Partner Battlecard

Blumira
Threat Detection & Response

Quick Facts

- HQ in Ann Arbor, MI
- Founded in 2018
- SIEM & XDR
- MSRP: $21 per employee, per month
- 1-year log retention included
- 24/7 concierge support for critical 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, remote endpoints, 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. Blumira automates response by immediately containing endpoint threats.
- In addition to the platform, customers have access to a 24/7 concierge 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

Objection	Rebuttal
SIEMs are too expensive	We couldn't agree more; the high 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 security analysts, 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 for the busy IT admin, providing time to value faster with your existing team. Blumira's team handles the heavy-lifting - like parsing, creating integrations, detection management. Use our docs to set up log collection. Then, when you receive a security finding, follow the step-by-step instructions to respond and reach out to Blumira's 24/7 support for additional help.

Blumira

Objection	Rebuttal
I already pay for security tools that "stop everything"	A single tool will never stop all attacks - layering security provides greater protection. SIEMs are the foundation of a security program. Unless you already have a SIEM that is easy to use, ingests data from all other systems, retains it for one year, provides faster detection and response, you can benefit from Blumira.
My Customers won't buy a tool like this	Many cyber insurers require one-year log retention, auditing, and detection. It is also required by HIPAA, NIST, PCI, CMMC and other compliance regulations. Similar to MFA and EDR, SIEMs are becoming a mandatory baseline cost of doing business.

Blumira vs. the Competition

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

Value	Blumira	Other Vendors
Best ROI	• Predictable, per-employee 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 & automated 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 or automated remediation • Requires custom development to write new rules
Best Security Support	• 24/7 concierge team for urgent issues • Avg. response time 18 minutes • 99.7% CSAT (customer satisfaction) score • Ongoing consultations to improve security maturity	• Support is add-on • Not responsive, can take days • Outsourced or junior support is often stretched too thin & lacks expertise
Broad Coverage	• Windows, remote endpoints, Linux • Azure, M365, AWS, Google Workspace • Collects logs from endpoint, firewalls, security, cloud, on-prem	• Limited integrations • May cost extra for additional ingestion • No endpoint visibility