mailsite®

WHITE PAPER

Open Source Email Security Solutions: 10 Questions

A strategic resource for IT decision-makers in small and medium size businesses

A MailSite White Paper

November 2026

© 2026 Rockliffe Systems, Inc. All rights reserved. MailSite is a registered trademark of Rockliffe Systems, Inc. All other trademarks are the property of their respective owners.

1 Introduction

1.1 Email security: a strategic issue

Email security has become a strategic issue for IT executives. The risks of making a mistake are business critical. The cost of a wrong decision is measured not in wasted IT budgets, but in lost revenue, fraud, leaked confidential information and, increasingly, legal claims. A virus or a phishing message that gets through can stop your business for hours or days. A compromised mailbox can be used to send spam and malware to your customers and suppliers in your name.

Email attacks also keep growing in sophistication. Many no longer carry an obvious virus at all: they aim to steal user names and passwords, or to trick staff into paying a fake invoice.

1.2 Build or buy?

One of the key choices in an email security decision is whether to **build** or to **buy**. To build is to assemble your own solution around a mail server from separate programs, many of them open source. To buy is to choose a mail server that comes with its security filtering already integrated and maintained by its vendor.

This is less a question of open source against commercial software than it first appears. Much of the best email security software is open source, and good commercial products use it. MailSite 11, for example, scans mail with ClamAV, a widely used open source anti-virus engine. The core issue is who assembles the parts, who keeps them up to date and who is accountable when something fails: your own staff, or a vendor whose business depends on it.

1.3 Aim of this paper

This paper offers a checklist of risk management questions for IT executives facing a "build or buy" email security decision. It does not try to give the answers. It highlights the issues to address during the process. The answers will depend, among other things, on each organization's culture, skills, core competencies, strategic goals and cash flow.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

2 10 Questions

1. Do you need to review your build or buy culture?

As the technology market matures, fewer organizations keep a blanket preference for building or for buying. It has become good practice to judge each purchasing decision on its own merits, rather than on how things were done before.

If your organization still has such a preference, what is it based on? Is it one person's taste? If it rests on an informal risk assessment made years ago, is that assessment still valid?

Most small and medium size businesses don't use formal risk assessment methods. Even so, a regular informal review of the reasons behind past build or buy decisions helps stop old habits from becoming bad policy.

2. Is this the best use of your in-house resources?

Building and running your own solution takes more staff time than running an integrated product. That time has an "opportunity cost": the value of the other projects that are cancelled or delayed as a result.

The size of the opportunity cost depends on how important those projects are. For example, the cost of delaying a new online store depends on the revenue, customer retention or market share it was expected to bring.

The opportunity cost of diverting internal resources is an important part of the decision, and one that is often overlooked.

3. Is a home-built or an integrated solution more reliable?

For email, the main security question is not which operating system or which scanner is the most secure. It is whether the protection stays current. New threats appear every day, and filtering is only as good as its latest updates.

With a home-built solution, your administrator must watch every component, apply each update and check that the whole mail flow still works afterwards. If one component's updates stop, or an update breaks the chain, your administrator has to notice and fix it.

With an integrated product, keeping the components current is part of the product. Vendors usually limit their liability, but timely and reliable updates are core to their business: customers move elsewhere if updates fail. MailSite 11, for example, downloads new ClamAV virus definitions and new versions of the ClamAV engine by itself. Automatic updates are on by default, and the Console shows the update status.

4. Is your cost analysis comprehensive?

For any organization facing a build or buy choice, the total cost of the project will be a key factor, if not the key factor, in the decision.

Open source programs carry no license fee, but a solution built from them is not free. Compared with an integrated product, it needs more time to choose, install, configure and connect the programs, to apply their updates and to keep their threat data current. Each change also needs time for documenting, testing and fixing problems.

Other costs of a home-built solution are easy to overlook:

- **More staff time:** someone has to run, monitor and troubleshoot every component, every day.
- **Higher skills:** running and debugging a custom mail filtering chain needs more specialized expertise, which costs more to hire and to keep.

Compare these costs with the license and support cost of an integrated product over the same period.

5. Is this the best strategic fit for your company?

Map the implications of building or buying against your broader business pressures and strategic goals.

Building your own solution is a long-term commitment to keep in-house people who understand it. If keeping that resource is not a strategic goal for your organization, there is a risk that the people will be cut or moved to higher priority projects, and the solution left behind.

On the other hand, a packaged product can risk lock-in to a single vendor and rising license and support fees. You can reduce this risk by choosing a product built on open standards, which is easy to replace and adapts readily to changing needs. MailSite, for example, uses the standard mail protocols (SMTP, IMAP and POP), standard Sieve filtering rules and the standard Exchange client protocols, and keeps your mail on a server you control.

