AGILEBLUE

Cloud Detection and Response

Detect, Investigate, and Respond to Cloud Threats 24/7

Cloud environments change constantly as new users, permissions, services, and workloads expand the attack surface. AgileBlue continuously monitors activity across AWS, Microsoft Azure, and Google Cloud to detect suspicious behavior, investigate potential threats, and take the appropriate response based on your environment.

What AgileBlue Detects

Unauthorized Access

Identify unusual logins, compromised credentials, and suspicious attempts to access cloud systems and data.

Privilege Escalation

Detect unexpected permission changes and respond when an attacker attempts to gain greater control of cloud resources.

Suspicious User Behavior

Surface anomalous activity involving cloud users, admins, identities, and service accounts and contain activity that presents a validated risk.

Lateral Movement

Recognize and disrupt behavior that may indicate an attacker is moving between cloud resources, accounts, or connected environments.

From Cloud Activity to Actionable Detection

Collect
Continuously ingest cloud activity and security data

Detect
Identify suspicious behavior and potential threats

Investigate
Add environmental and cross-source context

Respond
Take action according to your predefined response protocols

The AgileBlue Difference

AI-Driven Investigation
Quickly separate meaningful cloud threats from noise.

Multi-Cloud Visibility
Monitor threats across AWS, Microsoft Azure, and Google Cloud.

Cross-Environment Context
Connect cloud activity with identity, endpoint, network, and other signals.

Stop Cloud Threats Before They Spread

Detect suspicious activity, understand its impact, and take action before it becomes a larger incident.

Talk With an Expert →

© 2026 AgileBlue. All rights reserved.