

BUYER'S GUIDE

Identity Security

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 Identity Security?	3
The Evolution of Identity Security	3
Choosing the Right Identity Security solution	4
Key Considerations	4
Comparison Criteria	6
Next Steps	6
Glossary	7

IDENTITY SECURITY

What is Identity Security?

Identity Security is a critical component of a business's security stack. Attackers increasingly log in rather than break in: According to Sophos's State of Identity Security 2026 survey, 71% of organizations experienced an identity-related breach in the past year. Human error and poorly managed non-human identities, such as service accounts and API keys, were the leading causes, which is why identity threat detection and credential hygiene belong on any evaluation checklist.

An identity is no longer just a person with a username and password. It now covers employees, contractors and privileged admins, machines such as service accounts, API keys and workloads, and AI agents that act on a person's behalf, or on their own. Gartner describes identity as the primary security perimeter and attack surface, as organisations embrace remote work, cloud solutions and AI in their workflows.

Identity security tools aim to make sure the right identity has the right access, for the right reason, and to detect and respond when that access is misused. Security leaders are taking notice: 41% of respondents in an Omdia survey named identity as a current priority, ahead of AI governance at 38%.

IDENTITY SECURITY

The Evolution of Identity Security

Traditionally, identity capabilities were bought, deployed and owned as separate categories. Identity and Access Management (IAM) answered "who are you?" with single sign-on (SSO), multi-factor authentication (MFA), provisioning and application integration, usually built on an identity provider (IdP). Identity Governance and Administration (IGA) answered "should you have this?" through access reviews, entitlement visibility and shadow IT discovery. Privileged Access Management (PAM) answered "is elevated access safe?" with credential vaulting, session recording and browser isolation. Identity Threat Detection and Response (ITDR) later added detection of anomalous sign-ins and credential theft.

These silos have been converging. Vendors now sell governance and privileged access alongside SSO and MFA, and some offer just-in-time (JIT) access, which used to sit squarely in PAM territory. The overlaps include IAM with IGA (lifecycle, access requests and reviews, posture), IAM with PAM (privileged access within IdP suites), IGA with PAM (JIT access, break-glass, policy enforcement on privileged resources) and, where all three meet, governance of non-human identities and AI agents, risk-based access and unified visibility.

The risk has also moved from sign-in to authorisation. Most organisations have rolled out SSO, but breaches increasingly come from what identities can reach once they are inside. Over-provisioning is the common thread: joiner, mover, leaver (JML) processes are still largely manual on major identity platforms, so leavers keep access and movers collect it. Identity threat prevention adds a further layer, detecting unusual behaviour and changes to the permissions themselves.

For businesses, this means shopping by acronym can lead to paying for the same capability twice, or assuming a gap exists where there isn't one.

IDENTITY SECURITY

Choosing the Right Identity Security solution

In today's cyber security landscape, it can be challenging to distinguish between the numerous identity vendors, particularly as the traditional categories blur. The aim of this guide is to simplify your decision-making process and guide your review of the market. Our advice is to buy for outcomes, not categories.

IDENTITY SECURITY

Key Considerations



Technology Stack

- **Current Identity Tools:** Most organisations already have an identity provider in place. Establish what your existing platforms already cover, including any governance or just-in-time access capability, before buying more. This avoids paying for the same capability twice. It is also worth evaluating the capabilities of your workplace productivity tools, and any broader security platforms, as pockets of identity security capability are becoming common place.

- **Identity Sources:** A joined-up foundation starts by connecting your HR system to your IdP, so that joiners, movers and leavers drive access automatically. Check what each solution integrates with on both sides.

- **Privileged Access Needs:** Not every business needs the heaviest tool in every category. If privileged access is mainly to cloud resources, JIT access through a governance platform may be enough. Vaulting, session recording and browser isolation are what justify a dedicated PAM product.

- **Identity Coverage:** Does the solution cover every identity, not just employees? Non Human Identities (NHIs) such as Machines, service accounts, API keys and AI agents, along with applications outside SSO, should all be visible and governed.



