DATA SHEET

Blumira
Free SIEM
blumira.com/free

Blumira's Free SIEM

Sign up for free, no credit card or sales conversation required.

Get easy, effective security your team can actually use to defend against breaches and ransomware, while meeting compliance and cyber insurance requirements. Blumira's SIEM detects threats earlier for faster threat response and better security outcomes.

Detect & Respond to Cloud Threats

Blumira's Free SIEM detects and helps you respond to cloud security threats, including initial access, account takeovers, suspicious activity, and other techniques used in business email compromise (BEC), ransomware and other malware campaigns.

With our Free SIEM edition, you'll get:

- Unlimited users and data -- choose up to 3 cloud integrations (from Google Workspace, Google Cloud, Microsoft 365, Duo Security, SentinelOne, Cisco Umbrella, Mimecast, Webroot, Azure, Sophos, Jumpcloud, OneLogin, 1Password)
- Easy cloud SIEM setup in minutes with Cloud Connectors
- Detections automatically activated, fine-tuned for noise
- Summary dashboard of key findings & basic reports
- Playbooks to guide you through response steps
- 14 days of log data retention (upgrade to paid for 30 days or one year)

Microsoft 365 · SentinelOne · WEBROOT · Microsoft Azure · Cisco Umbrella · onelogin by ONE IDENTITY · DUO · mimecast · Google Workspace · Google Cloud

Looking for AWS and other integrations?

Check out all our plans at blumira.com/pricing

Why Free?

Automate Security Tasks
We do all the heavy lifting for your team to save them time, including parsing, creating native third-party integrations, and testing and tuning detection rules to reduce noisy alerts. Spend less than 15 minutes a day on average managing your security with Blumira.

Faster Time to Security
Our unique approach to detections notifies you of threats other security tools may miss, sending you real-time alerts in under a minute of initial detection to help you respond to threats faster than ever.

Security Coverage For 3 Cloud Integrations
Choose from up to 3 cloud integrations, including Google Workspace, Google Cloud, Microsoft 365, Duo Security, SentinelOne, Cisco Umbrella, Mimecast, Webroot, Azure, Sophos, Jumpcloud, OneLogin, 1Password

For broader coverage, expand to cover both on-prem, cloud, and remote endpoints with Blumira Agent. Get full 24/7 support from Blumira's Security Operations team for onboarding, guided response and more!*

**Available for paid editions*

DATA SHEET

Blumira
Free SIEM
blumira.com/free

Findings: Coverage of Real Cloud Threats

Blumira leverages threat intelligence and behavioral analytics to detect attack patterns. We do the heavy lifting for you, automatically activating detection rules to identify:

Detect Attacker Activity

- Privilege escalation of Exchange admin accounts
- Creation of forwarding & redirect rules
- Suspicious inbox rule creation
- When files are shared with personal email addresses
- The mass download of files
- Whenever an email send limit is exceeded to protect against spam campaigns

Ransomware & Malware

- Ransomware activity (high rate of file uploads or deletion activity could indicate an adverse encryption process)
- Malware campaigns detected in SharePoint and OneDrive
- Malware campaigns detected after delivery
- Malware auto-purge failed due to user configuration (Microsoft's email protection features disabled)

Unusual Behavior

- Any activity from anonymous or suspicious IP addresses
- Activity from infrequent countries or terminated users
- Any unusual external file activity
- Increases in phishing emails or ISPs (internet service providers) for an OAuth application
- Any suspicious email sending patterns detected

User & Access Security

- Multi-factor authentication (MFA) is disabled for an Azure Active Directory (AD) user
- Anomalous access attempts or the creation or deletion of an application password
- Anytime a user clicks on a malicious URL or is restricted from sending an email
- Any impossible travel activity, indicating unauthorized access
- Multiple failed user logon attempts

DATA SHEET

Blumira

Free SIEM
blumira.com/free

Deeper Visibility Into Microsoft 365

With Blumira's Microsoft 365 reports, your organization can track security trends over time to learn about your attack surface. *No knowledge of complex query languages required to run a report.*

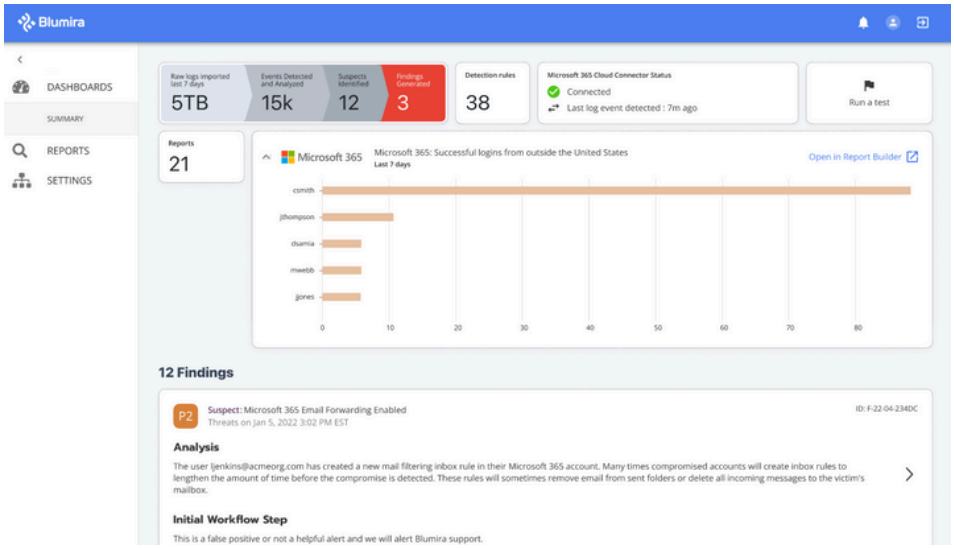
Here are a few examples of pre-built reports you get for free:

