xorlab | AVANTEC Competence. Security. Trust.

Maximale E-Mail Security für sicheres Arbeiten

Die xorlab Security Platform schützt Ihre Mitarbeitenden vor sämtlichen bekannten und unbekannten E-Mail-Angriffen und sorgt mit KI-gestützter Klassifizierung für eine effiziente Kontrolle der Angriffsfläche.

Die Anzahl der deutschen Unternehmen, die Schäden durch Phishing verzeichnen, hat sich von 18% im Jahr 2021 auf 31% im Jahr 2023 fast verdoppelt[1]. Neue und innovative Angriffstaktiken verändern die Bedrohungslage ständig. Aktuelle, bei Kunden erhobene Daten zeigen: **bei 4 von 5 Phishing-E-Mails handelt es sich um sogenannte Zero-Hour-Angriffe[2]**, deren "Indicators of Attack" bis dahin unbekannt sind. E-Mail bleibt für Angreifer die effektivste Methode für den initialen Angriff und gleichzeitig verlieren herkömmliche Sicherheitsmassnahmen zunehmend an Wirksamkeit.

"Heutige E-Mail-Angriffe sind auf den Kontext des Opfers zugeschnitten: Angreifer antworten auf tatsächlich geschriebene E-Mails oder geben sich als vertrauenswürdige Absender aus. Die "Indicators of Attack" sind oft unbekannt. Das erschwert die Erkennung der Angriffe. Wir haben xorlab entwickelt, um genau das zu ändern."
– Antonio Barresi, CEO und Mitgründer von xorlab

Context Matters – die Lösung von xorlab

Die xorlab Security Platform bietet maximale Sicherheit für M365 und On-Premise-Umgebungen:

- **Proaktive Abwehr** auch unbekannter Angriffe dank **KI-gestützter Klassifizierung**.
- Erkennung von Angriffen, die von **kompromittierten Partner-Accounts ausgehen.**
- Müheloses Minimieren der Angriffsfläche E-Mail mit **Policies**, die sich **Ihrem Kontext anpassen.**
- Situative, auf den Kontext zugeschnittene **Benutzerwarnungen.**
- **Automatisierungen in der Analyse** von intern gemeldeten E-Mails und fallbezogene Feedbacks.

4x mehr Bedrohungen blockiert
im Vergleich zu gängigen professionell betriebenen Umgebungen[2]

1.500 Stunden Zeitersparnis
bei der Bearbeitung gemeldeter E-Mails durch das Sicherheitsteam[2]

Hunderte von Signalen pro E-Mail
werden mit den erwarteten Kommunikationsmustern abgeglichen, um Bedrohungen zu erkennen

"xorlab ist eine der wenigen Lösungen, die nicht nur mehr Sicherheit bietet sondern gleichzeitig Kosten spart."

Michael Meli, Chief Information Security Officer,
Bank Julius Bär

xorlab auf einen Blick

Maximale Sicherheit
xorlab analysiert jede E-Mail im Kontext der Organisation und ermöglicht so eine präzise Klassifizierung aller Nachrichten.