Operational Model

- **Sequencing:** Start with visibility, add governance, then add privileged controls where the risk justifies them. An early-stage customer may begin with discovery and add IAM or PAM depth later. There should be a clear plan for each stage.
- **Lifecycle Automation:** Joiner, mover, leaver processes should be automated rather than manual, with access requests, approvals and reviews that are simple for managers and reviewers to complete. Manual lifecycle management is a common cause of over-provisioning.
- **Typical Journey:** Most businesses progress in stages. Connect the HR system to the IdP, deliver SSO and MFA for role-based access, introduce a password manager to balance security and friction, add JIT privileged access for sensitive systems, then implement IGA to continuously assess, validate and approve access.
- **Daily Interaction:** A modern identity platform should require minimal administration beyond general monitoring, scheduled access reviews and the occasional investigation.
- **User Experience:** Security should not come at the cost of friction. Consider how SSO, MFA and passwordless options feel to users, and whether a password manager is needed to balance password and biometric complexity without frustrating them.



Additional Consideration/Platform Capabilities

- **Identity Threat Detection:** Some platforms detect anomalous sign-ins, credential and token theft and privilege escalation, run identity posture checks (ISPM) and respond automatically, for example by revoking sessions. Review how these fit alongside your existing detection tooling.
- **Non-Human Identities and AI Agents:** Machine identities and AI agents are growing quickly. Functionality differs significantly between vendors, so if this is a priority it is worth specifically challenging them on what they can and cannot govern.
- **Specialist Capabilities:** Password management, identity verification (IdV) and Cloud Infrastructure Entitlement Management (CIEM) are often delivered as separate tools. Saepio can help you assess which, if any, you need.
- **Customer Identity (CIAM):** In some industries the business value in identity lies with the businesses' customers and consumers rather than employees. Developer-first CIAM platforms support standards-based login and MFA for B2C and B2B apps and can secure AI agents as well as people. It is worth evaluating several options, including open source. Pricing and packaging change often, so verify.

IDENTITY SECURITY

Comparison Criteria

- **Commercials:** What are the pricing metrics, and do they extend to machine identities and AI agents? What is the annual purchase cost? How expensive would it be to add identities as the organisation grows?
- **Roadmap:** Does the vendor have a clear roadmap, both for new features such as governance, privileged access and non-human identities, and to respond quickly to new threats?
- **Integration:** Does the solution support standards such as SAML, OIDC and SCIM, and integrate with your existing technology stack, notably HR, SIEM and ITSM tooling?
- **Customer Service:** How would the contract be managed, is support available when it is required?
- **Resilience:** Identity is the front door to every application. 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?

IDENTITY SECURITY

Next Steps

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

Step 1. Define your requirements

Understand your identity estate, where you are on your identity journey, 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

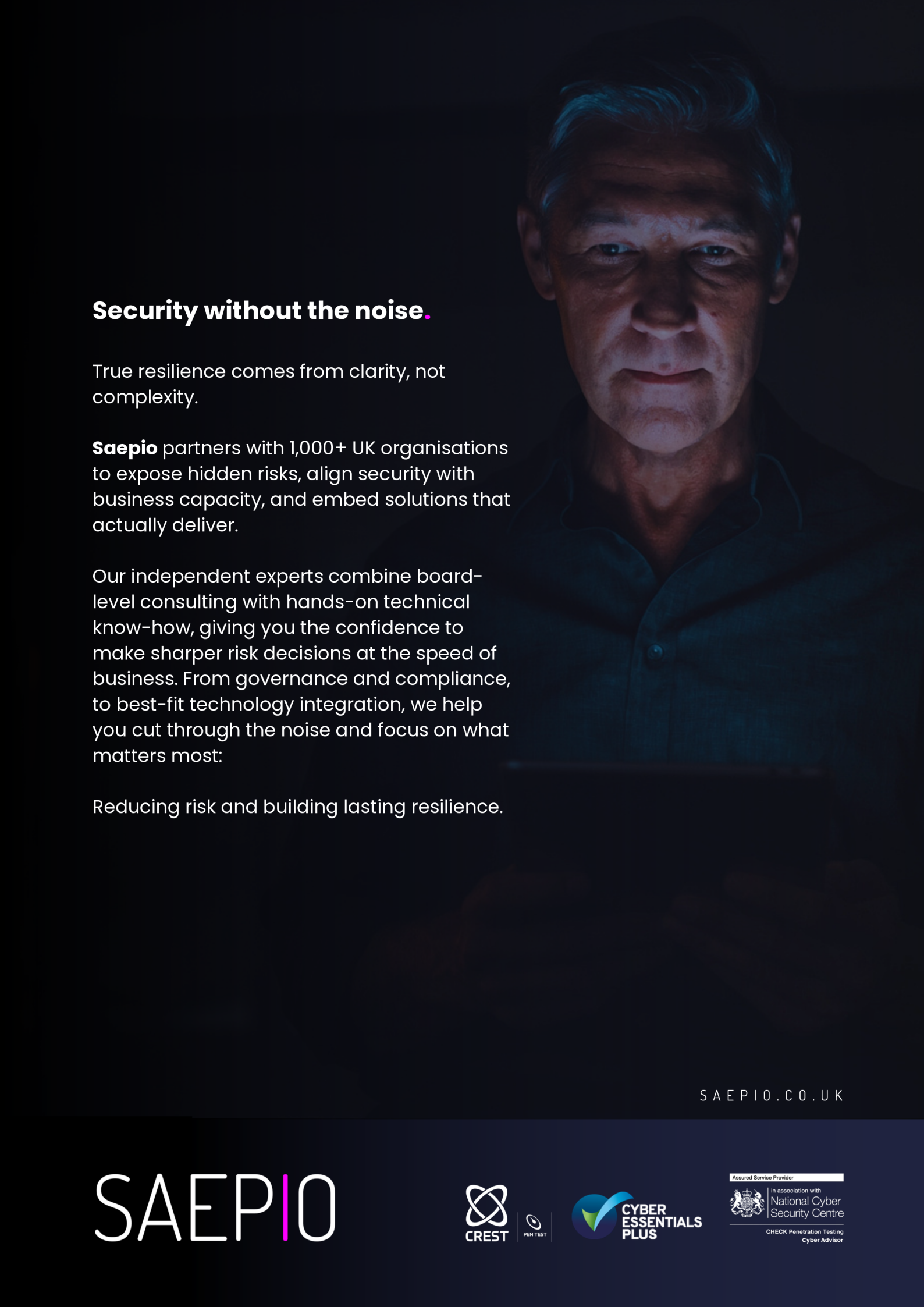
We can assist with contract negotiation and commercial alignment, as well as ensuring that onboarding plans are realistic and aligned with your internal timelines.

