Take your Email Platform to the Next Level

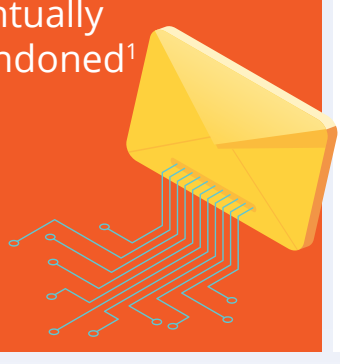
THE TRUE COST OF UNSUPPORTED EMAIL

The real cost of email isn't always visible on a budget sheet. It appears in maintenance effort, security exposure, compliance demands, and lost productivity.

1 Hidden Cost of DIY Solutions

A recent industry research from Exclaimer (1) highlights the hidden costs organizations face when building and maintaining IT solutions themselves. What appears cost-effective at first can create significant operational costs over time:

71%
of DIY tools are eventually abandoned[1]



$20K-$100K
in hidden maintenance costs reported by 66% of teams surveyed[1]

up to 10-50 hours/month
spent just maintaining their infrastructure [1]

8%
of in-house projects finish on time. Only 11% stay on budget.[1]

2 People Trap

Maintaining in-house solutions comes at a productivity cost:

91% say maintaining in-house tools directly reduces their team's productivity[1]

of which

41% report the impact is significant, not just a minor drag on the day[1]

of which

1 in 2 say it stops them focusing on strategic work entirely[1]

3 Compliance Gap

Unsupported email creates business risk. Inconsistent patching can leave IT teams exposed to vulnerabilities, attacks, and downtime. Without a vendor behind your email, compliance becomes your problem, and your liability.

Missed Patch
Critical updates are delayed or overlooked.

Open Vulnerabiluty
Attackers can exploit known flaws in your systems.

Security Incident
Unauthorized access, malware, ransomware or data breach occurs.

Downtime/ Compliance Pressure
Operations are disrupted customers are impacted, and compliance is at risk.

64% of organizations experience preventable downtime[1]

Email remains the leading attack vector for cyber threats. Recent Exclaimer research found that 59% of UK legal organizations (3) and 73% of US businesses (2) experienced an email security incident in the past year.

KEEP THE FREEDOM. GAIN THE SUPPORT.

What changes when you move to a fully supported email platform:

Unsupported Solution	Fully Supported Zimbra
Community-maintained patches	Proactive vulnerability monitoring
No vendor response	Expert support when you need it
Delayed or absent CVE fixes	Regular security patch releases
Limited modern capabilities 71% of tools eventually abandoned	Continued investment in R&D - 130+ new features delivered in the last 12 months
Manual compliance evidence	Public CVE history and patch documentation

71% of CTOs say vendor solutions are more secure and dependable than internal builds (1).
The question isn't whether you can afford to switch - it's whether you can afford not to.

READY TO MAKE THE MOVE?

Talk to a Zimbra Expert

Sources
1. The Build vs. Buy Report: Making the Case for Bought Software. Exclaimer Ltd., 2024. Base: n=2,000+ IT and cybersecurity decision-makers across the US and UK. All rights reserved.
Data cited for informational purposes with attribution.
2. US Business Email Report 2025. Exclaimer Ltd., 2025. Base: n=1,000+ US-based IT decision-makers. All rights reserved. Data cited for informational purposes with attribution.
3. UK Business Email Report 2025. Exclaimer Ltd., 2025. Base: n=1,000+ UK-based IT decision-makers. All rights reserved. Data cited for informational purposes with attribution.