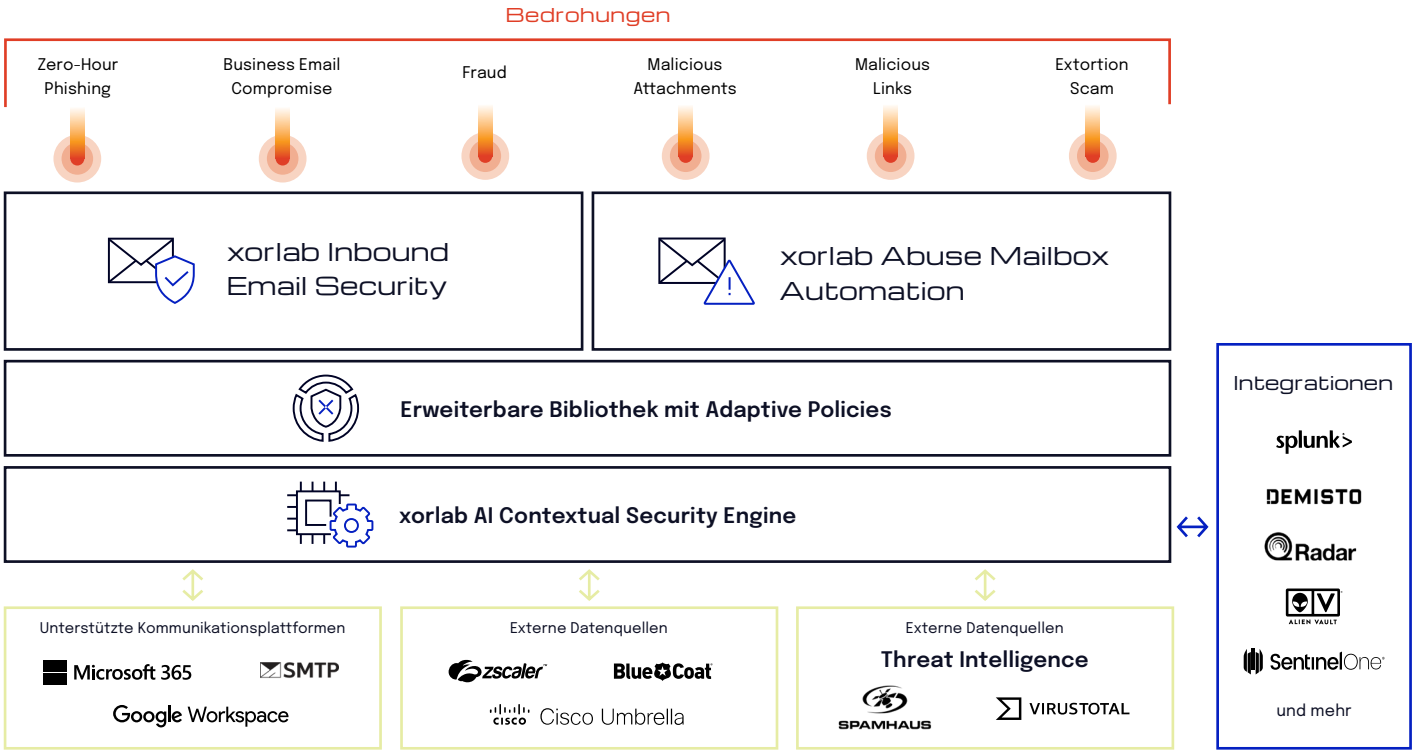
Tiefere Kosten
Die Analyse und Bearbeitung der von den Benutzern gemeldeten E-Mails wird automatisiert und die manuelle Pflege von Block- und Allow-Lists entfällt.

Mehr Kontrolle
Die Entscheidungen von xorlab sind nachvollziehbar und mit den Einblicken in die Kommunikationsmuster lassen sich die Adaptive Policies einfach an die eigenen Bedürfnisse anpassen.

1 Bitkom Research 2023. Report "Wirtschaftsschutz 2023". 1. September 2023.
2 Basierend auf xorlab-Daten für Kunden mit Ø 5.000 E-Mail-Postfächern.

xorlab | AVANTEC Competence. Security. Trust.

Die xorlab Security Platform wurde speziell dafür entwickelt, Zero-Hour Angriffe zu erkennen und abzuwehren. Kombiniert mit Microsoft 365 oder integriert in On-Premise-Umgebungen bietet xorlab maximalen Schutz vor Phishing, Business Email Compromise und Ransomware bei einer sehr niedrigen False Positive Rate.



Die xorlab Security Platform besteht aus:

xorlab AI Contextual Security Engine:
Klassifiziert E-Mails und identifiziert potentielle Bedrohungen frühzeitig, indem Hunderte von Signalen in jeder E-Mail analysiert und mit bekannten Mustern der regulären Kommunikation verglichen werden.

Erweiterbare Bibliothek mit Adaptive Policies:
xorlab liefert eine Vielzahl an Adaptive Policies. Sie können diese an die Bedürfnisse Ihrer Organisation anpassen sowie eigene Policies hinzufügen. Die Policies entwickeln sich mit dem Kontext Ihrer Organisation weiter und reduzieren so den Aufwand für die Pflege der Block- und Allow-Lists.

xorlab Inbound Email Security:
Filtert eingehende E-Mails und stoppt Zero-Hour Phishing, Business Email Compromise und Ransomware. Teil dieses Moduls ist ein Portal, in dem die Mitarbeiter ihre Quarantäne selbst verwalten und verdächtige Nachrichten in einer sicheren Vorschau beurteilen können.

xorlab Abuse Mailbox Automation:
Sammelt interne Verdachtsmeldungen und untersucht diese auf mögliche Angriffe. xorlab priorisiert die Meldungen anhand des Risikos und beantwortet jede Meldung mit einem fallspezifischen Feedback. Dadurch spart das IT Helpdesk oder Sicherheitsteam Zeit bei der Bearbeitung dieser Meldungen. Die Sicherheit wird verbessert und die Kosten werden gesenkt.

Ihr Partner AVANTEC AG:

Heinrichstrasse 267
8005 Zürich, Schweiz
044 457 13 13
info@avantec.ch
www.avantec.ch

Diese Unternehmen vertrauen auf xorlab:

CERN, coop, HAUFE.Group, Implenia, Julius Bär, KIRCHHOFF AUTOMOTIVE, DIE POST, swisscom, USZ Universitäts Spital Zürich

xorlab AG, Binzmühlestrasse 170D, 8050 Zürich, Schweiz.

Februar 2024 | xorlab.com