Blumira Editions

Blumira

The Value of Blumira's Free SIEM

Security monitoring for 3 cloud apps in minutes

Making Security Accessible to All

Help SMBs struggling w/security costs & complexity

- Affordable (free)
- Easy-to-deploy in minutes by existing team
- All-in-one - cloud SIEM, 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 activated 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*

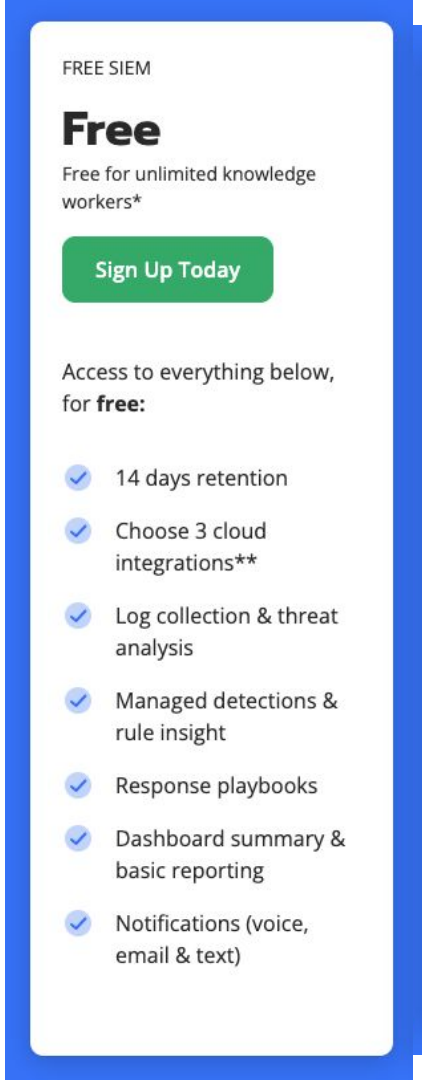
**Paid editions only*

Blumira

What You Get For Free

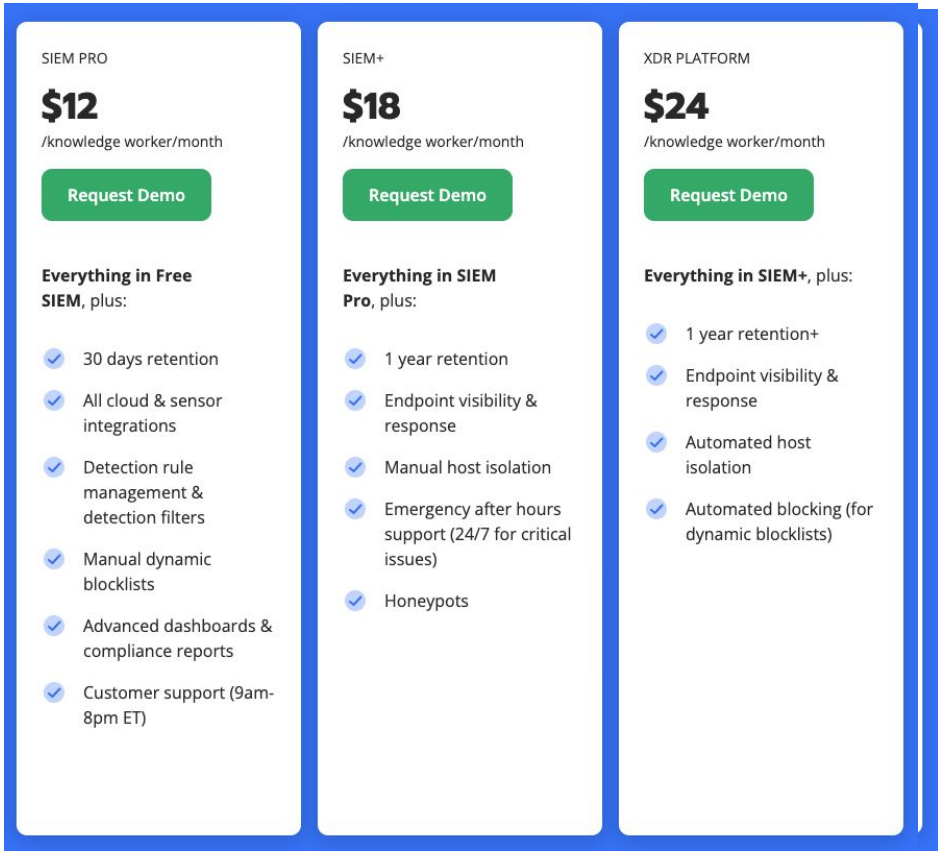
Security monitoring for 3 cloud apps – unlimited knowledge workers & data

- **Free cloud SIEM** for 3 cloud apps – choose from M365, Duo, SentinelOne, Webroot, Mimecast or Google Workspace
- **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
- **Managed detections** are maintained by our engineers
- **A summary dashboard** of your rules, connection status and security reports
- **1 week of log data retention** (upgrade for up to a year to meet compliance/insurance requirements)



