSec performs deep link inspection. This means it simulates a click through to the linked site and examines the destination page for evidence of phishing and other security risks.
No Installation Required	aiEmailSec requires no installed software; works with any mail client: web, mobile, or desktop.
Report Phishing Attempts	aiEmailSec can add a “Report this Email” link to every email, allowing end users to report spam, phish, and other problematic email from any endpoint device, with no special software (i.e., from any mail client).
HTML Sanitization	aiEmailSec parses and sanitizes all HTML email to remove cross-site scripting (XSS) attacks. By default, it upgrades plain text emails to HTML emails, to support link rewriting in plain text emails.
Advanced Reporting	The Admin reporting dashboard shows which threats have been identified and blocked. Admins can run time-bounded queries to view what threats have been encountered and blocked, and can drill down into individual messages.

For more information and pricing, please contact Seceon at sales@seceon.com

Seceon’s Dynamic Threat Model, Machine Learning, AI with actionable intelligence for proactive threat detection of known and unknown threats, and real-time containment and elimination empowers all-size Enterprises and MSSPs to provide comprehensive cybersecurity in the digital-era. Leveraging intelligent data collection and analysis, Seceon’s Open Threat Management (OTM) Platform provides unmatched visibility across the entire network – from users and devices to applications and flows – detecting and surfacing the most relevant threats in real-time and the means necessary to eliminate them immediately. Seceon offers different solutions – aiSIEM, aiMSSP, aiNBAD, aiEmailSec - built on a Big/Fast Data Architecture.

To learn more about Seceon and its solutions, please visit www.seceon.com or call (978) 923-0040.