Blumira

DATA SHEET

Cloud Security Monitoring

Cloud-first organizations can easily monitor cloud applications for unusual behavior and respond quickly with actionable data surfaced by Blumira's cloud SIEM.

Detect & Respond Quickly to Cloud Threats

Blumira provides comprehensive visibility, response and reports of your cloud environment. Blumira's cloud security monitoring solution provides:

- **Easy-to-deploy cloud SIEM**: A scalable cloud-delivered SIEM that connects to existing cloud technology, collects and centralizes logs in a matter of hours.
- **Broad coverage for a cloud environment**: Natively integrate to protect cloud infrastructure, identity providers, endpoint security and other cloud services.
- **Prioritized alerts to reduce noise**: Blumira surfaces only clear indicators of attacks to reduce false-positives with automatic log parsing, prioritized alerts, context-rich data, and correlated threat analysis.
- **Security playbooks for easy response**: Blumira helps small teams respond quickly with automated blocklists and playbooks that guide IT teams through next steps to contain threats.
- **Honeypots to detect attackers**: With easy-to-use honeypot software, you can detect an attacker's lateral movement and automatically contain cloud threats.
- **Automated, scheduled security reports**: Customize dates, run preset reports and easily export them for auditors and executives.

Centralized Data Collection, Analysis & Response

- **5x faster** deployment than average SIEM
- Pre-tuned alerts & playbooks
- Set up in hours, detect right away
- Blumira integrates with:
  - — AWS
  - — Azure
  - — G Suite
  - — Office 365
  - — Duo Security
  - — Okta

Quick glance at Blumira's cloud security monitoring:

- Built-in integrations across hybrid cloud infrastructure, applications and services
- 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

Start a Free Trial!
blumira.com/trial

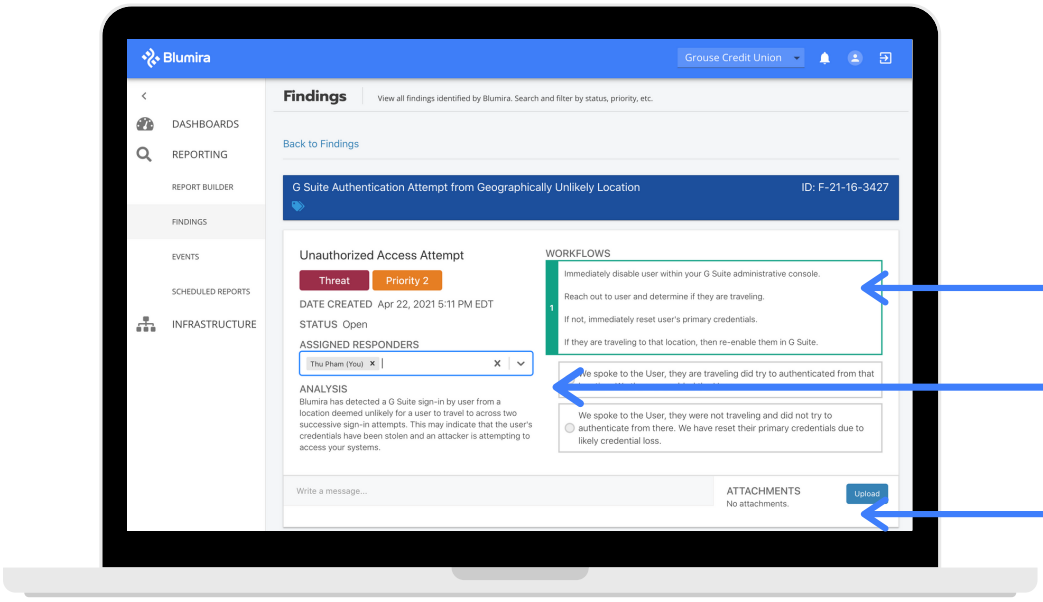
Blumira

DATA SHEET

Blumira Detects & Enables Response to Cloud Threats

Blumira's cloud-based security leverages threat intelligence and behavioral analytics to detect patterns of attacker, alerting you to high priority threats such as:

- **Cloud infrastructure threats** - Common misconfigurations, modified security groups, worms or malware indicating a compromised EC2 instance, attempts to connect with C2 (attacker-controlled) servers
- **Identity-based attacks** - Attempts to log in to your systems, including geo-impossible logins and fraudulent login attempts that could indicate the theft of usernames and passwords
- **Email & document risks** - Anomalous access attempts, external document sharing, email forwarding and new inbox rules created by attackers
- **Endpoint security threats** - Malware, unknown or blocklisted applications, malicious executables, and compromised processes running on devices within your network



Playbooks walk you through response

Contextual threat analysis with relevant data

Contact our security experts for 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

"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