Blumira

XDR & SIEM Editions

EASY-TO-USE EDITIONS DESIGNED FOR EVERY ORGANIZATION

	FREE	SIEM +	XDR PLATFORM
Pricing per month	**Free**	**$20/seat**	**$25/seat**
DATA + PRICING			
Data Ingestion - Unlimited log volume for complete visibility	☑	☑	☑
Data Retention - Access to a history of your past logs, ideal to meet most compliance requirements	14 days	1 year	1 year
Long-Term Storage Option - More than 1 year available			Talk to rep
SOURCES			
Cloud Integrations - Set up a cloud integration in minutes via APIs. Free SIEM users can pick 3 from: Microsoft 365, SentinelOne, Webroot, Mimecast, Duo Security, Cisco Umbrella, Sophos, OneLogin, JumpCloud, 1Password	Pick 3	☑	☑
Sensor Integrations - Firewalls, servers, endpoint protection and others collect logs via a sensor and send it to Blumira's SIEM platform		☑	☑
Endpoint Visibility + Response (Blumira Agent) - A lightweight agent that collects remote endpoint data to send to Blumira's platform for detection & response. Available for Windows, macOS & Linux		50-Unlimited 1 per seat	50-Unlimited 1 per seat
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 detection rules to keep up with the latest threats	☑	☑	☑
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		☑	☑
RESPONSE			
Response Playbooks - Every finding comes with easy-to-understand instructions to guide users through how to respond	☑	☑	☑
Manual Host Isolation - Through Blumira Agent, users can manually isolate devices associated with a finding		☑	☑

Blumira

	FREE SIEM	SIEM +	XDR PLATFORM
RESPONSE			
Manual Dynamic Blocklists - Users can manually respond to findings, add known threats to their blocklists and block access by known bad IPs	☑	☑	☑
Automated Host Isolation - Through Blumira Agent, devices associated with a threat detected will be automatically isolated or contained		☑	☑
Automated Blocking (for Dynamic Blocklists) - Automatically resolve findings, add a threat to your blocklist 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
Compliance Reports - Basic: Access compliance reports related to 3 cloud integrations. Advanced: All compliance reports (ISO, NIST, CMMC, CIS & more)	Basic	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		☑	☑
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 - Scheduled sessions with a dedicated Solution Architect for custom integration setup, troubleshooting and testing		$500	$0
Ongoing Support (9am-8pm ET) - Contact Blumira's SecOps team for assistance with troubleshooting, security advice, configurations & more		☑	☑
Emergency After Hours Support (24/7 for critical issues) - Blumira's SecOps 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 + Recurring Syncs (Quarterly) - Regular sessions with a customer service manager to help ensure your ongoing security success		☑	☑
DECEPTION TECHNOLOGY			
Honeypots - Deception technology that identifies unauthorized access attempts & lateral movement, alerts you and helps you respond		☑	☑

Blumira

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 from: Microsoft 365, SentinelOne, Webroot, Mimecast, Duo Security, Cisco Umbrella, Google Workspace, Sophos, OneLogin, JumpCloud, Azure*
****Additional agents are available for purchase for $3/agent/month*

A seat is an employee with an email address; pricing based on total number of employees in your organization (not Blumira users or admins). Plans receive 1 agent per seat with additional available for monthly fee.

*The one thing that really stood out right away was the ease of deployment - **I had a working trial operational inside of an afternoon**.*

-- Fritz Ludemann, Information Systems Admin, The City of Crescent City

TRY XDR TODAY

Blumira makes security easy and effective, helping organizations 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.

Visit blumira.com/xdr-trial

©2024 Blumira, Inc. All rights reserved. | Public