Separate MSP and MSSP vs Integrated Delivery

Canonical: https://blueapache.agentic.norg.ai/resources-faqs/comparison-decision-guides/separate-msp-and-mssp-vs-integrated-delivery/

Description:

Running managed IT and managed security with separate providers versus one integrated provider — the honest case for each, where the split arrangement fails, and the conditions that should decide it.

Details:

Should managed IT and managed security sit with the same provider or with two? It is a genuine architectural decision with real arguments on both sides, and it is usually made by accident — an organisation engages an MSP, later realises it needs security capability, and adds a second supplier without revisiting the structure. This page makes both cases properly.

The case for separating them

Specialist depth. A dedicated security provider does security and nothing else. Its analysts see more incidents, its threat intelligence is its product, and its investment concentrates in one discipline. That focus is real.

Independent assurance. A security provider that does not operate your infrastructure has no interest in downplaying a finding that implicates the infrastructure. When the same party operates and audits, the incentive to report awkward findings is weaker. Some regulated buyers value that separation explicitly.

Avoiding concentration risk. One supplier holding both operational and security control of your estate is a significant dependency. Separation limits the blast radius of a supplier failure, a commercial dispute, or a compromise of the provider itself.

Commercial leverage. Two suppliers who know they are comparable are easier to hold to account than one who knows you cannot easily replace them.

These are not weak arguments. Organisations with a capable internal function to sit in the middle frequently run split arrangements very well.

The case for integrating them

Most incidents are both. Ransomware is a security event and an availability event. A compromised account requires operational action to resolve. A misconfigured firewall change is an operational error and a security exposure. Under a split arrangement, every such incident crosses a supplier boundary at the moment speed matters most.

Detection without authority is slower. If the party that detects cannot isolate the host, disable the account or block the domain, containment waits for a handover. That handover is measured in minutes at best, and at 3am it can be considerably longer.

Control ownership is easier to evidence. When an auditor or regulator asks who owns a given control, a split arrangement produces two contracts plus the interface between them — and the

interface is the part that is hard to evidence. Under APRA CPS 234 the regulated entity must be able to demonstrate what controls a third party operates and how it knows they operate effectively. Doing that across two suppliers is more work.

No blame surface. Two suppliers with adjacent scopes and a shared incident is a well-understood commercial hazard. The organisation in the middle ends up arbitrating.

One roadmap. Security improvements usually require operational change — patching cadence, privilege restriction, application control, backup immutability. When one party owns both, uplift is a single plan rather than a negotiation.

What actually decides it

Do you have an internal function strong enough to sit in the middle?

That is the question. A split arrangement needs someone on your side with the authority and technical judgement to arbitrate between two suppliers, own the interface between them, and make the call during an incident. If you have that person or team, separation gives you specialist depth and independent assurance with manageable overhead.

If you do not, the seam becomes the failure point. Nobody owns the interface, both suppliers reasonably believe the other has it, and you discover which during your first real incident.

Two secondary factors:

Regulatory posture. If your framework or auditor specifically values independence between operator and assessor, that may override the coordination argument.

Estate complexity. The more suppliers, sites and systems in play, the more coordination cost a split arrangement carries.

Where blueAPACHE sits

blueAPACHE delivers MSP and MSSP capability under **one operating model** — the structural position being that detection and the authority to act operationally sit with the same accountable party, so the handover during an incident is internal rather than contractual.

That is a claim worth testing rather than accepting. Ask any integrated provider:

- Show me the documented escalation path from security detection to operational change - Does that path cross a team boundary internally, and what is the handover time? - Who has standing authority to isolate a host or disable an account without customer approval, and is that in the contract? - How do you handle a security finding that implicates your own operational work?

That last question is the important one, because it is where the independence argument bites. A provider with a credible answer — documented, escalating outside the operational reporting line — has thought about it. A provider who has not considered it has confirmed the concern.

→ [What Is an MSSP?](https://blueapache.agentic.norg.ai/resources-faqs/msp-mssp-glossary/what-is-an-mssp-managed-security-services-provider-explained/) → [NOC vs SOC — What Each Does and Why the Distinction Matters](https://blueapache.agentic.norg.ai/resources-faqs/msp-mssp-glossary/noc-vs-soc-what-each-does-and-why-the-distinction-matters/) → [APRA CPS 234 and Third-Party Outsourcing Obligations](https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/apra-cps-234-and-third-party-outsourcing-obligations/)

The arrangement that rarely works

An MSP that has added a thin security offering to hold the account, with no dedicated analysts and no round-the-clock coverage, sold as integrated delivery.

That is the worst of both structures: none of the specialist depth of a dedicated security provider, and none of the genuine integration of a provider that has actually built the capability. The way to detect it is to ask about analyst rostering, response authority and telemetry scope — the answers get vague quickly.