- **Disabled Azure AD accounts**, deleted contacts and any group changes
- **Password changes or resets**, and user or device added
- **Failed user login attempts**, overall login reports and logins outside of U.S., Canada and Mexico
- **Impossible travel activity** and successful logins outside of the U.S.
- **Delegation of mailbox permissions,** mail items accessed (other than the owner) and emails forwarded to new domains
- **Files previewed or accessed** - SharePoint

Upgrade to a paid edition for advanced reporting features:

- Show immediate security value to your manager or CEO with **Executive Summaries**, generated monthly & quarterly
- Schedule reports to send automatically to your team; drill down deeper into report details for investigation and compliance
- Get at-a-glance Security, Manager and Responder dashboards
- Prove your compliance easily to auditors with pre-built compliance reports, such as NIST

View plans and pricing at blumira.com/pricing



Summary Dashboard of Free SIEM

Benefits of Blumira:

- **Faster time to security** - deploy in minutes, 5x faster than industry average
- **Save your team's time** - automate manual triage and response
- **Lower TCO** - transparent, all-in-one platform priced per seat (not by data ingestion)
- **Access to security experts** - responsive support included; no need for in-house analysts

"We chose Blumira for its simplicity – I needed a solution that would simplify, consolidate and show me what I really need to see."

- Jim Paolicelli, IT Director, Atlantic Constructors

ATLANTIC CONSTRUCTORS

SIGN UP FREE

blumira.com/free

DATA SHEET

Blumira

Free SIEM
blumira.com/free

Upgrade to Unlock Greater Security Value

It's easy to upgrade to a paid edition for:

- **24/7 Support** - Get help with guided response from Blumira's security operations team; access onboarding and troubleshooting from dedicated Solution Architects
- **Expanded Coverage** - Gain broader visibility across your entire environment with access to all cloud and on-prem integrations
- **Endpoint Visibility** - Identify endpoint risks, reduce your attack surface and stop the spread of attacks with Blumira Agent
- **Automated Response** - Save time & improve outcomes by blocking malicious traffic immediately and automatically isolating endpoint threats
- **One Year of Data Retention** - Get on-demand access to historical data for compliance and cybersecurity insurance requirements, starting at one year
- **Detection Filters** - Customize your detection rules with filters that help reduce noisy alerts; avoid alerting on known safe activity

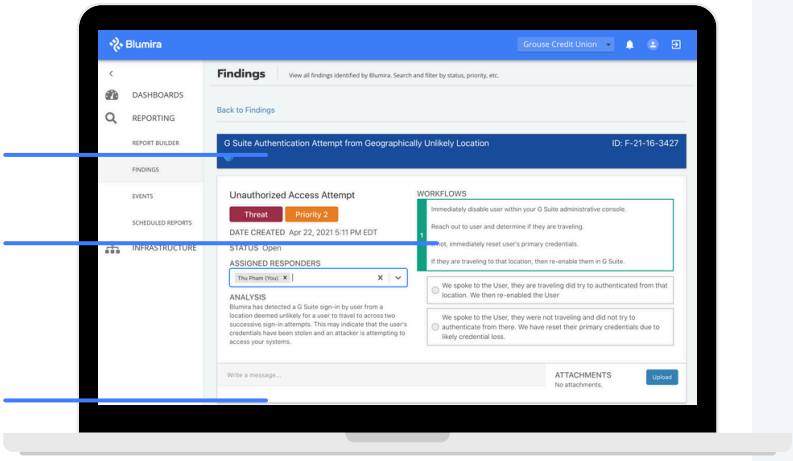
View plans and pricing at blumira.com/pricing

Security Made Accessible to All

Detailed Threat Analysis

Playbooks For Response

Direct Message a Security Expert*



**Available for paid editions*

"I would recommend Blumira -- it makes our daily job so much easier and it's simple to set up security for our customers. We only receive alerts that we need to act upon."

- Adam Thomas, Director of Cybersecurity, Path Forward IT (MSP)

PathForward IT
BE CONFIDENT IN YOUR IT.

"SIEMs have been unreachable for small or medium-sized companies for far too long and we are glad to say that with Blumira, that's not the case anymore."

- David S. CISO

SIGN UP FREE

blumira.com/free