Blumira

Blumira Value

Blumira makes detection and response easy and effective for small and medium-sized businesses (SMBs) so they can respond to threats faster to prevent ransomware and data breaches.

Faster Time to Security, Automate Tasks For you

IT admins can easily deploy Blumira's platform in minutes to hours, rather than months compared to other SIEMs, for broad on-prem & cloud coverage with unlimited third-party integrations.

Our unique approach to detections notifies you of threats other security tools may miss, sending you real-time alerts in under a minute of initial detection to help you respond to threats faster than ever.

We do all the heavy lifting for your team to save them time, including parsing, creating native third-party integrations, and testing and tuning detection rules to reduce noisy alerts.

Mapped to Product Demo:

- Easy sign up; fast setup with Cloud Connectors for key cloud apps (M365, AWS, SentinelOne, Duo)
- Sensor setup for on-prem integrations
- Automatically apply detection rules
- Deploy in minutes vs. months compared to competitors

Easily Meet Compliance

With a year of data retention and deployment that takes minutes to hours, we help you meet cyber insurance and compliance easily and quickly with the team you have today.

Reduce risk, consolidate solutions, and satisfy compliance requirements for logging, retention, detection and response.

Mapped to Product Demo:

- Show reporting and ability to search logs
- Show popular reports historical view over time
- PCI DSS requires automated log review; Blumira's SIEM automatically deploys rules and analyzes logs for findings

Reduce Noice, Focus on Real Threats

A Director of IT can prioritize their team's time with Blumira's detections, fine-tuned to reduce noisy alerts. Blumira sends you findings based on real attacker's behaviors so you don't waste your time on false positives.

Mapped to Product Demo:

- On the summary dashboard, you can see a list of active rules applied (tested, tuned for noise by our engineers)
- See an example finding based on real attack behaviors
- Notification settings - set how you want to be notified to best fit your team's needs.
- Reduce noise with Blumira's Detection Rule Management that allows you to toggle rules on and off (paid editions only).

Automated Threat Response

Enable your team to do more, around the clock, without hiring additional security staff. Blumira automatically detects threats, sends you playbooks on how to respond, and takes automated action to contain threats by:

- **Isolating endpoints** - Detect endpoint-related threats, then immediately cut off an endpoint's access to your network to stop attacks in progress. Requires Blumira Agent.
- **Blocking malicious traffic** - Detect known malicious sources of traffic, then immediately block their access to your environment. Requires on-prem sensor and firewall integration.
- **Disable compromised users** - Detect suspicious users, then take action by disabling users & revoking their sessions. Requires Microsoft 365 Cloud Connector and threat response configuration.

Mapped to Product Demo:

- Show example finding and walk through the workflow to close it out
- Blumira's **dynamic blocklists** enables you to automatically block IP addresses and domains found in threat intelligence feeds, no human intervention required. Requires firewall integration (paid editions only).
- In example finding, point out where you can message Blumira's SecOps team directly, in-app (paid editions only)