SOCURA

eBook



Beyond the noise

7 signs it's time to **rethink** your cyber security partner

For IT and security leaders

socura.co.uk

Your security provider might be meeting its SLAs. **But is it giving you confidence?**

Effective security is about more than technology, tools and contractual commitments. It's about trust, transparency, consistency and knowing the right people are there when you need them.

The difference between an adequate provider and a great one often shows in everyday interactions: unanswered questions, missed commitments, unclear reporting or the feeling that you're doing more work to manage your provider than they are doing to support you. On their own, these frustrations seem minor. Over time, they add pressure to your team and chip away at confidence.

Cyber security is complex. Working with your security partner shouldn't be.

The seven signs at a glance

For each sign, we cover what you might notice, what better looks like and one question to ask.

01	**A lack of transparency** When visibility is limited, confidence disappears.	p.3
02	**Inconsistent delivery** Good security shouldn't depend on a good day.	p.4
03	**Unexpected costs** Clarity should extend to your contract.	p.5
04	**Reactive support** Being available isn't the same as being present.	p.6
05	**A one-size-fits-all approach** Your organisation isn't standard. Your security shouldn't be either.	p.7
06	**A lack of accountability** Trust comes from follow-through.	p.8
07	**An unwillingness to collaborate** The strongest security partnerships work together.	p.9

Then use the **self-assessment on page 11** to reflect on your current arrangements.

01 / 07



A lack of transparency

When visibility is limited, confidence disappears.

Reports can be overly technical, incomplete or focused on activity rather than outcomes. Gaps in coverage and the limits of the service can stay unclear. It's rarely deliberate; more often it's a symptom of poor process or communication. Either way, if you can't see what's happening, you can't make informed decisions about your risk.

What you might notice

- Reports full of activity counts, with little explanation of what they mean
- Uncertainty about which systems are being monitored and which aren't
- Questions that get vague answers, or none at all

What better looks like

Reporting explains what happened, why it matters and what was done about it. Limitations are discussed openly, and asking questions never feels awkward.

The question to ask

Can we clearly explain what our provider is doing to protect us, and where our remaining risks lie?

02 / 07



Inconsistent delivery

Good security shouldn't depend on a good day.

Impressive technology and credentials mean little if everyday service falls short. Missed deadlines, patchy communication and commitments that slip rarely compromise security on their own. What they do reveal are weaknesses in process and accountability, which are exactly what you'll rely on during a serious incident. You shouldn't need a breach to find out whether your provider is dependable.

What you might notice

- Deadlines and agreed actions that regularly need chasing
- Service quality that varies depending on who you speak to
- Changes you find out about after they've happened

What better looks like

Expectations are realistic and consistently met. Responsibilities are clear, commitments are tracked and you hear about changes early, from your provider.

The question to ask

Does our provider do what it says it will, without us having to chase?

03 / 07



Unexpected costs

Clarity should extend to your contract.

Providers include different things in their contracts. Activities that look standard may be charged as extras, and changes in scope or data volumes can shift costs significantly. There's nothing wrong with charging for additional work, as long as it doesn't come as a surprise. And the lowest headline price is rarely the best value over the life of a contract.

What you might notice

- Invoices that don't match the figure you budgeted for
- Routine requests treated as chargeable changes
- No clear picture of how costs will change as you grow

What better looks like

Before you sign, you know what's included, what isn't and where extra charges could arise. When your needs change, the cost implications are talked through plainly and in advance.

The question to ask

Do we understand the full cost of our service, including what happens when our needs change?

04 / 07



Reactive support

Being available isn't the same as being present.

Some providers deliver exactly what the contract specifies and very little more. Meetings are hard to arrange, answers are slow and guidance can feel like a favour. That adds work for your team and leaves you wondering what support you'd get if something were genuinely urgent.

What you might notice

- You mostly hear from them when something has gone wrong
- Requests for information take days rather than hours
- Service reviews that feel like a box-ticking exercise

What better looks like

A partner who is easy to reach and stays in regular contact, keeps up with your changing priorities and suggests improvements before issues become urgent.

The question to ask

Does our provider help us stay ahead of challenges, or do we only hear from them when something needs attention?

05 / 07

A one-size-fits-all approach

Your organisation isn't standard. Your security shouldn't be either.



A hospital, a university and a bank may face similar threats, but their environments, constraints and priorities differ enormously. Rigid processes force customers to adapt to the provider, adding complexity and work. Standard processes help keep a service consistent, but they shouldn't come at the expense of understanding how you work.

What you might notice

- Your team reshapes its own processes to suit the provider
- Recommendations that don't account for how you actually operate
- Little interest in what makes your organisation different

What better looks like

Proven processes, plus time spent learning how you operate, which systems matter most and what constraints your teams face. You shouldn't need an exception to every rule, just a service that fits the way you work.

The question to ask

Does our service reflect the way we operate, or are we constantly adapting to our provider?

06 / 07



A lack of accountability

Trust comes from follow-through.

