Partner Battlecard

Blumira
Threat Detection & Response

Quick Facts

- HQ in Ann Arbor, MI
- Founded in 2018
- Proprietary Cloud SIEM
- MSRP: $16 per user, per month
- 1-Year Log Retention Included
- 24/7 SecOps Support for Urgent Issues

Value of Blumira: Talking Points

Industry Trend/Drivers
Log retention, auditing, and log monitoring and detection requirements are becoming a ubiquitous standard across all industries and company sizes.

The Challenge
Finding an affordable solution can be challenging -- most are too expensive and too complex to manage without specialized expertise and provide little support or meaningful threat detection.

Blumira's mission is to make good security simple and affordable to help understaffed organizations that have been neglected, priced-out, or, simply-failed-by existing solutions.

How It Works

- Blumira collects logs across your various systems and applications - Windows, Linux, Mac, firewalls, user authentication, security, and cloud applications like Microsoft 365, Azure, Umbrella, Duo, etc
- Using this data, Blumira's team has the necessary visibility to detect attackers based on their tactics, tools, and behaviors
- The platform surfaces findings based on behavioral activity, resulting in higher efficacy and less noise than signature-based detections
- In addition to the platform, customers have access to a 24/7 security operations team for support with urgent security issues
- With Blumira, you can affordably satisfy compliance requirements and stop attacks like ransomware earlier in the attack chain before they become a widespread breach

Buy Blumira because you're required to have it. Keep Blumira because it helps you sleep at night.

Objection	Rebuttal
SIEMs are too expensive	We couldn't agree more; the exorbitant cost of SIEMs is the reason why Blumira was created in the first place. Blumira's cloud-based platform is designed to automate the work of a tier 1 SOC analyst, drastically reducing deployment and maintenance costs. Blumira makes advanced security easy for IT admins, with a predictable and affordable pricing model.
I don't have any security staff to run the tool	Blumira is designed with the busy IT admin in mind, so you'll realize value from the platform with your existing team. Blumira's team handles the heavy-lifting - like parsing, configuration, writing detections, and rule deployment and tuning - so all you need to do is follow our docs to set up log collection. Then, when you receive a security finding, just follow the step-by-step instructions and know that Blumira's 24/7 support has your back whenever needed.

Blumira

Objection	Rebuttal
I already pay for security tools that "stop everything"	When a vendor says, 'This tool is the last thing you'll ever need,' you want to believe them. Unfortunately, one look at the news can dispel this mistruth. Security experts recommend SIEM tools for a reason. Unless you already have a SIEM that is easy to use, ingests data from all other tools and applications, retains it for one year, and provides detection and enables quick remediation, you can benefit from Blumira.
My Customers won't buy a tool like this	Cyber insurance will soon require one-year log retention, auditing, and detection as mandatory requirements. It is also required by HIPAA, NIST, PCI, CMMC and other compliance regulations. Similar to MFA and EDR, SIEM tools will soon be a mandatory baseline cost of doing business.

Blumira vs The Competition

Traditional SIEMs are expensive, difficult to deploy and maintain. In comparison, Blumira is made easy for IT people:

Value	Blumira	Other Vendors
Best ROI	• Predictable, per-user pricing • Little maintenance required • 24/7 urgent issue support • 1 year log retention	• Priced per data volume • Hidden fees add up • Unpredictable to budget for • Takes too much time to maintain
Faster Time to Security	• Cloud setup in minutes • Use existing team • Pre-tuned rules and integrations, ready out of the box	• Can take weeks to months • Requires add'l professional services • Costs extra or requires dev to write rules & parsers
Ease of Management	• Actionable findings, tuned for noise • Step-by-step response • Proactive threat hunting • Integrated threat intelligence • New rules automatically rolled out to platform	• Too many noisy alerts, lack of context • No incident-response help • Requires custom development to write new rules
Security Support	• 24/7 security operations team for urgent issues • Guide you thru incident response procedures • Ongoing consultations to improve security maturity	• Support is add-on • Not responsive, can take days • Outsourced support is often stretched too thin
Broad Coverage	• Windows, Mac, Linux • Azure, M365, AWS, GSuite • Collects logs from endpoint, firewalls, security, cloud, on-prem	• Limited integrations • May cost extra for additional ingestion