IDENTITY SECURITY

Acronym Cheat Sheet

Term	Definition
AI agent	Software that acts on a person's behalf, or autonomously, and holds its own credentials and permissions.
Break-glass access	Tightly controlled emergency access to a privileged account, used when normal routes are unavailable and closely logged.
CIAM Customer Identity and Access Management	Identity management for customers and partners using external-facing applications, rather than employees.
CIEM Cloud Infrastructure Entitlement Management	Tools that find and reduce excessive permissions across cloud platforms.
Entitlement	A specific permission or access right granted to an identity, such as membership of a group or a role within an application.
IAM Identity and Access Management	The tools and processes that establish who a user is and control their sign-in, typically including SSO, MFA and provisioning.
IdP Identity Provider	The system that authenticates users and confirms their identity to applications. It usually underpins SSO.
IdV Identity Verification	Confirming that a person is who they claim to be, for example by checking a photo ID against a live selfie.
IGA Identity Governance and Administration	Managing and reviewing who has access to what, through access requests, certification reviews and entitlement visibility.
ISPM Identity Security Posture Management	Continuous checks on identity configuration to spot weaknesses such as dormant accounts, missing MFA or excessive permissions.
ITDR Identity Threat Detection and Response	Detecting and responding to identity-based attacks, such as anomalous sign-ins, credential and token theft, and privilege escalation.
ITSM IT Service Management	Tools used to manage IT requests and tickets, including access requests and approvals.
JIT access Just-in-time	Granting elevated access only when it is needed and for a limited time, rather than leaving it in place permanently.
JML Joiner, Mover, Leaver	The lifecycle of an employee's access as they join, change role within, or leave an organisation.

MFA Multi-factor Authentication	Requiring two or more proofs of identity to sign in, such as a password plus a code or biometric.
NHI Non-Human Identity	An identity belonging to a machine rather than a person, such as a service account, API key or workload.
OIDC OpenID Connect	A modern standard for sign-in that lets an identity provider confirm a user's identity to applications.
PAM Privileged Access Management	Securing elevated accounts through credential vaulting, session recording and access controls.
Passwordless	Signing in without a password, using methods such as biometrics, passkeys or hardware security keys.
Provisioning	Creating, updating and removing user accounts and access in applications.
SAML Security Assertion Markup Language	A long-established standard for passing authentication information between an identity provider and applications for SSO.
SCIM System for Cross-domain Identity Management	A standard for automating the provisioning of user accounts between systems.
Shadow IT	Applications and services used without the knowledge or approval of the IT team.
SIEM Security Information and Event Management	A platform that collects and analyses security logs from across the estate to detect threats.
SSO Single Sign-On	Letting users access multiple applications with one set of credentials and a single sign-in.



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