6. Is there a satisfactory disaster recovery strategy?

Even the most comprehensive and sophisticated email security cannot guarantee 100% protection. If an infection does occur, or data is compromised, what matters most is the speed of recovery.

Successful recovery depends on having the skills to clean up the network, find the cause of the problem and fix it.

The skills needed for recovery are usually higher for a home-built solution than for an integrated one. This has cost implications. It can also slow recovery badly if the solution can only be debugged and patched by the engineers who built it, and they are away or have left the company.

Whatever you choose, keep tested backups of your mail and configuration, and practice restoring them.

7. Is there adequate provision for maintenance and updates?

Virus definitions are only part of the job. Spam changes constantly, so someone must also tune the spam rules, maintain the lists of known bad senders and keep the filter learning from new mail. Ask who will do this work, and who is accountable if it is not done.

This is a key part of what an integrated product offers. MailSite 11 scores each message with Bayesian classification and with checks such as SPF, DKIM and DMARC failures, hidden text and disguised links. It looks up senders and links in public reputation lists, and it can delay first-time senders with greylisting. Administrators adjust the weights and word lists in the Console, without restarting the server.

Automated updates, installed with no administrator action, save time and money. They are also a faster and more dependable way to keep defenses current.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

8. Are deployment and update time estimates accurate?

Thanks to the tools built by the open source community, installing individual filtering programs has become much faster. Connecting several of them into one reliable mail flow still takes time, and each update can mean testing the whole chain again. It will usually take longer than deploying a product with its security modules already integrated.

Good integrated products also come with documented, standards-based interfaces that make it quicker to fit them into your existing systems. MailSite 11 installs with one PowerShell command. Virus scanning, spam scoring, greylisting and Sieve filtering are then configured in the same Console as domains and mailboxes.

As a result, deployment and update timelines for an integrated product should be significantly shorter.

9. Is there adequate provision for creating and maintaining the documentation?

One of the key challenges for an in-house solution is keeping its documentation complete and current. Even with the best intentions, competing work often pushes documentation down the list, and it is neglected.

A good packaged product has detailed administration guides that the vendor updates regularly. A good vendor backs them up with support services, technical papers and a knowledge base. MailSite 11 comes with an Administrator Guide and release notes for each release, plus a knowledge base and support cases through the MailSite support portal.

An administrator's email security masterpiece can quickly become an expensive liability if its authors leave the company, or are simply on leave.

10. Will this solution help differentiate you from your competitors?

If your organization is in finance, internet services or web hosting, or handles sensitive data, you know that email security is a strategic differentiator. Securing your clients' communications and data is a core business requirement.

Security threats spread around the world in minutes, and the same threat can come back within hours in many slightly different forms. Protecting against them needs the best defenses your budget can buy.

It used to be said that organizations should "buy for parity, build for advantage". That maxim holds only if what you build protects you at least as well as what you could buy. Often the advantage lies elsewhere: in the time your team saves for the work that really sets you apart.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

3 Checklist

10 questions to ask yourself before choosing a home-built email security solution

#	Question	Yes / No
1	Do you need to review your build or buy culture?	
2	Is this the best use of your in-house resources?	
3	Is a home-built or an integrated solution more reliable?	
4	Is your cost analysis comprehensive?	
5	Is this the best strategic fit for your company?	
6	Is there a satisfactory disaster recovery strategy?	
7	Is there adequate provision for maintenance and updates?	
8	Are deployment and update time estimates accurate?	
9	Is there adequate provision for creating and maintaining the documentation?	
10	Will this solution help differentiate you from your competitors?	

Read more about MailSite's anti-virus and anti-spam protection, or start a free trial and test them on your own mail.

4 About MailSite

About Rockliffe Systems

Rockliffe Systems develops MailSite, a mail and collaboration server for Windows and an alternative to Microsoft Exchange, for service providers, hosting providers, enterprises and businesses. Rockliffe has built messaging software since 1995.

MailSite 11 delivers email, calendars, contacts, tasks and notes to Classic Outlook over MAPI over HTTP, to its own ExpressPro webmail and to iPhone and Android devices over Exchange ActiveSync. Its built-in security includes ClamAV anti-virus, Bayesian anti-spam with reputation lists and greylisting, Sieve filtering and free Let's Encrypt certificates for every domain.

MailSite Professional Services

Rockliffe Professional Services can help with migrations to MailSite and other projects. To discuss your needs and arrange a quote, contact us or email sales@mailsite.com.

www.mailsite.com