BUYER'S GUIDE

Email Security

SAEPIO.CO.UK

SAEPIO

Assured Service Provider

in association with National Cyber Security Centre

TABLE OF

Contents

WHAT IS

Email Security

1

Email Security is a critical component of a business's security stack, with phishing accounting for over 80% of cyber attacks against UK businesses. Email security tools aim to significantly reduce the risk of email borne attacks and have evolved rapidly to meet new challenges and developments.

While Microsoft and Google's inbuilt security has developed significantly, most customers choose to enhance them with a separate tool to address the increasingly sophisticated attacks through this long standing communications channel.

Increasingly sophisticated attacks through this most risky of communication channels.

THE EVOLUTION OF

Email Security

2

Early solutions focused on spam and keyword filtering based on lists of known bad senders or words together with signature-based antivirus protection. As email-borne attacks became pervasive and more sophisticated, many businesses chose to implement a Secure Email Gateway "SEG" to filter spam, phishing and malware-based threats at the corporate perimeter, utilising rules and signatures-based detection and filtering before mail reaches the end user.

Cybercriminals advanced their tactics in the face of traditional SEGs, increasingly leveraging AI tools to produce sophisticated targeted emails with spear phishing becoming the new AI-driven normal. New attack vectors including QR code and multi-stage payload attacks are increasingly leveraged. This has led to the rise of next-generation email security tools known as ICES (Integrated Cloud Email Security) that use AI Machine Learning and Natural Language Processing for content and behaviour analysis enabling them to detect threats such as impersonation and zero-day attacks.

This approach has become vital with the rise of Business Email Compromise BEC in which attackers use impersonation to hijack legitimate accounts and exploit trust relationships using deception and social engineering rather than malware. These attacks frequently target finance and HR departments. In fact, BEC currently generates approaching 3x more direct financial loss than ransomware. It certainly doesn't get 3x the media headlines and awareness.

ICES tools establish a baseline for the communications of every sender and recipient, enabling them to detect anomalous behaviour and adapt to new attack forms. These solutions typically sit alongside an email platform like Microsoft using API integrations rather than being in line with the Mailflow.

CHOOSING THE RIGHT

Email Security Solution

3

In today's cyber security landscape, it can be challenging to distinguish between the numerous email security vendors. The aim of this guide is to simplify your decision-making process and guide your review of the market.

KEY

Considerations

4

Technology Stack

- **Current Security Tool:** Many customers currently have a SEG in place, some choose to retain this alongside a next generation solution, but most Saepio customers decommission it once the new tool is fully up and running. It is important to evaluate if there are operational reasons to retain the gateway alongside a new solution.
- **Email Provider:** Most tools integrate with both Microsoft and Google, but it is important to check this. Some solutions were built from the ground up around specific platform and therefore have particular strengths with that ecosystem.
- **Mailflow:** Most customers value the simplicity of the API-based integration over the traditional method of altering MX Records. However, it is important to consider any specific Mailflow requirements, including ticketing/customer support systems where mail is not routed to an end user mailbox. These solutions require a customised approach to email security.

Operational Model

- **Ease of setup:** The tool should be simple to implement and have a strong learning period to learn the baseline normal for your organisation. There should be clear plan to move the tool from learning to full protection while minimising disruption.
- **Daily interaction:** A modern email tool should require minimal interaction beyond general monitoring and the occasional threat hunting activity.
- **Ease of Use:** As above, the solution should have an intuitive, simple UI. Focus on two areas: delivery of key statistics and events, together with ease of threat hunting and investigation of emails/email campaigns when needed.
- **End User Experience:** This is a key focus area. Do you want your staff insulated as much as possible with all potentially malicious and suspicious mail removed from their inbox or would you prefer an education led approach with 'sanitised' mail and banners? Different solutions approach this in differing ways, and it is important to find the right balance for your teams and organisation.

- **End User Reporting:** Most solutions offer a form of end user phishing reporting, with streamlined workflows to investigate suspicious emails. Some tools even offer AI led investigation streams to fully automate the process. It is important to consider this while reviewing tools.

- **Customisation:** Some customers choose to leave the solutions in 'out of the box mode' while others may wish to heavily customise the actions and responses taken by the tool. This is dependent on the needs of users and your organisation. If you do require customisation, it is important to review how this is done. Some vendors enable you to customise the solution right down to individual users and mailboxes, others may require a support ticket. You should ensure that possible future requirements can be easily addressed.

- **Integration:** If needed, can the solution integrate with your existing technology stack, notably SIEM or MDR tooling?

Additional Consideration/Platform Capabilities

- **End User Training:** Some tools can additionally deliver sophisticated end user training including videos and targeted test emails. These can even be based on genuine attacks aimed at the user/organisation for maximum authenticity.

- **Collaboration:** Some tools extend their protection to collaboration tools such as Slack and Teams which form an increasingly exploited attack vector. Note that the functionality of solutions differs significantly, so if this is a priority for you and the organisation it would be worth specifically challenging the vendors on what their solution can and cannot do in this area.

- **Outbound Security:** Data Loss Protection is a developing focus area, and some solutions offer additional tools to mitigate this. Again, the functionality varies widely between tools ranging from preventing misdirected email/mistyped recipient through to fully fledged DLP solutions. If this is important to your organisation, you should review this alongside the inbound security tool, and it may be worthwhile looking at a separate outbound solution if a robust data loss posture is crucial.

- **Archiving/Backup:** Historically, solutions for email archiving and mailbox backup were offered as part of a comprehensive package by SEGs. This i snot currently common with ICES tools. Saepio can assist you in assessing your requirements in this area, as they differ from organisation to organisation.

