xorlab

AI-powered Email Security for on-premise and M365

The xorlab Security Platform minimizes the attack surface on email with an AI-powered engine and protects your employees from the full spectrum of email threats.

The number of German organizations reporting damages from phishing nearly doubled, rising from 18% in 2021 to 31% in 2023[1]. Threats constantly change as attackers find new ways to spread ransomware, steal login credentials, and carry out fraudulent activities. According to data from our customers, **4 out of 5 phishing threats are zero-hour attacks:** their indicators of attack have never been seen before. For criminals and state actors, email remains the most effective initial attack vector and, at the same time, traditional email security is becoming less and less effective.

"Today's email attacks are personalized to your context: attackers hijack existing threads or impersonate trusted senders. On top, the indicators of attack are not yet known. This makes attacks hard to detect and easy to click on. We've built xorlab to change that."
– Antonio Barresi, CEO and co-founder of xorlab

xorlab's solution

Combine xorlab with M365 or on-premise environments to maximize email security. The xorlab Security Platform enables you to:

Stop advanced attacks proactively with AI-based classifiers and policies.

Detect attacks from **compromised partners.**

Minimize email attack surface effortlessly with **policies that adapt** to your context.

Warn users with **contextual banners.**

Automate analysis and **triage of user-reported email** and send feedback.

1 Bitkom Research 2023. Report "Wirtschaftsschutz 2023". 1. September 2023.

12x more threats detected compared to alternative solutions run in professionally managed environments

90% less effort when analyzing and triaging user-reported suspicious emails

3x fewer false positives than alternative solutions

"xorlab is one of the rare cybersecurity solutions that enhance security and optimize cost. Plus: it lets our employees contribute to our defense at no extra cost by automating abuse reports."

Michael Meli, Chief Information Security Officer,
Bank Julius Bär

xorlab at a glance

Maximize email security.
xorlab analyzes every email in the context of your organization and thus enables precise classification of all messages.

Optimize email security spend.
Automate the analysis and response to user-reported emails and get rid of block and allow lists.

Stay in control.
Trace security decisions back to indicators of attack, gain full visibility into communication patterns, and tune the xorlab platform to meet the unique needs of your organization.

xorlab AG · CYBERSECURITY MADE IN EUROPE · Allianz für Cyber-Sicherheit · swiss made software · CERTIFIED ISO/IEC 27001 · GDPR · xorlab.com

xorlab

The xorlab Security Platform is designed to detect and stop zero-hour email threats. Combine xorlab with Microsoft 365 or on-premise environments to protect email mailboxes from advanced phishing, business email compromise and ransomware threats. By uniquely understanding your communication context, xorlab achieves a very low false positive rate.
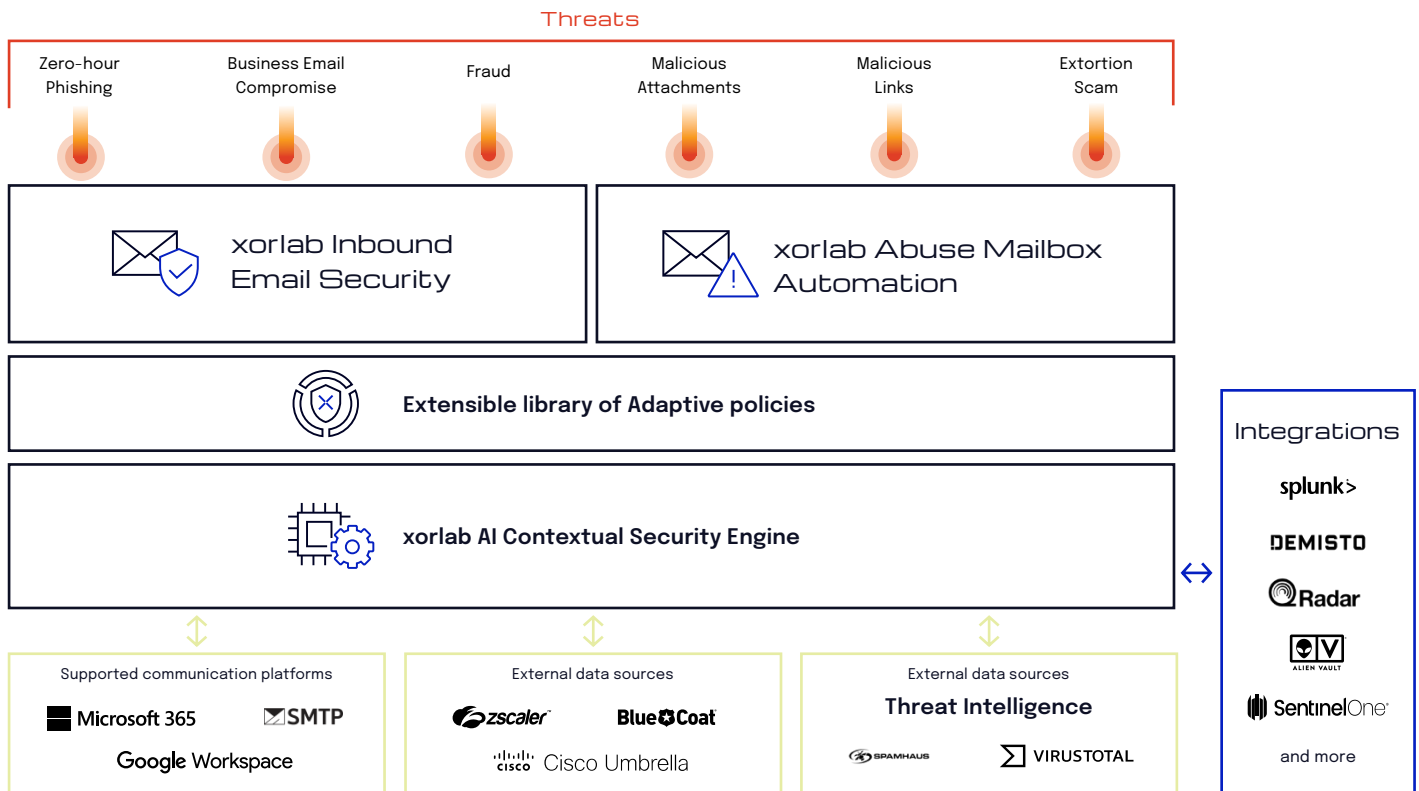
The xorlab Security Platform includes:

xorlab AI Contextual Security Engine:
Classify emails and identify potential threats by analyzing a wide range of signals within each email and comparing them to a learned reference of legitimate communication patterns within your organization.

Extensible library of Adaptive policies:
Customize xorlab's built-in security policies or build your own on top. Adaptive policies automatically adjust to your context, minimizing the need and effort to manage block and allow lists.

xorlab Inbound Email Security:
Rapidly reduce risk by protecting your organization from zero-hour phishing, business email compromise, and ransomware threats. Part of this module is a portal where employees can manage their own quarantine and evaluate suspicious messages in a secure preview.

xorlab Abuse Mailbox Automation:
Collect user-reported emails and analyze them for possible attacks. xorlab prioritizes reported emails based on risk and responds with case-specific feedback. This saves your security staff valuable time in processing these reports. xorlab automates your abuse mailbox management, maximizing security and reducing costs.

Get in touch:

xorlab AG
Binzmühlestrasse 170d
8050 Zurich, Switzerland
contact@xorlab.com

Trusted by:

CERN · coop · HAUFE.Group · Implenia · Julius Bär

KIRCHHOFF AUTOMOTIVE · DIE POST · swisscom · USZ Universitäts Spital Zürich

xorlab.com