Upgrade For Compliance, Endpoint Security & Support

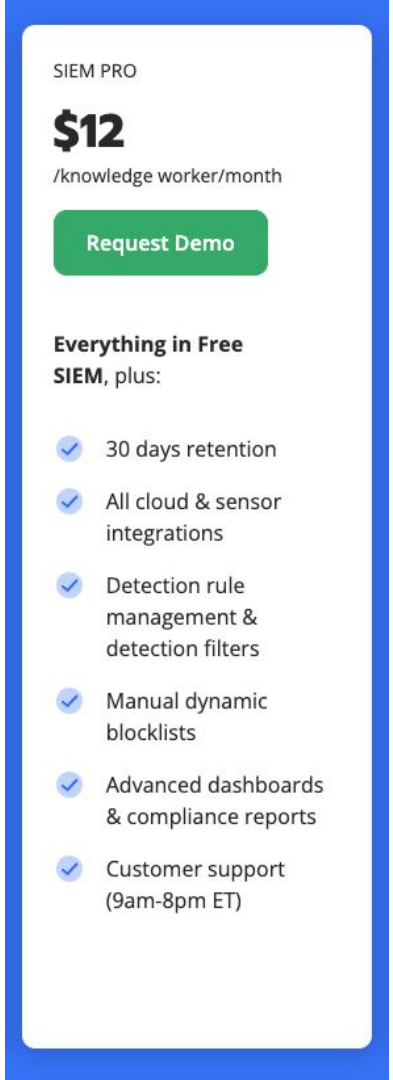
- **Additional integrations** across on-prem, cloud & remote endpoints for greater visibility
- **24/7 security operations team support** for urgent priority issues
- **Up to 1 year of log data retention**, ideal for compliance & cybersecurity insurance
- **Automated response** to block threats immediately (dynamic blocklists) & isolate endpoints (automatic host isolation)
- **Advanced reporting & dashboards**, including executive summaries and pre-built compliance reports



Paid: SIEM Pro

Get everything in Free, plus:

- **Access to all cloud & sensor integrations** for greater coverage (including infrastructure (AWS), endpoint security, firewalls, servers, and more)
- **Customer support** for urgent priority issues from 9am-8pm ET
- **Advanced reporting & dashboards** to see security trends (Responder, Manager & Security view) and send scheduled reports. Includes pre-built compliance reports & Executive Summaries
- **30 days of data retention**, useful for investigation
- **Detection rule management & detection filters** to toggle rules on/off, or further customize to suit your organization's needs
- **Manual dynamic blocklists** integrated with your firewall notifies you of known malicious sources of traffic, asking if you want to block the source and add them to your blocklist

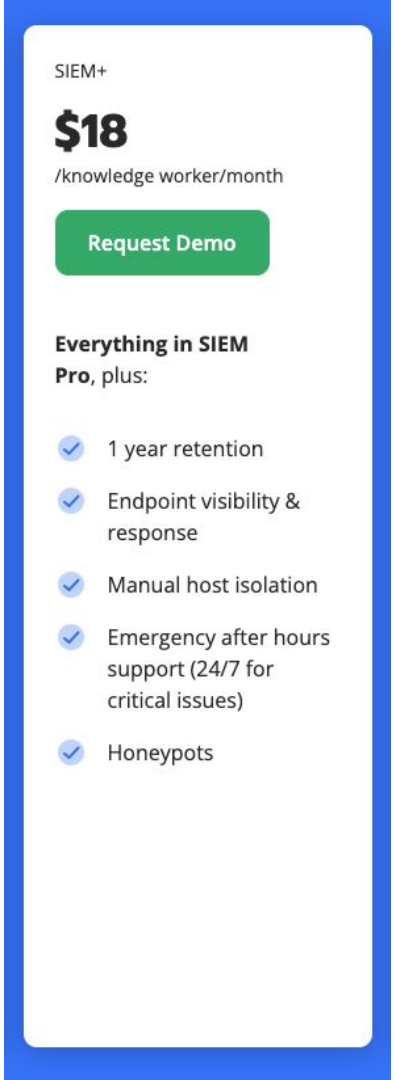


Paid: SIEM+

Get everything in SIEM Pro, plus:

- **24/7 Security Operations (SecOps) support** for urgent priority issues, dedicated onboarding and ongoing SA (Solution Architect) sessions, technical troubleshooting
- **1 year of data retention**, needed to meet most compliance and cyber insurance requirements
- **Endpoint visibility & response** for greater coverage across remote endpoints*
- **Manual host isolation** allows you to remotely isolate an affected endpoint to contain an identified threat
- **Honeypots** to gain visibility into active threats, like unauthorized access attempts within your environment

** 1 agent per knowledge worker is included in pricing. Additional agents/endpoints are available for purchase.*



Paid: XDR Platform

Get everything in SIEM+, plus:

- **1 year of data retention**, with options for access to additional data
- **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