Why use Bluedog's M365 Monitoring Service on top of the Microsoft 365 Licence?

We are often asked why an organisation would use Bluedog's M365 Service on top of the subscription they pay to Microsoft, especially the additional Advanced Threat Protection (ATP) licence.

So, let's look at a comparison with MS Licence:

The main difference is that the bluedog service is a Managed Service. This means that we are constantly monitoring your M365 tenancy, 24 hours a day, 7 days a week, 365 days per year on your behalf. We have physical eyes on screens. If something unusual happens – regardless of the time, day or night - on your M365 tenancy our skilled SOC staff are straight on the case.

Because we use advanced AI, ML and – unlike ATP - human intervention, we don't create hundreds of 'false positive' alerts that waste your time, create lots of "noise" and mask the really important alerts; we are able to filter down to just the most important ones.

Of course, Microsoft provides some excellent dashboards and information, but it's a DIY solution, this means you are responsible for checking and monitoring your tenancy. It means that for you to provide the same level of care and oversight, you'd have to employ many skilled staff members just to monitor your tenancy 24/7/365.

Let's look at just one of many case studies from one of our resellers which is a perfect example:

Steve - [redacted] Systems

It was not possible to have security activity monitoring on remote locations for users. Being able to provide information on compromised accounts instantly is important. **Without bluedog services this would not be possible to achieve.**

> Hi Tim & Team,
>
> I'm just having a bit of a panic attack at the minute, as I'm trying to work out what's going on as we've got a bit of a situation coming up, that BlueDog keeps notifying us of...
>
> So, yesterday we got a BlueDog notification of an unusual login location for one of our customers ([redacted] Co). The IP address was [redacted] and showing as being located in Toronto, CA. The customer definitely isn't there - they are in [redacted] It shows as a successful login, and confirmed this in Azure Audit Logs too. That said, nothing else seems to have happened with it, beyond just login, so have put it down to a scammer managing to try the account, but then have left it with the intention of coming back at a later date - which we wouldn't have known about if it wasn't for BlueDog.

This is the kind of insight that our M365 Monitoring customers are given, and note as this customer states... Without Bluedog the customer would not have known that there had been a rogue login!