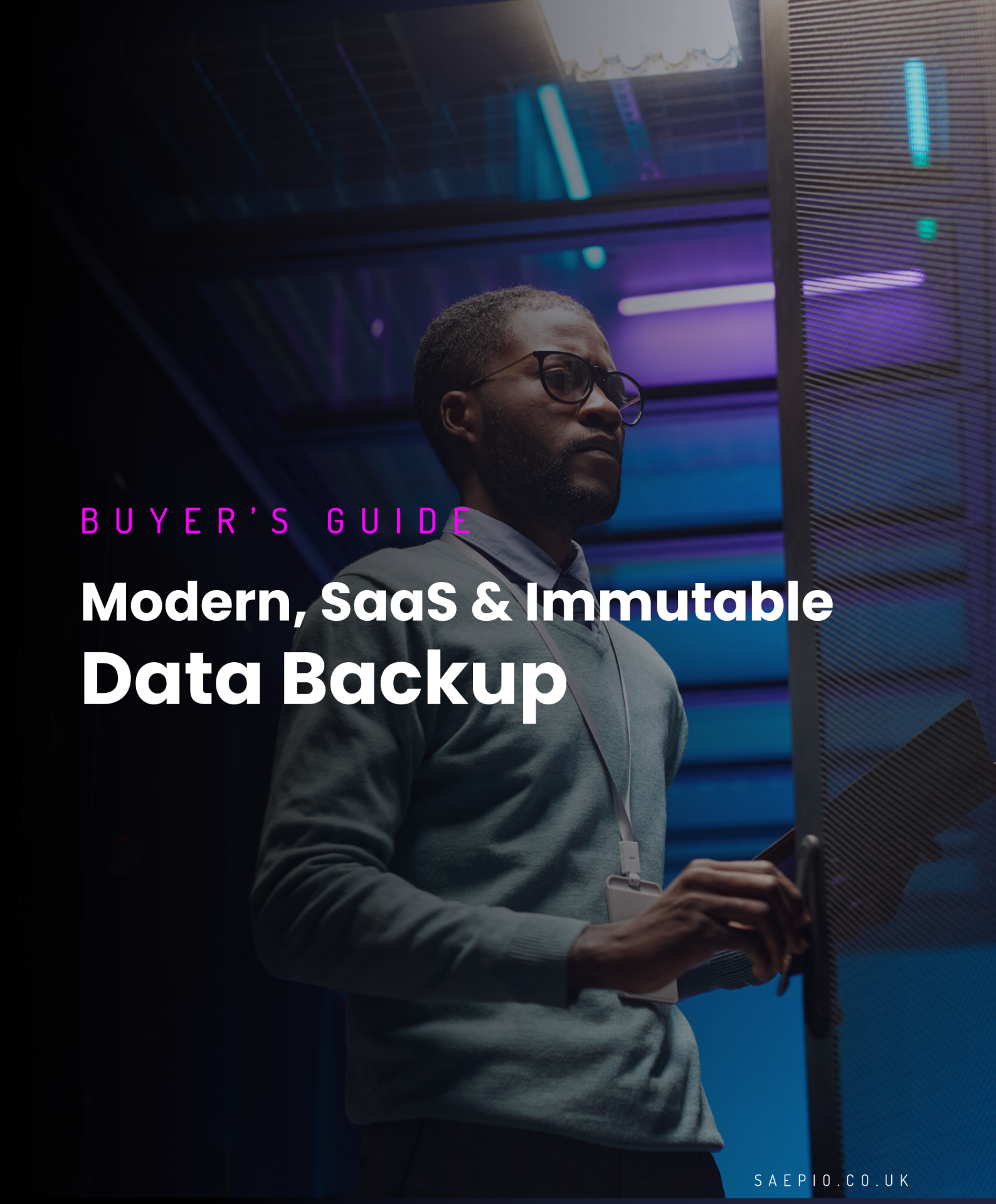


BUYER'S GUIDE

Modern, SaaS & Immutable Data Backup

SAEPIO.CO.UK

SAEPIO

CREST PEN TEST

CYBER ESSENTIALS PLUS

Assured Service Provider

in association with National Cyber Security Centre

CHECK Penetration Testing

Cyber Advisor

TABLE OF

Contents

Contents 2

What is Backup? 3

Why do you need a modern, immutable backup provider? 3

Importance of choosing the right backup provider 4

Key Considerations 5

Key Questions to Ask 6

Next Steps 7

DATA BACKUP

What is Backup?

Traditionally, backup has been focused on recovering lost data and restoring business operations after hardware failures, accidental deletion, corruption, or disaster events to minimise downtime and data loss.

Modern backup providers help businesses in the process of duplicating and storing data with automated backup, fast recovery and often includes ransomware resilience capabilities with compliance focussed retention. Many providers assist organisations in both cloud and on-premises workloads. Modern backup solutions are no longer just about data availability. They bring together data resilience, operational security, and rapid recovery capabilities to help organisations meet increasingly stringent security and compliance requirements.

DATA BACKUP

Why do you need a modern, immutable backup provider?

Many modern Backup providers address the risk around data safeguarding in a landscape where ransomware is prevalent. Threat actors often prioritise the infection of backup stores to prevent organisations restoring securely. Modern backup providers safeguard critical data across SaaS applications, cloud workloads and on-premise environments. These solutions provide independent and immutable (unchangeable) backup and recovery capabilities, helping reduce the risk of backup data compromise, ransomware impact, business resilience and recovery speed.

Traditional and non-security-centric backup solutions face several issues, including cost, maintenance and security risks and fall into 'single points of failure,' where proprietary local backup appliances can fail entirely. If a threat actor gains domain administrator credentials, they could move laterally through the network, locate and compromise backup servers before deploying ransomware on live systems.

Dedicated SaaS and Modern Backup providers are ideal for organisations that:

- Have significant SaaS adoption
- Hybrid or multi-cloud environments
- Critical data storage within Microsoft and Google environments