No service is perfect. What separates a dependable provider from an ineffective one is how problems are handled. When actions stay open for months, recommendations are dropped without a word or decisions are made without you, trust soon wears thin. Unresolved weaknesses can also have consequences well beyond the relationship.

What you might notice

- Items dropping off action logs or improvement plans without agreement
- Issues explained away rather than owned
- Decisions affecting your service made without consultation

What better looks like

Issues have a named owner and you get honest updates on progress. Actions are recorded, responsibilities are agreed, changes are explained and priorities are set together.

The question to ask

When something goes wrong, does our provider take responsibility and show real progress?

07 / 07

An unwillingness to collaborate

The strongest security partnerships work together.



Security is a shared responsibility. A good provider will sometimes push back on your requests, and that kind of challenge is valuable. Resisting almost everything is a different matter. When every request meets a barrier, good outcomes become harder to reach and the relationship starts working against you.

What you might notice

- A 'no' with no explanation and no alternative
- Your team's knowledge overlooked or second-guessed
- Simple changes turned into lengthy negotiations

What better looks like

They listen, explain their recommendations, respect your expertise and stay open to alternatives. If a request carries too much risk, they tell you why and help you find a safer way to get there.

The question to ask

Does our provider make it easier for our teams to achieve their objectives securely?

What great looks like

Less uncertainty. **More confidence.**

A security service shouldn't be judged only by the absence of incidents. The experience of working with your provider matters too. A great partnership makes complex challenges easier to understand, takes pressure off your team and gives you a clear view of your risk, along with confidence in how it's being handled.

The best partnerships combine

01

Technical expertise

Skilled people and proven technology, applied to your environment.

02

Dependable processes

Commitments tracked and delivered, without you having to chase.

03

Clear communication

Reporting and advice you can understand, question and act on.

04

Genuine understanding

A partner who knows how your organisation works and what matters most to it.

The right partner leaves you better informed, better supported and **ready for what comes next.**

Self-assessment

Is your cyber security partnership **delivering?**

Use these seven questions to reflect on your current arrangements. Tick the answer that feels most honest today.

	Question	Yes	Partly	Not yet
01	**Transparency** Do we have clear visibility of our security environment, service performance and outstanding risks?	☐	☐	☐
02	**Consistency** Does our provider reliably deliver against its commitments?	☐	☐	☐
03	**Commercial clarity** Do we understand what we're paying for and where extra costs may arise?	☐	☐	☐
04	**Proactive support** Does our provider engage with us beyond incidents and contract obligations?	☐	☐	☐
05	**Flexibility** Does the service reflect our environment and operational needs?	☐	☐	☐
06	**Accountability** Are issues and recommendations clearly owned and followed through?	☐	☐	☐
07	**Collaboration** Does our provider work constructively alongside our teams?	☐	☐	☐

There's no single score.

Some gaps close with better communication and clearer expectations. Others point to deeper problems with capability, culture or fit. What matters is recognising them before they affect your security.

Choosing with confidence: **look beyond the technology.**

Capabilities, platforms, certifications and price all matter, but they rarely tell the whole story. The people, the processes and the way a provider engages with its customers are what shape the partnership.

Independent accreditation, such as CREST, offers valuable assurance about capability and operating standards. References, evidence of service performance and conversations with the people who will actually deliver the service tell you even more. When you speak to a provider, ask how they work in practice.

1. How are incidents handled?

Ask them to talk you through a recent example, from first alert to resolution.

2. How are service improvements managed?

Look for an improvement plan that you review together, regularly.

3. How is accountability maintained?

Find out who owns each action and how progress is reported back to you.

4. What happens when expectations aren't met?

Listen for honesty, a clear escalation route and a plan to put things right.

Above all, find out **how they'll work alongside you when the pressure is on.**

In the end, choosing a cyber security provider **comes down to trust.**



Why Socura?

We're here to help make the digital world a safer place and change the way organisations think about cyber security. We blend technical expertise and industry experience with a people-centric approach, working right alongside our clients to guide them along their cyber security journey.

That people-centric approach is what sets us apart, and it comes down to three core values.

Share the journey

Wherever you are on the journey, we're right there alongside you, and only ever winning when you are.

Be the light

Sharing our knowledge and insight to empower your people and light the way to a smarter, more effective security approach.

Make it count

Making every interaction count, filtering out the noise and delivering real value on the things that matter most.

Accredited and trusted

Certifications and standards

UK government

Assurance and partnerships

Want a clearer view of your current arrangements? **Let's talk.**

Tell us a little about your set-up and we'll arrange a time to talk it through.

Arrange a conversation

or email **hello@socura.co.uk**

SOCURA

When calm leads, **confidence follows.**

hello@socura.co.uk | socura.co.uk | Socura



This guide shares general guidance drawn from our experience. It isn't tailored to any specific organisation, so for advice on your own environment, please get in touch. Third-party names, logos and trademarks are the property of their respective owners.

Socura Limited · Registered in England and Wales No. 12200836 · © Socura. All rights reserved.