

¿Por qué usar el servicio de monitoreo **Bluedog M365 Monitoring Service** además de “Microsoft 365 Licence”?

A menudo nos preguntan por qué una organización utilizaría el Servicio M365 de Bluedog además de la suscripción que pagan a Microsoft, especialmente la licencia adicional de Protección Avanzada contra Amenazas (ATP).

Así que, miremos una comparación con “MS Licence”:

La principal diferencia es que el servicio de bluedog es un servicio gestionado. Esto significa que estamos siempre monitoreando su tenencia de M365, 24 horas al día, 7 días a la semana, 365 días al año en su nombre. Tenemos ojos físicos en las pantallas. Si ocurre algo inusual -independientemente de la hora del día o la noche- en su tenencia de M365, nuestro personal SOC cualificado está inmediatamente en el caso.

Como utilizamos IA avanzada, ML y, a diferencia de ATP, intervención humana, no creamos cientos de alertas de “falsos positivos” que le hagan perder el tiempo, creen mucho “ruido” y oculten las alertas realmente importantes; somos capaces de filtrar sólo las más importantes.

Por supuesto, Microsoft proporciona algunos paneles e información excelentes, pero es una solución que tiene que resolverse a sí mismo, lo que significa que estas responsable de comprobar y supervisar su arrendamiento. Esto significa que para proporcionar el mismo nivel de atención y supervisión, tendría que emplear a muchos miembros del personal cualificado sólo para supervisar su tenencia 24/7/365.




Veamos uno de tantos estudios de caso de uno de nuestros distribuidores que es un ejemplo perfecto:

Steve - Systems

No era posible monitorear la actividad de seguridad en ubicaciones remotas para los usuarios. Ser capaz de proporcionar información sobre las cuentas comprometidas al instante es importante. **Sin los servicios de bluedog esto no sería posible de lograr.**

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  (Co). The IP address was  and showing as being located in Toronto, CA. The customer definitely isn't there - they are in . 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.

Este es el tipo de perspectiva que nuestros clientes de monitoreo “Bluedog M365 Monitoring Service” obtienen. Tome nota de la observación de unos de nuestros clientes: ¡Sin Bluedog el cliente no habría sabido que había habido un inicio de sesión fraudulento!