Blumira

DATA SHEET

AWS Security Monitoring

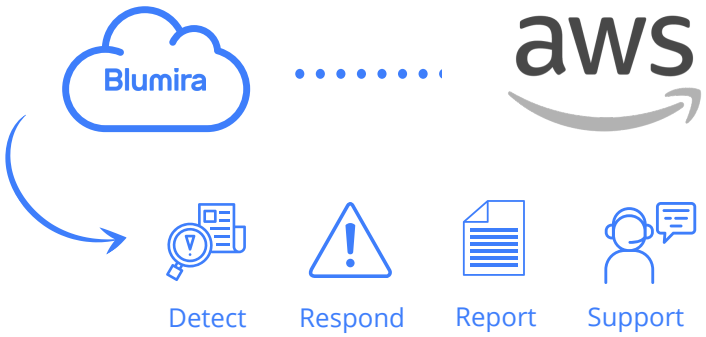
With Blumira's AWS Security Monitoring & Response solution, you can quickly detect and respond to cloud security threats across your AWS environment.

Blumira monitors logs from GuardDuty, VPC Flow Logs and CloudTrail, surfacing prioritized alerts of attacker activity and providing playbooks to guide you through remediation.

Protect Your AWS Cloud Infrastructure

Blumira's comprehensive AWS monitoring solution provides:

- **Easy-to-deploy cloud SIEM**: A scalable SIEM that connects to AWS cloud infrastructure, collects and centralizes logs in a matter of hours.
- **Broad coverage across AWS data sources**: Analyze billions of logs from GuardDuty, VPC Flow Logs and CloudTrail
- **Prioritized alerts to reduce noise**: Blumira surfaces only clear indicators of attacks to reduce false-positives with automatic log parsing, context-rich alerts, and correlated threat analyses.
- **Security playbooks for easy response**: With automated blocklists and playbooks, IT teams are guided through next steps to contain threats.
- **Honeypots to detect attackers**: Easy-to-use honeypots detect an attacker's lateral movement to alert you to cloud threats.
- **Automated, scheduled security reports**: Get automated, scheduled security reports for deeper investigation into the source of a threat.
- **Premium support from trusted security advisors**: Need more help? Get access to our security experts whenever you need advice.



Deploy in Hours; Detect & Respond Faster

- **5x faster** deployment than average SIEM
- Pre-tuned alerts & playbooks
- Integrate with data sources:
  - — GuardDuty
  - — CloudTrail
  - — VPC Flow Logs
  - — CloudWatch

Quick glance at Blumira's AWS Security Monitoring:

- Built-in integrations with AWS GuardDuty, VPC Log Flow and CloudTrail
- Simplified log collection, threat detection & response playbooks for remediation
- Scheduled, automated & customizable reports of security threats
- Access to Blumira's security experts for additional security advice

"We were able to get Blumira up and running in a matter of hours with immediate access to security expertise and actionable insights."

– Brian S., Director IT Security & Operations, Mid-Market

Start a Free Trial!
blumira.com/trial

Blumira

DATA SHEET

aws partner network

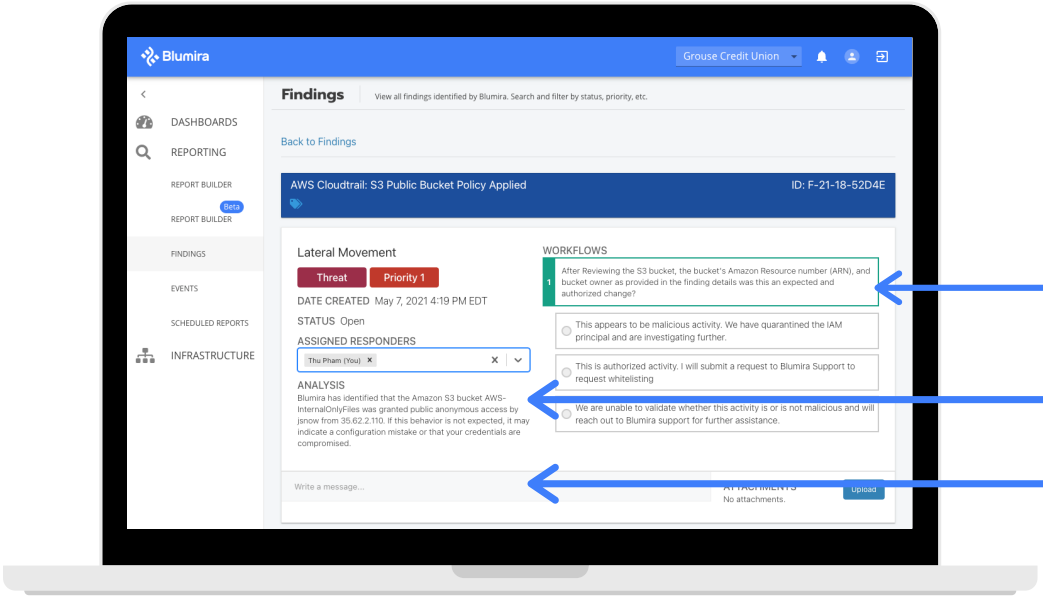
Reviewed

Detect Attacks in Progress & Respond to Limit Impact

Blumira's AWS Security Monitoring & Response solution sends you only high-confidence alerts to reduce the noise and enable your team to focus on what's important. Our platform detects:

- **S3 Bucket Misconfigurations** - Changes to policies that could result in data exposure, like a user granting an S3 bucket public anonymous access
- **Critical Anomalous IAM Behavior** - Unusual identity and access management (IAM) activity that indicates your credentials may be compromised, including malicious API usage
- **CloudTrail Root Account Logins** - Root logins and user activity that could indicate an AWS account compromise
- **GuardDuty Network Anomalies** - Unusual EC2 activity, such as brute-force attacks, port scans, unusually large amounts of network traffic, and more

Easily Respond With Contextual Alerts & Security Playbooks



Playbooks walk you through response

Contextual threat analysis with relevant data

Contact our security experts for advice

Blumira is an Official AWS Independent Software Vendor Partner

- Solution has been reviewed to meet highest industry standards
- Ensures Blumira meets AWS standards for security, reliability & operational excellence
- Listed in the AWS Marketplace & APN Solution Finder

"Other tools are noisy; we don't have time to dig through layers and layers of data. Blumira does a good job summarizing detections and giving us advice on how to remediate."

- Steve Gatton, VP of IT, Fechheimer

Start a Free Trial!
blumira.com/trial