- Strict security compliance requirements
- Organisations that require centralised data protection, rapid, reliable and tested backup processes, as well as consistent governance across IT environments.

Modern Backup providers often prioritise ransomware resilience by combining immutable backups, air gapped storage and versioning that allows clean and rapid point in time recovery. Alongside this, they continuously monitor for suspicious activity and can pause backup processes to prevent corruption.

Regulatory frameworks such as DORA, NIS2 and UK Cybersecurity Frameworks also demand specific, highly granular backup procedures and data segregation. This, combined with the growing need for immutable, tamper-proof backups, regular recovery testing, and rapid restoration capabilities, makes the adoption of dedicated backup solutions a business-critical requirement.

DATA BACKUP

Importance of choosing the right Backup provider

Choosing the right backup provider is a critical decision. The ideal backup provider should become a trusted partner for our customers, ensuring your data is protected and securely recoverable in a manner that delivers on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), as well as compliance needs to ensure business continuity.

Traditional backup solutions were built to recover data after outages, hardware failures, or accidental deletion. However, as ransomware and cyber threats have become more prevalent, Saepio customers are increasingly looking for solutions that do more than just restore data. Modern security focused backup platforms combine backup and recovery with capabilities such as immutable backups, isolated storage, ransomware detection, and simplified management, helping organisations improve cyber resilience, reduce operational overhead, and recover with greater assurance that clean data is being restored with integrity more rapidly when incidents occur.

While backup has traditionally been the responsibility of IT teams, there is an increasing need for shared visibility between IT and Security. Organisations should prioritise solutions that provide a unified view of data protection, cyber resilience, and recovery posture, helping bridge operational silos and strengthen overall security.

The modern security landscape highlights a real importance for ‘security first’ backup solutions and better data resiliency processes, with 93% to 94% of ransomware attacks actively targeting and compromising backup systems.

