EMAIL SECURITY

Schützt Kommunikation und Produktivität.

Vollständig gemanagt. Anpassungsfähig. Intelligenter Schutz.

E-Mail bleibt der wichtigste Angriffsvektor – heute zusätzlich verstärkt durch KI, Identitätsmissbrauch und Business E-Mail Compromise (BEC). Klassische Filter kommen mit modernen Bedrohungen wie Phishing oder Thread Hijacking nicht mehr mit. Unternehmen benötigen mehr als nur die Grundlagen: Sie brauchen eine vollständig gemanagte, lernfähige E-Mail-Sicherheitslösung.

Email Security von Open Systems kombiniert leistungsstarke Secure Email Gateway Funktionaltiät mit adaptiver, KI-gestützter Erkennung. Ob grundlegende Abesenderauthentifizierung und Verschlüsselung oder verhaltensbasierte Bedrohungsanalyse: Unser mehrschichtiger Service schützt jede E-Mail Konversation und reduziert gleichzeitig die Komplexität für IT- und Compliance-Teams.

Was unsere Lösung ausmacht

MEHRSCHICHTIGER BEDROHUNGSSCHUTZ

Kombiniert SEG-Kontrolle mit ICES-ähnlicher Erkennung – blockiert Malware, Phishing, BEC und neuartige Bedrohungen, bevor sie im Posteingang landen.

INTEGRIERTE, FLEXIBLE KONTROLLE

Granulare Absenderprüfung, richtlinienbasierte Verschlüsselung und Self-Service-Transparenz – nahtlos eingebettet in Ihre bestehende IT- und SASE-Infrastruktur.

LERNFÄHIG UND KONTINUIERLICH OPTIMIERT

Eingebaute Prävention und fortlaufende Modellanpassung bilden ein adaptives Sicherheitsnetz, das mit neuen Bedrohungen wächst – weniger Fehlalarmen und höhere Resilienz.

Drei Service Levels

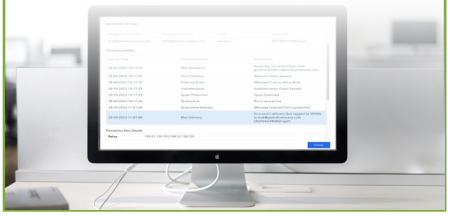
KUNDENPORTAL

Echtzeit-Einblick und Kontrolle

Anwendung: Sicherheitsteams benötigen Echtzeitzugriff auf E-Mail-Flows und Bedrohungen.

Vorteile: Rollenbasierter Zugriff und detaillierte Analysen ermöglichen schnelle, sichere Entscheidungen.

Was Open Systems auszeichnet: Intuitive Self-Service-Funktionen reduzieren die Support-Abhängigkeit – Governance und Audit-Fähigkeit bleiben erhalten.



EXPERTEN-SUPPORT

Umsetzung und Optimierung

Anwendung: Neue SPF/DKIM Absender Konfigurieren, Partner-Verschlüsselung oder die Behebung von Fehlklassifizierungen.

Vorteile: Rund-um-die-Uhr-Expertensupport sorgt für schnelle, präzise Fehler-Erkennung und Behebung.

Was Open Systems auszeichnet: Eskalationen und Anpassungen werden direkt durch E-Mail-Sicherheitsexperten betreut – für weniger Fehlalarme und stabile Policies.

DEDIZIERTES ACCOUNT MANAGEMENT

Strategie & Individualisierung

Anwendung: Individuelles E-Mail Routing oder ein DMARC-Rollout und –Update in Phasen.

Vorteile: Massgeschneiderte Richtlinien und sichere Umsetzung geschäftskritischer Anforderungen.

Was Open Systems auszeichnet: Technical Account Managers bieten persönliche, proaktive Beratung, insbesondere für den Schutz von C-Level E-Mail Postfächern und die Verteidigung der Domain-Reputation.

Servicevorteile

UMFASSENDER BEDROHUNGSSCHUTZ

Phishing, Malware, Spam und Zero-Day-Angriffe werden durch KI-basierte Echtzeiterkennung und bewährte SEG-Abwehrmechanismen zuverlässig gestoppt.

NAHTLOSE COMPLIANCE IM BETRIEB

Verschlüsselung, Richtliniendurchsetzung und Logging sind als integraler Bestandteil alltäglicher Workflows integriert – ideal zur Erfüllung von Standards wie DORA, NIS2 und DSGVO.

