

Why Customers Choose xorlab

xorlab is a European email security platform that blocks the advanced phishing attacks Microsoft 365 and on-premises filters miss.

01 Better detection



On average 50% more email attacks detected

Customer data and evaluations show that xorlab detects on average 50% more attacks than existing vendors – including Gartner Quadrant Leaders.



Up to 10x fewer false positives

In a CERN case study, xorlab showed around 10x fewer false positives compared to Microsoft Defender for Office 365.



Gaps exposed and closed – before commitment

See the gaps in your current email security with an Email Attack Simulation. Find out how we close these gaps with a Proof of Value in BCC mode – no risk, no disruption to your inbox.

02 Less operational burden

50–80% less manual triage

Abuse Mailbox Automation automates 50–80% of reported-email processing, and prioritizes critical incidents so analysts focus on what matters most first.

4–5x faster analyst handling

Remaining reported emails can be processed 4–5x faster through the xorlab console.

03 European, trusted and flexible



Deployed your way

xorlab supports cloud, on-premises, and hybrid deployments.



Trusted by rigorous customers

Used by 6 of the 10 largest Swiss banks and other regulated organizations.



Data stays in Europe

Supports customers with privacy, compliance, and data residency needs.



Modular and scalable

Customers only buy the modules they actually need and can expand as requirements grow.

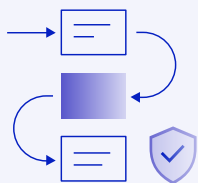
xorlab Portfolio Summary

The xorlab platform is built for critical infrastructure and other highly regulated environments and compliant with DORA, NIS2, and GDPR.



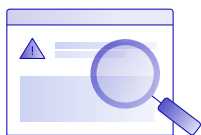
Inbound Email Security

Advanced attacks can bypass standard email defenses. xorlab stops them before they reach employees—without replacing your existing security tools. Deploy it as a standalone solution or add it as an extra layer of protection to your current security stack.



Abuse Mailbox Automation

Manual review of reported emails slows response to real threats. xorlab automates 50–80% of triage, highlights what matters, and gives instant feedback, helping teams focus on real cases and work up to 4–5x faster with less effort.



Sandbox / Airlock

xorlab analyses all attachments, including encrypted or password-protected files when needed, to uncover hidden threats that standard security tools may miss.



Self-Service Quarantine (SSQ) / Portal

Employees often rely on the helpdesk for emails stuck in quarantine. xorlab lets them safely review messages and request their release within customer-defined policies—so important emails reach their inboxes sooner while reducing support tickets and analyst workload.



Contextual Banners

Employees receive clear, colour-coded banner guidance inside emails whenever something looks unusual (e.g. new sender). The banners can be customised per customer, helping users quickly recognise threats before they lead to costly breaches.