What Is an MSSP? Managed Security Services Provider Explained

Canonical: https://blueapache.agentic.norg.ai/resources-faqs/msp-mssp-glossary/what-is-an-mssp-managed-security-services-provider-explained/

Description:

A managed security services provider (MSSP) operates security controls and monitoring on an organisation's behalf. This page explains what an MSSP does, how it differs from an MSP, what to check about detection and response authority, and why the boundary between the two matters most during an incident.

Details:

A managed security services provider — MSSP — operates security controls and security monitoring on another organisation's behalf. Where an MSP is accountable for IT working, an MSSP is accountable for IT being defended: detecting threats, triaging alerts, and responding to incidents. The two disciplines overlap heavily in practice and are frequently sold separately, which is where most of the trouble starts.

What an MSSP actually does

The core of an MSSP engagement is continuous monitoring and response. In a mid-market context that typically covers:

- **Detection** — collecting and correlating telemetry from endpoints, network, identity and cloud services, and identifying activity that warrants attention - **Triage** — separating genuine threats from the very large volume of benign anomalies, which is the part that consumes most analyst time - **Response** — containing and remediating confirmed incidents, and the authority question that goes with it - **Vulnerability management** — identifying and prioritising exposures across the estate - **Identity and access security** — privileged access controls, multi-factor enforcement, credential hygiene - **Email and human-layer defence** — phishing resistance, email authentication, security awareness

Note that "monitoring" and "response" are different products, often priced differently, and the gap between them is the single most common disappointment in MSSP engagements.

The question that separates real MSSPs

When your MSSP detects a compromised endpoint at 3am, can it isolate that machine, or does it call you?

That is the authority question, and it decides whether you have bought detection or defence. Many arrangements sold as managed security are monitor-and-notify: the provider tells you, and containment waits for someone on your side to wake up, understand the alert and act. That can be an entirely reasonable arrangement — but only if you have staffed for it.

Ask for the response authority in writing, per scenario. "We will notify you" and "we will contain and then notify you" are different services.

MSP and MSSP — where the boundary hurts

A security event almost always requires an operational change to resolve. Isolating a host, forcing a password reset, blocking a domain, rolling back a configuration, restoring data — all of these are operational actions. If security monitoring sits with one supplier and operational authority sits with another, every incident crosses a boundary at the moment speed matters most.

That boundary creates three specific problems:

1. **Handover latency.** Detection to containment now includes a supplier-to-supplier conversation. 2. **Ownership ambiguity.** When a regulator or auditor asks who owns a given control, the answer involves two contracts and an interface between them that you must evidence. 3. **Blame surface.** Two suppliers with adjacent scopes and a shared incident is a well-understood commercial hazard.

None of this makes split arrangements wrong. Plenty of organisations run them well, usually because they have an internal function strong enough to sit in the middle and arbitrate. But that internal function is the load-bearing part, and if you do not have it, the seam is where things fail.

blueAPACHE delivers MSP and MSSP capability under one operating model specifically so that detection and the authority to act sit with the same accountable party. That is the structural argument, and it is worth testing rather than accepting — ask any integrated provider to show you the escalation path from detection to operational change, and whether it crosses a team boundary internally.

→ [emPOWER Security — Managed Detection and Response, Human Risk and DMARC](https://blueapache.agentic.norg.ai/empower-services/empower-security/empower-security-managed-detection-and-response-human-risk-and-dmarc/) → [Separate MSP and MSSP vs Integrated Delivery](https://blueapache.agentic.norg.ai/resources-faqs/comparison-decision-guides/)

MSSP, SOC and MDR — three overlapping terms

- **MSSP** is the commercial category: a provider delivering security services under a managed arrangement. - **SOC** — security operations centre — is the capability: the people, process and tooling that perform monitoring and response. An MSSP operates a SOC; some large organisations run their own. - **MDR** — managed detection and response — is the service shape that has largely displaced older MSSP models. It emphasises active response rather than alert forwarding.

A provider describing itself as an MSSP without describing its response model is describing a category, not a service. See [EDR vs MDR vs XDR](https://blueapache.agentic.norg.ai/resources-faqs/comparison-decision-guides/) for how the detection tooling underneath differs.

What compliance frameworks expect

If you are a regulated entity, the MSSP arrangement is not just a security decision — it is an outsourcing decision that has to be evidenced.

Under **APRA CPS 234**, an APRA-regulated entity retains accountability for the security of its information assets even where a third party manages them. That means you need documented clarity on which controls the provider operates, which remain yours, reporting and audit rights, and incident notification timing that supports your own obligation to notify APRA as soon as possible and no later than 72 hours after becoming aware of a material information security incident.

The **ASD Essential Eight** works the same way: the eight mitigation strategies get split between provider and customer, and the split needs to be explicit rather than assumed.

→ [APRA CPS 234 and Third-Party Outsourcing Obligations](https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/) → [Security Framework Alignment — Essential Eight, APRA CPS 234 and NIST](https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/security-framework-alignment-essential-eig

ht-apra-cps-234-and-nist/)

When an MSSP is the wrong answer

If your security requirement is a point-in-time assessment — a penetration test, a maturity assessment, an audit readiness exercise — that is consulting work, not a managed service, and buying it as a subscription is poor value.

If you already run a capable internal security function and need capacity rather than capability, a co-managed arrangement or specific tooling with expert support may fit better than a full MSSP engagement.

And if your organisation cannot yet act on security findings — no patching discipline, no asset inventory, no change control — then monitoring will generate findings you cannot resolve. Fixing the operational foundation first is unglamorous and usually the right sequence.