EXPERTENUNTER-STÜTZUNG INKLUSIVE

Ob SPF-/DKIM-Einrichtung bis zur BEC-Abwehr: Unser Expertenteam übernimmt Planung, Optimierung und Eskalation für sichere, skalierbare Leistung.

Service-Bestandteile

STANDARD EMAIL SECURITY

Absenderverifizierung: SPF, DKIM und DMARC schützen vor Spoofing und Domainmissbrauch

Inhaltsanalyse: Signatur- und heuristikbasierte Filter kombiniert mit Bedrohungsdaten und Phishing-Erkennung

Richtliniendurchsetzung: Anpassbare Regeln für Routing, Tagging, Verschlüsselung und Quarantäne

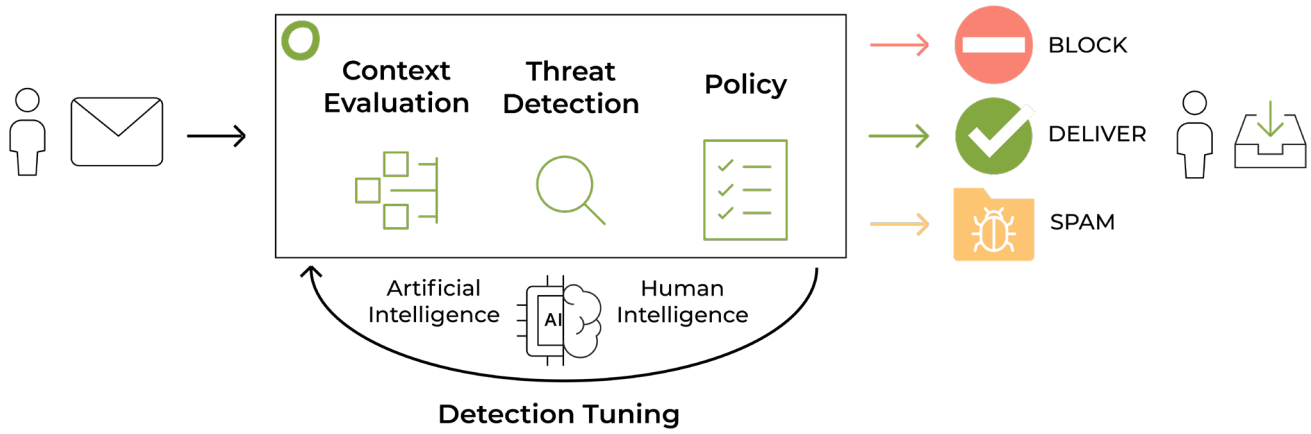
ADVANCED EMAIL SECURITY

Kontextanalyse: Analyisiert Absender-Verhalten und Verlauf und Tonalität zur Erkennung von Anomalien

Bedrohungserkennung: Stoppt Zero-Hour-Phishing, KI-generierte Inhalte, QR-basierte Malware und Identitätsmissbrauch

Modellanpassung: Analysen fliessen in Echtzeit in das Lernsystem ein und verbessern die Erkennungsgenauigkeit fortlaufend

So funktioniert es



Kontextanalyse & Richtlinien

SPF, DKIM und DMARC schützen Markenreputation und blockieren gefälschte Absender. TLS-Verschlüsselung sichert die regelkonforme Übertragung. Administratoren verwalten Block-/Allow-Listen und Richtlinien sowohl auf Verbindungs- als auch auf Inhaltsebene.

Mehrschichtige Filterung & Bedrohungserkennung

E-Mails werden mit mehreren Technologien analysiert: signaturbasierte AV-Systeme, verhaltensbasierte Spamfilter, URL-Scans und Advanced Threat Protection. KI-basierte Kontextanalyse erkennt gezielte Angriffe wie Deepfake-Nachrichten oder Thread Hijacking noch vor der Zustellung.

Adaptive Modelloptimierung

Erkennungsregeln werden kontinuierlich anhand realer Vorfälle verbessert. Support-Analysen fliessen direkt in den Lernprozess ein. Spezielle Konfigurationen – etwa für Führungskräfte oder DMARC-Einführung – werden durch dedizierte TAMs begleitet.

Opensystems

Open Systems bietet Managed SASE-Lösungen, die Netzwerk- und Sicherheitsfunktionen in einer cloudbasierten Plattform vereinen und hybride IT-Umgebungen sicher vernetzen – für mehr Effizienz, Sicherheit und maximale Skalierbarkeit.