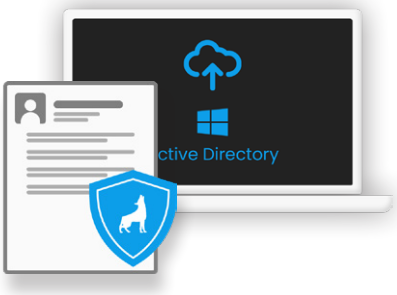
MICROSOFT® AZURE SECURITY MONITORING

Protect your cloud with bluedog Azure Monitoring

The world has changed, your staff and your data are more vulnerable now. You need to protect your information and data not just within your office network but in the cloud too.

Having your data in the cloud has many benefits, but attackers can also abuse this ease of access. User credentials are being leaked and stolen every day, with attackers abusing these stolen credentials and trying to log into your organization's cloud remotely.

Bluedog's Azure Security Monitoring can protect your staff and information wherever they are; we can protect your company's extended network.



If you're one of the millions of businesses using Microsoft® Azure you need to think seriously about security monitoring for your Azure tenancy.

Your staff working remotely or from home are vulnerable. You can't monitor their network when they are working away from the office.

It's relatively easy for cyber criminals to gain access to your Azure tenancy in the same - and often an easier way - than they can gain access to your office network.

Because Azure is cloud based, it's more difficult for you to even know there's been a breach!

You need a way of ensuring the safety of your information even for employees working from home or remotely.

If you are using Azure within your organization and are looking to secure your environment, then look no further.

Bluedog can take in all Azure events, as well as the Azure Security Center with a few clicks. There might be suspicious account login attempts from outside the office, data exfiltration from SharePoint or phishing emails arrive in your employee's email.

Bluedog provides Enterprise Grade security for your Azure tenancy at an entry level price

- Protect Azure users regardless of location
- Your data will be secured even for remote or home workers
- Your remote users will be protected in the same way as those working within your office network

How does it work?

- Our software constantly monitors your Azure tenancy
- Anomalies are immediately reported to you and our 24/7/365 Security Operations Centre
- Our Security Experts have constant eyes on the screens
- You also get access to the Monitoring Dashboards
- In real time you can see who's doing what, when and where
- We recommend what changes are needed to make your tenancy more secure
- You can also feed in logs from almost infinite external sources into Azure Log Analytics to be monitored by our platform.

What makes bluedog's Azure Monitoring so different?

Every potentially serious alert from the monitoring system is not only alerted to the end user customer, but also fed through to our highly skilled SOC team, who investigate the alerts; making the kind of correlations with other recent events that only humans can do.

When bluedog sees your Azure usage, the data scientists inside the bluedog Security Operations Centre (SOC) correlate user behavior to identify abnormal behavior. This is the kind of information that truly identifies attackers are inside an organization.

When a cloud account is breached, anti-virus solutions or internal solutions like firewalls won't be triggered. The bluedog SOC can spot an attacker as they navigate their way across the network. An unusual login location or lateral movement across the network to find and exfiltrate files is what stands out.

What do we see?

- Successful Logins from unusual locations – quickly cut off potential external attacks
- Failed and attempted logins – is someone trying to gain access to your Azure tenancy?
- Account creations – attackers may be moving sideways through your system by creating new accounts
- File accesses and exfiltration – we can alert unusual file downloads or large amounts of data being saved to other cloud services
- Account Operations – Are passwords being changed, accounts deleted, accounts created, permissions changed?
- Application Installations - If a user authorises the installation of a new application within your Azure tenancy you can quickly prevent rogue applications doing damage.

What don't we see?

We don't see file contents!

Why is Bluedog the best solution for Azure Security?

- The only security solution for Microsoft Azure backed by a fully staffed 24/7 SOC
- Works for any level of Azure subscription!
- Low monthly subscription - Affordable by any business size
- No setup fees
- No minimum number of users
- Fast setup in about 10 minutes
- 30 Days no commitment Proof of Concept Trial
- Fair billing based on events per second – not number of users

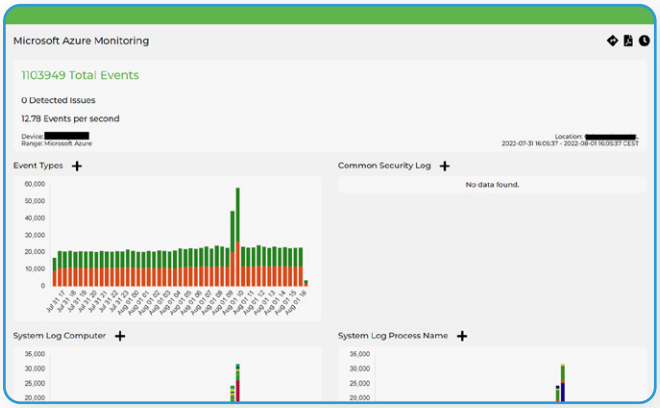


Image Content is just a sample of our dashboard process.

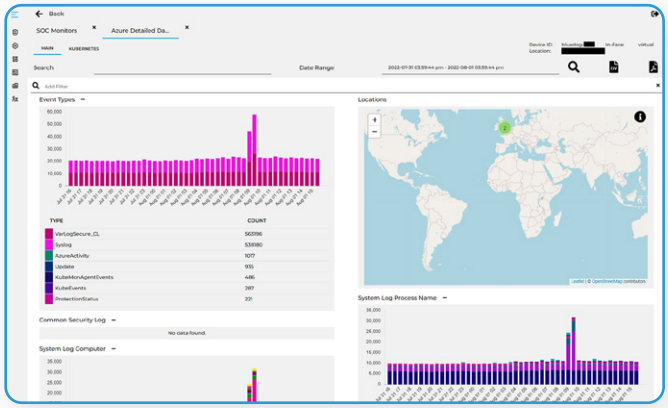


Image Content is just a sample of our dashboard process.

Image Content is just a sample of our dashboard process.

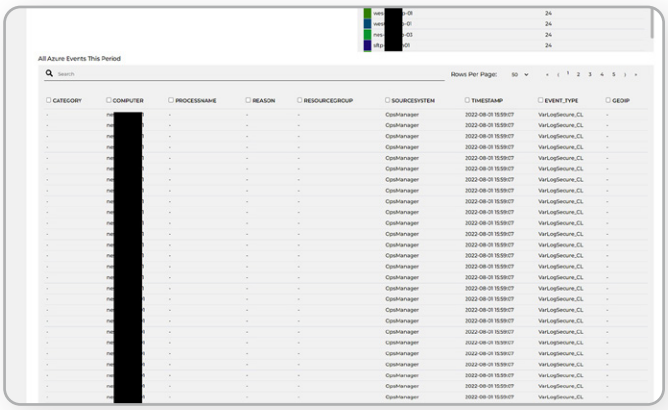


Image Content is just a sample of our dashboard process.

To find out more about our Microsoft® Azure Monitoring Service and our other solutions, email us at sales@bluedogsec.com or visit **bluedog-security.com**.

ISO 27001 CERTIFIED

bluedog SECURITY MONITORING