Blumira Editions

Blumira

The Value of Blumira

Security monitoring in minutes

Making Security Accessible to All

Help SMBs struggling w/security costs & complexity

- Affordable
- Easy-to-deploy in minutes by existing team
- Greater security value - built-in detection & response

Easiest, Fastest Time to Security

Avg SIEM setup often fails or takes weeks to months to get operational

- Cloud Connectors takes minutes for setup
- Logs imported & rules applied automatically
- Any IT admin can do it

Security Coverage For Microsoft 365 & More

M365 is commonly used by SMBs and targeted by attackers

- Key integration to start log collection & detection
- Expand to cover entire tech stack - on-prem & cloud*
- 24/7 support for urgent issues*

**Paid editions only*

Blumira

Free SIEM

Security monitoring for 3 cloud apps, unlimited employees

- **Free cloud SIEM** for 3 cloud apps – choose from Microsoft 365, Google Workspace, SentinelOne, Webroot, Mimecast, Duo Security, Cisco Umbrella, Sophos, JumpCloud, OneLogin, 1Password, Google Cloud, Azure, CrowdStrike, and MS Defender for Cloud Apps
- **Easy, guided setup** through Cloud Connectors in minutes
- **Actionable findings** surfaced by Blumira's automated detection and response
- **Rule insight – see all active detection rules** automatically deployed
- **Detection rule management** to turn on/off rules to reduce noise
- **Managed detections** are maintained by our engineers (real-time only for free users. Paid editions get all detections for anomalies over time)
- **A summary dashboard** of your rules, connection status and security reports
- **14 days of log data retention** (upgrade to a year to meet compliance/insurance requirements)

Blumira

SIEM Starter

$12
Per employee/month

Meet compliance standards; expanded security coverage with all integrations & endpoint detections

Get everything in Free, plus:

- **1 year of data retention**, critical for investigation and compliance
- **Access to all integrations (Cloud Connectors & sensors)** for greater coverage
- **Endpoint detections** delivered via sensor
- **Option to add Blumira Agent** for easy endpoint detection deployment
- **Customer support** for urgent priority issues from 9am-8pm ET
- **White glove onboarding** with a dedicated Solution Architect, one-time fee required ($250)
- **Advanced reporting & dashboards** to see security trends & send scheduled reports. Includes pre-built compliance reports and Executive Summaries (quarterly only).
- **Detection rule management & detection filters** to toggle rules on/off, or further customize to suit your organization's needs

Blumira

SIEM+

$16
Per employee/month

Enhanced protection with 24/7 emergency security support

Get everything in SIEM Starter, plus:

- **24/7 Security Operations (SecOps) support** for urgent priority issues
- **Microsoft 365 Threat Response** allowing you to manually respond to M365 findings to disable users, directly through Blumira
- **Blumira Agent** for endpoint visibility and response (1 per employee)
- **Manual host isolation** allows you to remotely isolate an affected endpoint to contain an identified threat
- **Manual dynamic blocklists** sends you an alert about known malicious sources of traffic, asking if you want to block the source & add to your blocklist
- **SAML** to authenticate users with your preferred identity provider
- **Blumira Investigate** for easy log searching & reports for investigation
- **Honeypots** to gain visibility into access attempts into your environment
- **White glove onboarding** with dedicated Solution Architect for one-time required fee ($500)
- **External threat surface scans** biannually
- **Dedicated CSM** w/meetings on a quarterly basis

Blumira

XDR

$21

Per employee/month

Stop threats faster with comprehensive coverage & automated response

Get everything in SIEM+, in addition to:

- **1 year of data retention**, with longer term retention options
- **White glove onboarding** with a dedicated Solution Architect included with no additional fee
- **Automated host isolation** immediately isolates an affected endpoint to contain an identified threat when a finding is triggered (priority of finding is configurable)
- **Automated blocking (for dynamic blocklists)** immediately blocks access by known malicious traffic when a finding is triggered by your firewall, with no need for your team to review or respond to the finding
- **API access** to get access to Blumira's findings data

Blumira