BATTLECARD

Blumira

Threat Detection & Response

Blumira Value

With so many different products, services and security acronyms out on the market today, it's hard to know what's worth investing in for the greatest return in security value. We break it down for you below:

Industry Challenges

- SMB/MSPs are increasingly targeted by attacks - but priced out by most security solutions, resulting in the lack of visibility across their environment
- Other IT/security tools generate too much data and noise, making it hard to know what’s critical to focus on
- Staffing security talent is too expensive, and SMBs/MSPs typically don’t have dedicated security practitioners – without security expertise, traditional security tools don’t actually reduce risk
- Relying on humans alone (24/7 in-house SOC or SOC as a service) does not scale/can result in errors – these options are often too expensive to adopt

Blumira Solution

Blumira’s advanced security platform is designed to be simple, affordable and accessible to organizations of all sizes, built for ease of use by IT admins.

We take care of all the heavy lifting for you, automating typically manual tasks.

- **Deployment**: takes just minutes, no additional infrastructure or personnel required
- **Log collection:** parses diff data types automatically, collecting data from different sources for correlation, threat analysis and historical investigation (often required by compliance)
- **Detections**: written, tested & tuned by Blumira’s detection engineers – updated every 2 wks. Using behavior-based detection (not just signature), we alert on a higher confidence of real threats to detect issues your EDR/MDR cannot catch alone
- **Response**: instructions on how to respond to threats come pre-built with every finding, with our SecOps team providing 24/7 support for urgent priority issues, acting as an extension of your own team
- **Reports**: gain insights from your data and see security trends over time with pre-built and scheduled reports
- **Help meet compliance**: 1 year of log retention, monitoring, audit log trails, detection and response help you easily meet many industry compliance regulations

With Blumira, you can stop attacks like ransomware earlier before it becomes a widespread breach – we focus on reducing your risks and increasing your security maturity over time.

Other Products

Managed Detection & Response (MDR)

- 24/7 or 9x5 monitoring by SecOps staff
- Review, investigate, triage and send alerts to customer
- May offer limited response
- If agent-based, can stop things immediately for remediation
- Cannot add local context of your organization
- Don't have IT admin access to everything for full remediation
- Limited/no visibility outside of their agent
- Limited data retention; may or may not satisfy EDR requirement

Managed Services or MSSP

- Sells you a set of security tools
- If agent-based - can carry out actions on an affected device to contain threats
- Cannot add local context; likely don't have IT admin access for full remediation (no silver bullet)
- Limited data retention; may or may not satisfy compliance objectives

Blumira

- Platform automates manual monitoring, fine-tuned for you to reduce false positives and analyst fatigue
- 24/7 detection & guided response coverage sends alerts directly to your team, no delay in notification
- MDRs can slow down that process and you may not receive alerts until hours or days later
- **There is no one product that can fully take care of all security response** - many actions require local context to carry out
- Blumira gives you analysis and next steps written with IT admins in mind to carry out actions yourself in our playbooks that come with every finding
- Blumira sends you alerts faster, with full context to help with investigation and remediation
- The Blumira SecOps team engages with you on any finding to help further investigate when needed

Other Products

Traditional SIEMs

- Takes weeks to months to set up - requires team of security analysts to deploy and maintain
- Complex and not user-friendly
- Search queries require knowing certain languages/security experience
- Requires writing and fine-tuning detections, log parsing, correlating data to get any value out of it

Blumira

- Cloud Connectors makes setup easy in minutes for cloud apps
- Simple for small IT teams to set up without additional resources
- Platform comes with ongoing, fine-tuned detection rules, parsed logs and correlated data - all heavy lifting is done by Blumira
- No agents required to gather data for cloud services

Other Products

Traditional SIEMs, Continued

- May require sensors or agents
- Remediation still requires coordination with IT team
- Cold storage can result in slow queries, taking several minutes to run simple reports
- Priced by data ingestion volume; resulting in unpredictable cost
- Additional cost for 1 year of data retention and 24/7 support

Blumira

- All data is stored in hot storage, resulting in speedy queries
- Unlimited data ingestion
- 1 year data retention standard, ideal for compliance

Other Products

SOAR

- Security orchestration, automation and response provides automated response actions thru other tools
- Usually only valuable if you already have a mature SIEM deployment in place

Blumira

- Blumira's dynamic blocklists enables you to automatically block known malicious IP addresses
- Available through easy-to-setup firewall integrations that support dynamic blocklisting

Other Products

EDR

- Typically limited to signature-based detections for endpoints
- Gathers additional data, but requires security expertise to write detections or make use of the data in investigations
- Without qualified security professionals EDR becomes an expensive and noisy NGAV (nxt-gen antivirus)
- Limited ability to correlate endpoint data to other telemetry sources (on users, network traffic, etc.)
- Satisfies many compliance requirements

Blumira

- Expands beyond signature-based detections to behavior-based, providing higher confidence level of a real threat detected
- Blumira's incident detection engineering team writes, tunes and maintains detections every two weeks
- Correlates data across many sources to identify attack patterns and give you more insights for investigation
- Uses many different threat intelligence platforms to incorporate the latest data into new detections

Blumira

BATTLECARD

Other Products

SOC-as-a-Service

- 24/7 global SOC security monitoring
- Security concierge support
- Very expensive to pay for outsourced security analysts
- Alerts often lack meaningful context or relevant data, making investigation and response difficult
- Requires custom fine-tuning work to reduce false positives
- Reporting is often not a focus - can be slow, manual and difficult to generate reports
- May not have access to your data without a support ticket to request specifics

Blumira

- 24/7 detection and response coverage - automated by Blumira's platform to decrease human error and fatigue
- Includes 24/7 SecOps support for urgent priority issues
- On average, 40% less expensive than other SOCaaS providers (AW)
- Findings include all gathered, relevant data, stacking similar alerts to provide an easy-to-use history for investigation
- Cloud SIEM comes with rules fine-tuned by Blumira's security engineers to reduce false positives
- Pre-built, global reports allow you to easily populate and schedule security reports to send directly to you (no additional knowledge of query languages required)
- Proactive technical account manager support

Other Products

SOC

- Prohibitively expensive to hire, train, manage Tier 1 SOC analysts to watch environment 24/7
- Manual investigation, triage, response
- Not realistic to build out in-house for SMBs or most orgs - requires resources of large enterprise

Blumira

- Blumira provides affordable advanced detection, analysis, guided response, log retention and monitoring
- Blumira speeds up the investigation and triage process by providing all relevant, correlated data in findings
- 3-step rapid response guides your team with playbooks, automated response (dynamic blocklists) and 24/7 SecOps support for urgent priority issues

Compared to other products on the market today, Blumira strives to automate and simplify advanced security for organizations of all sizes, focusing on driving better security outcomes and continuously maturing your overall security posture.