AGILEBLUE

THE AI POWERED SECOPS PLATFORM

Configuration & Success Blueprint

Executive Summary · What full protection looks like, and how to get there

The difference between monitored and protected

Being monitored isn't the same as being protected. How much you get out of AgileBlue depends on how completely your systems are set up – what we can see, how we respond, and who does what when something happens. The full Configuration & Success Blueprint covers all of that across eight areas. This summary is the short version: what a complete setup looks like, and why each part matters to you.

8	80	29
KEY AREAS	SETUP ITEMS	MUST-HAVES

Why a complete setup matters

- **We can only protect what we can see –** Every device and account left out is a place a problem can go unnoticed. A complete setup brings all of it into view.
- **Seeing a threat isn't enough –** We agree in advance how threats are handled, so confirmed problems get stopped, not just reported to you.
- **Real alerts, not constant noise –** We fine-tune alerts from the start, so your team hears about the things that matter instead of a stream of false alarms.
- **Microsoft 365 gets extra attention –** It's where most attacks start, so we connect it fully and review its security on a regular schedule.

The eight areas we cover

#	AREA	WHAT IT MEANS FOR YOU	MUST-HAVES
1	**Client Scope & Environment**	We map out everything you run – devices, users, cloud, and tools – so monitoring starts with the full picture.	**4** / 15
2	**Integrations & Log Sources**	We connect your key systems so their activity flows to us. Anything left out is something we can't see.	**3** / 12
3	**Agent Deployment**	Our software on your devices lets us spot threats and actually stop them, not just watch.	**1** / 5
4	**Response Actions**	We agree up front how threats get handled, so confirmed problems are stopped quickly instead of waiting on a decision.	**1** / 6

#	AREA	WHAT IT MEANS FOR YOU	MUST-HAVES
5	**Tuning & Exceptions**	We fine-tune alerts from day one, so your team hears about real issues, not a flood of false alarms.	**1** / 7
6	**M365 Security**	Microsoft 365 is where most attacks begin, so we connect it fully and check its settings on a regular schedule.	**4** / 12
7	**Communication Expectations**	We set clear contacts and roles in advance, so no time is lost when something happens.	**7** / 12
8	**Escalation Playbooks**	Everyone knows who does what the moment a threat is confirmed.	**8** / 11

The Must-Haves column shows how many items in each area are essential for full protection. The rest are strongly recommended for every customer – the steps that take you from monitored to fully protected.

How we work through it together

- **Getting started –** We walk through each area with you to see what's already in place and what's missing.
- **During setup –** We work through the list together as a plan, making sure every must-have is in place before monitoring begins.
- **Over time –** We review it with you at each quarterly check-in to keep your protection current as things change.

AI-Native Protection. Human Support. Real Peace of Mind.

AgileBlue pairs smart automation that catches and contains threats quickly with a real team of experts watching around the clock. A complete setup is what lets both do their best work for you.

Next step: Ask your AgileBlue team to walk through the full Blueprint with you and confirm the must-haves for your environment.