DATA BACKUP

Key Considerations



Technology Stack

- **Current Backup Tool:** Many customers have some form of backup solution in place. However, many Saepio customers question whether their current solution can protect against ransomware and support rapid recovery through features such as immutable backups, isolated storage, and threat detection?
- **Coverage Across the Environment:** Alongside Physical Servers, Virtual Machines, Databases, Kubernetes and application data, it is imperative to ensure the solution can protect all cloud workloads, including Microsoft 365 and Google Workspace environments. It is important to note that Microsoft and Google protect the infrastructure and provide retention and recovery capabilities for service outages, but they do not guarantee protection against all forms of data loss, such as accidental deletion, malicious insiders, ransomware, user error, or retention policy misconfigurations.



Operational Model

- **Ease of Management:** Consider the operational overhead required to manage multiple backups, storage, infrastructure, updates, and capacity planning with regular testing. Regulations like GDPR, ISO 27001, SOC 2, and DORA mandate regular, documented restore testing to prove data can be retrieved within defined Recovery Time Objectives (RTO).
- **Scalability:** Can the solution grow with the business without requiring significant investment in additional hardware, storage, or management resources?
- **Recovery Time Objectives:** Customers should assess how quickly critical applications must be restored, validate that recovery targets are achievable through regular testing, and ensure the chosen solution can meet both their recovery time and recovery point objectives without introducing operational complexity.



Additional Consideration/Platform Capabilities

- **Compliance and Governance:** The solution should support retention requirements, auditability, and regulatory obligations while providing visibility into protected data.
- **Future Readiness:** Consider whether the platform can support future cloud adoption, evolving security requirements, and broader cyber resilience initiatives without requiring multiple additional products. This can also assist with cost predictability.

DATA BACKUP

Key Questions to Ask

- How would you recover if a privileged user deleted a large volume of Microsoft 365 or Google Workspace data?
- Are your cloud applications, endpoints, servers and cloud infrastructure backed up with unified visibility?
- Are you relying on Microsoft or Google to restore deleted or corrupted data?
- Do you have isolated copies of data outside the production SaaS environment?
- Are you confident you can restore individual emails, files, users, Teams data, or entire workloads quickly?
- How long could the business operate without access to critical data?
- What are your required Recovery Time Objectives (RTOs)?
- What are your Recovery Point Objectives (RPOs)?
- How quickly do business units expect critical data to be recovered following an incident?
- Have you tested recovery against these expectations?
- What regulatory obligations do you need to meet (GDPR, DORA, ISO 27001, etc.)?
- Is backup data encrypted in transit and at rest?
- Who has access to backup repositories?
- Would you prefer a platform that can consolidate backup and cyber resilience capabilities?

Next Steps

Step 1. Define your requirements

Work with one of Saepio's Backup specialists to assess your environment, identify any data resilience gaps, and understand your compliance requirements. We'll review your current backup strategy, recovery objectives, and overall resilience maturity to determine the key drivers behind your project and define what success looks like.

