Blumira

XDR & SIEM Editions

Easily meet compliance with SIEM data retention, security reporting, 24/7 SecOps and more.

	FREE SIEM	SIEM STARTER	SIEM+	XDR
Pricing per month	**Free**	**Contact for pricing**	**Contact for pricing**	**Contact for pricing**
DATA				
Data Ingestion - Unlimited log volume for complete visibility	Limited	Unlimited	Unlimited	Unlimited
Data Retention - Access to a history of your past logs, ideal to meet most compliance requirements	14 days	1 year	1 year	1 year
Long-Term Storage Option - More than 1 year available			☑	☑
INGESTION				
Cloud Connectors - Set up a cloud integration in minutes via API. Free SIEM users pick 3: Microsoft 365, Google Workspace, SentinelOne, Webroot, Mimecast, Duo Security, Cisco Umbrella, Sophos, JumpCloud, OneLogin, 1Password, Google Cloud, Azure, CrowdStrike, & MS Defender for Cloud Apps	Up to 3	☑	☑	☑
Sensors - Firewalls, servers, endpoint protection and others collect logs via a sensor and send it to Blumira's SIEM platform		☑	☑	☑
ENDPOINT				
Endpoint Detections - Managed detections delivered through a lightweight agent for early identification of endpoint threats. Available for Windows, macOS & Linux		Via Sensor	Blumira Agent	Blumira Agent
Included Agents			1/employee	1/employee
Ability to Buy Additional Agents		☑	☑	☑
Endpoint Visibility - Insight into endpoint security trends with reports			☑	☑
LOGGING				
Log Collection - Blumira collects, centralizes & parses your logs automatically	☑	☑	☑	☑
Threat Analysis - Blumira's platform monitors logs 24/7 for signs of a threat	☑	☑	☑	☑
DETECTION				
Managed Detections - Auto-applied at deployment, Blumira's engineers write, tune & manage 550+ detection rules to keep up with the latest threats	Real-time only	☑	☑	☑
Detection Rule Insight - See every rule enabled in your environment	☑	☑	☑	☑
Detection Rule Management - Toggle rules on or off as needed	☑	☑	☑	☑
Detection Filters - Customize rules to allow known safe users, IPs and more		☑	☑	☑
Custom Detections Available - Request custom rules from Blumira team			☑	☑
EDR - Endpoint detection and response		Sensor detections	☑	☑

Blumira

	FREE SIEM	SIEM STARTER	SIEM +	XDR PLATFORM
AUTOMATED RESPONSE				
Automated Dynamic Blocklists - Automatically resolve findings, add a threat to your blocklist and block access by known bad IPs				☑
Automated Host Isolation for Agent - Through Blumira Agent, devices associated with a threat detected will be automatically isolated or contained				☑
MANUAL RESPONSE				
Response Playbooks - Every finding comes with easy-to-understand instructions to guide users through how to respond	☑	☑	☑	☑
Microsoft 365 Threat Response - Users can manually respond to M365 findings to lock out potentially compromised M365 users			☑	☑
Manual Host Isolation - Through Blumira Agent, users can manually isolate devices associated with a finding			☑	☑
Manual Dynamic Blocklists - Users can manually respond to findings, add known threats to their blocklists and block access by known bad IPs			☑	☑
DASHBOARDS				
Dashboard Summary - See number of logs imported, blocked events, unresolved findings, detection rules, users & more	☑	☑	☑	☑
Advanced Dashboards - Responder, Manager & Security dashboards		☑	☑	☑
REPORTING				
Saved Reports - Basic: Dashboard Summary, Popular Reports for 3 cloud integrations, global reports for 3 cloud integrations. Advanced: All scheduled reports	Basic	Advanced	Advanced	Advanced
Compliance Reports - Basic: Access compliance reports related to 3 cloud integrations. Advanced: All compliance reports (ISO, NIST, CMMC, CIS & more)	Basic	Advanced	Advanced	Advanced
Report Builder - Access to your logs & ability to create your own reports	☑	☑	☑	☑
Blumira Investigate - Easily search logs by user, port, application or system			☑	☑
Executive Summaries - Monthly or quarterly auto-generated snapshots of your security program; ideal for stakeholders & executives		Quarterly only	☑	☑
DECEPTION TECHNOLOGY				
Honeypots - Deception technology that identifies unauthorized access attempts & lateral movement, alerts you and helps you respond			☑	☑
SPECIAL OFFERS				
Trava Compliance Services - Get discounted compliance security expertise for HIPAA, NIST, ISO, FedRAMP, GDPR, CCPA, SOC 2, HITRUST, and more		20% Off	20% Off	20% Off
FounderShield Insurance - Get insurance management for high-growth companies, including tech startups, financial services, and more		20% Off	20% Off	20% Off

Blumira

	FREE SIEM	SIEM STARTER	SIEM +	XDR PLATFORM
ADDITIONAL FUNCTIONALITY				
API - Access to Blumira's findings data via API				☑
SAML - Authenticate users with your preferred identity provider			☑	☑
NOTIFICATION + SUPPORT				
Notifications (Voice, Text & Email) - Choose your preferred method of notification of a Blumira finding, configured by priority or finding type	Email Only	☑	☑	☑
White Glove Onboarding (One-time fee required) - Scheduled sessions with a dedicated Solution Architect for custom integration setup, troubleshooting and testing		$250	$500	Included
Concierge Support (9am-8pm ET) - Contact Blumira's team for assistance with troubleshooting, security advice, configurations & more		☑	☑	☑
Emergency Support (24/7 for critical issues) - Blumira's team is on standby to provide support in the event of a critical priority issue			☑	☑
External Threat Surface Scans (Biannually) - Identifying unknown entry points in an organization's infrastructure to secure your environment			☑	☑
Dedicated CSM - Regular sessions with a customer service manager to help ensure your ongoing security success			☑	☑

MSP pricing and packaging will differ. Contact msp@blumira.com for more details.
**Subject to our Terms and Conditions.*
***Free SIEM can choose up to 3 cloud integrations: 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*

Pricing FAQ: What defines an employee?

Pricing is based on the total number of "employees" or knowledge workers in your organization (it does not refer to the number of users or admins with Blumira accounts). A knowledge worker is an employee with a corporate email address and workstation/device (may not include number of factory workers or students at a university).

This helps us determine a more accurate estimate of the amount of data you are sending to our platform.

Volume, education and nonprofit discounts available.
Contact sales for custom quote.

Republic used Blumira's Free SIEM for a year before upgrading to the SIEM + XDR solution for greater visibility and to strengthen their security posture.

"Prior to Blumira, we had a lack of visibility. Blumira gives us information that I didn't previously have, including reports of suspicious activities involving PowerShell, and many other things happening in our environment. I didn't have any other tools that provided this kind of insight."
– Andy Barcus, Director of IT, Republic

TRY XDR TODAY

Blumira makes security easy and effective for SMBs, helping them detect and respond to cybersecurity threats faster to stop breaches and ransomware.

Sign up for a free 30-day trial of Blumira's SIEM + XDR platform.

BLUMIRA.COM