What Is Cloud Security Monitoring?

[Cloud security monitoring](https://www.blumira.com/product/cloud-security/) is the practice of continuously supervising both virtual and physical servers to analyze data for threats and vulnerabilities. Cloud security monitoring solutions often rely on automation to measure and assess behaviors related to data, applications and infrastructure.

How Does Cloud Security Monitoring Work?

Cloud security monitoring solutions can be built natively into the cloud server hosting infrastructure (like AWS’s CloudWatch, for example) or they can be third-party solutions that are added to an existing environment (like Blumira). Organizations can also perform cloud monitoring on premises using existing security management tools.

[Like a SIEM](https://www.blumira.com/glossary/what-is-siem/), cloud security monitoring works by collecting log data across servers. Advanced cloud monitoring solutions analyze and correlate gathered data for anomalous activity, then send alerts and enable incident response. A cloud security monitoring service will typically offer:

*SIEM : security information and event management*

**Visibility.** Moving to the cloud inherently lowers an organization’s visibility across their infrastructure, so cloud monitoring security tools should bring a single pane of glass to monitor application, user and file behavior to identify potential attacks.

**Scalability.** Cloud security monitoring tools should be able to monitor large amounts of data across a variety of distributed locations.

**Auditing.** It’s a challenge for organizations to manage and meet compliance requirements, so cloud security monitoring tools should provide robust auditing and monitoring capabilities.

**Continuous monitoring.** Advanced cloud security monitoring solutions should continuously monitor behavior in real time to quickly identify malicious activity and prevent an attack.

**Integration.** To maximize visibility, a cloud monitoring solution [should ideally integrate](https://www.blumira.com/integrations/) with an organization’s existing services, such as productivity suites (i.e. Microsoft 365 and [G Suite](https://www.blumira.com/integration/google-gsuite/)), endpoint security solutions (i.e. [Crowdstrike](https://www.blumira.com/integration/crowdstrike-falcon/) and [VMware Carbon Black](https://www.blumira.com/integration/carbon-black-endpoint-protection/)) and identity and authentication services (i.e. [Duo](https://www.blumira.com/integration/cisco-duo-security/) and [Okta](https://www.blumira.com/integration/okta/)).