Step 2. Build a shortlist of providers

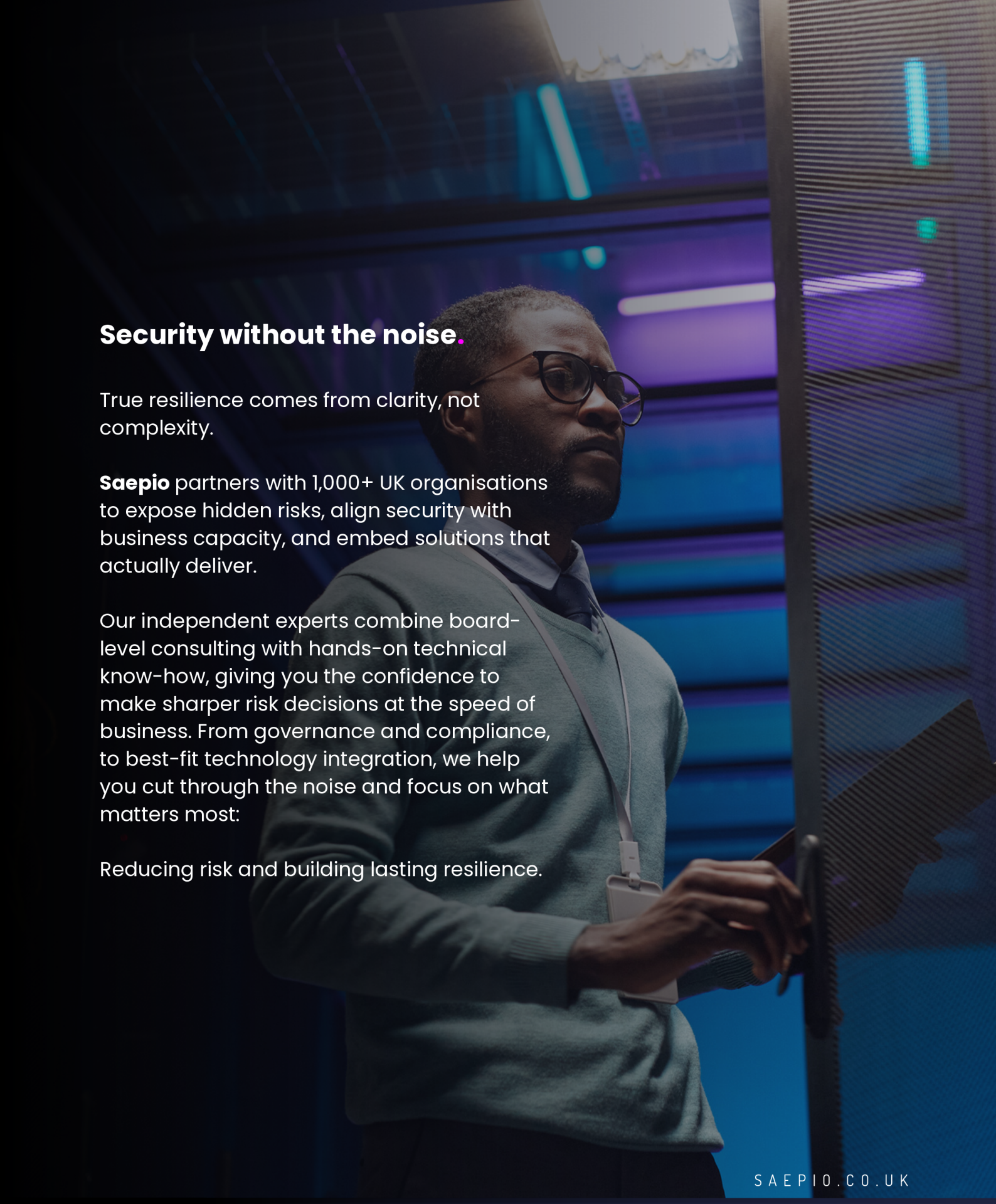
With extensive experience across the Backup market and a vendor-neutral approach, Saepio can help you navigate the available options and identify the solutions best suited to your needs. We'll provide unbiased guidance on the strengths, limitations, and considerations of each provider, helping you build a focused shortlist.

Step 3. Facilitate demos and proof of concepts

We'll coordinate technical deep dives, vendor demonstrations, and proof of concepts so you can evaluate each solution in the context of your own environment. This helps validate capabilities, usability, and alignment with your operational and security requirements.

Step 4. Support procurement and onboarding

Once a vendor is selected, we assist with contract negotiation and commercial alignment, as well as ensuring onboarding plans are realistic and aligned with your 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

CREST PEN TEST

CYBER ESSENTIALS PLUS

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing
Cyber Advisor