COMPARISON

Criteria

5

- **Commercials:** What are the pricing metrics? What is the annual purchase cost? How expensive would it be to add additional end users if the organisation grows?
- **Roadmap:** Does the vendor have a clear roadmap for the development of their solution, both in terms of new features, but also to quickly respond to new threats?
- **Customer Service:** How would the contract be managed, is support available when it is required?
- **Resilience:** Email is a critical communications tool for the business, does the solution guarantee a sufficient level of resilience and availability?
- **User feedback:** What do existing customers, especially within your industry say about the vendors?

NEXT

Steps

6

Choosing the right Email Security provider is a strategic decision, and Saepio is here to guide you every step of the way. Here's how we help customers move from evaluation to a confident selection:

Step 1. Define your requirements

Understand your environment, current challenges and goals and organisational specific requirements.

Step 2. Build a shortlist of providers

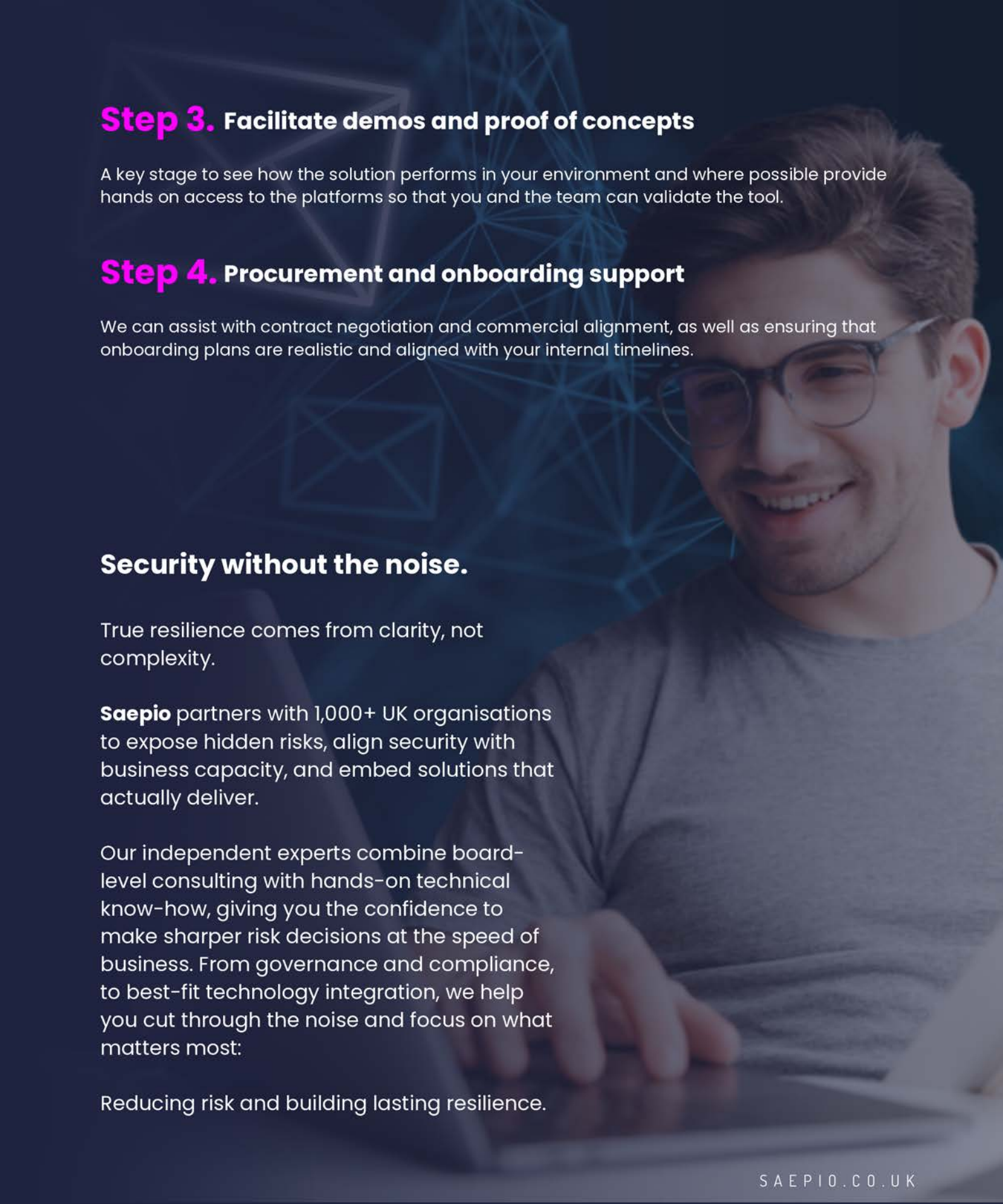
Using our vendor-neutral approach to shortlist providers based on your requirements.

Step 3. Facilitate demos and proof of concepts

A key stage to see how the solution performs in your environment and where possible provide hands on access to the platforms so that you and the team can validate the tool.

Step 4. Procurement and onboarding support

We can assist with contract negotiation and commercial alignment, as well as ensuring that onboarding plans are realistic and aligned with your internal timelines.



Security without the noise.

True resilience comes from clarity, not complexity.

Saepio partners with 1,000+ UK organisations to expose hidden risks, align security with business capacity, and embed solutions that actually deliver.

Our independent experts combine board-level consulting with hands-on technical know-how, giving you the confidence to make sharper risk decisions at the speed of business. From governance and compliance, to best-fit technology integration, we help you cut through the noise and focus on what matters most:

Reducing risk and building lasting resilience.

SAEPIO.CO.UK

SAEPIO

Assured Service Provider

in association with National Cyber Security Centre