Blumira's New Editions

SIEM & XDR
Designed For SMBs

Blumira

FREE SIEM

Free

Free for Unlimited Users*

Sign Up Today

Access to everything below, for **free:**

- 14 days retention
- Choose 3 cloud integrations**
- Log collection & threat analysis
- Managed detections & rule insight
- Response playbooks
- Dashboard summary & basic reporting
- Notifications (voice, email & text)

SIEM PRO

$12

/user/month

Contact Us

Everything in Free SIEM, plus:

- 30 days retention
- All cloud & sensor integrations
- Detection rule management & detection filters
- Manual dynamic blocklists
- Advanced dashboards & reporting
- Customer support (9am-8pm ET)

SIEM + ENDPOINT VISIBILITY

$18

/user/month

Contact Us

Everything in SIEM Pro, plus:

- 1 year retention
- 1 Blumira Agent per user (extras $6/ea)
- Manual host isolation
- Emergency after hours support (24/7 for critical issues)
- Honeypots

XDR PLATFORM

$24

/user/month

Contact Us

Everything in SIEM + Endpoint Visibility, plus:

- 1 year retention+
- 1 Blumira Agent per user (extras $4/ea)
- Automated host isolation
- Automated blocking (for dynamic blocklists)

Note - MSRP is listed here, and is not Partner Cost

Blumira

The Value of Blumira's Free Edition

Cloud security monitoring for Microsoft 365 & other cloud apps

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

M365 is commonly used by SMBs and targeted by attackers

- Choose up to 3 free cloud integrations – M365, Duo, SentinelOne, Umbrella, Webroot & Mimecast
- 24/7 support for urgent issues*

**Paid editions only*

Blumira

What You Get For Free

*Cloud security monitoring for Microsoft 365 & other cloud apps – unlimited users & data**

- **Free cloud SIEM** for 3 cloud apps – choose from M365, Duo, SentinelOne, Umbrella, Webroot & Mimecast
- **Easy, guided setup** through Cloud Connectors in minutes
- **Actionable findings** surfaced by Blumira's automated detection and response**
- **See all active detection rules** (30+ for M365)
- **A summary dashboard** of your rules, connection status and security reports
- **2 weeks of log data retention** (upgrade for up to a year)
- **Free help center** with documentation & articles

** Subject to our Terms of Service*

*** Due to the nature of our pre-tuned detections designed to reduce false positives, you may not receive an alert immediately. Example findings are available to view.*

FREE SIEM

Free

Free for Unlimited Users*

Sign Up Today

Access to everything below, for **free:**

- 14 days retention
- Choose 3 cloud integrations**
- Log collection & threat analysis
- Managed detections & rule insight
- Response playbooks
- Dashboard summary & basic reporting
- Notifications (voice, email & text)

Free Edition: How It Works

Sign up and set up takes only minutes – use existing Microsoft account

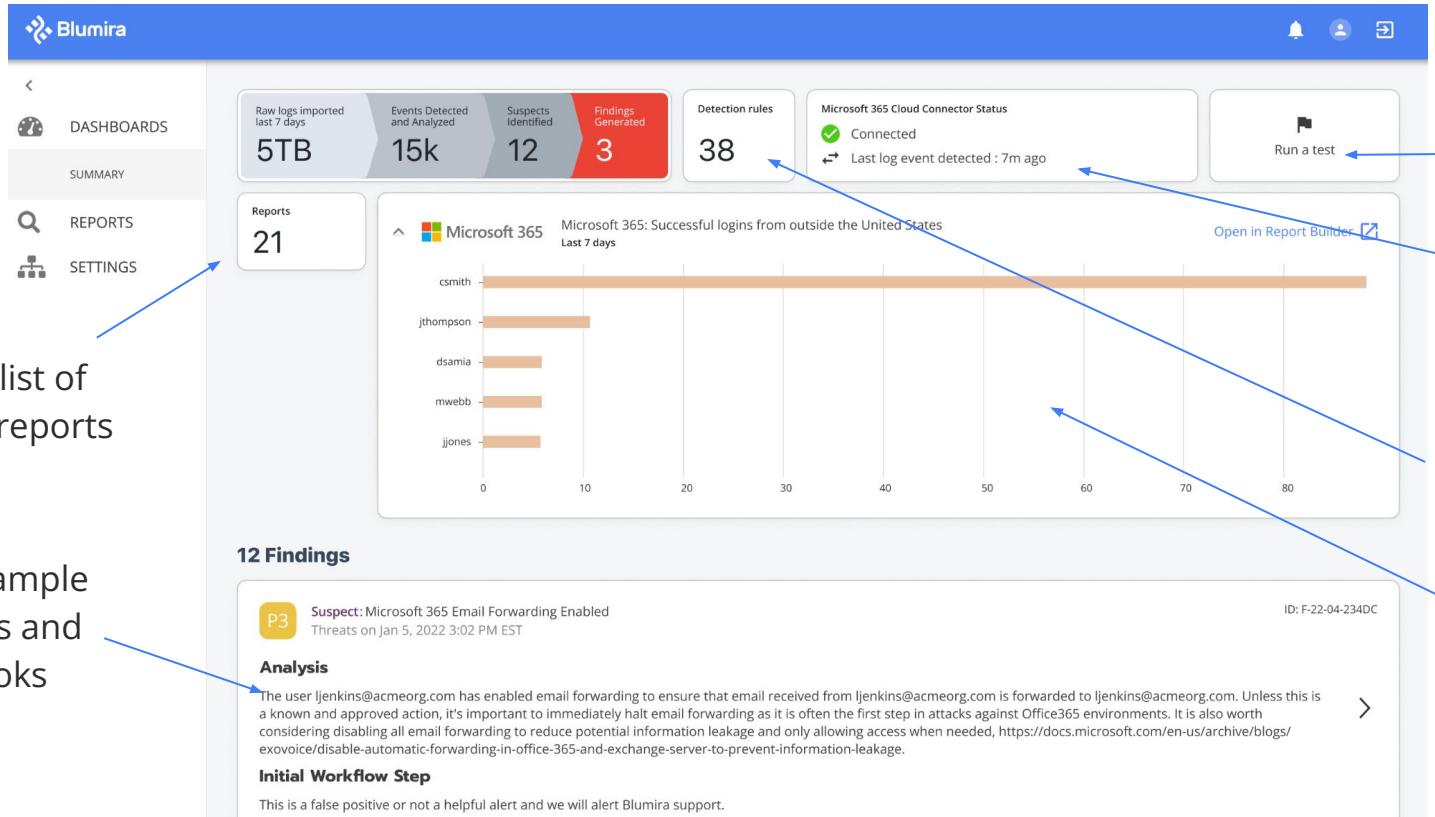
Watch the explainer video to learn:

- How to sign up
- Set up in minutes
- Send logs to Blumira
- Summary dashboard
- Example rules
- Example findings & playbooks
- Example reports

Note: MSP pricing will differ. MSP clients that would like to upgrade should contact their partner for more information.

Blumira

Free Edition: Summary Dashboard



See a list of basic reports

See example findings and playbooks

How to run a test of your detection rules

Confirm logs are being sent to Blumira

See list of active rules

See an example visual report

Blumira

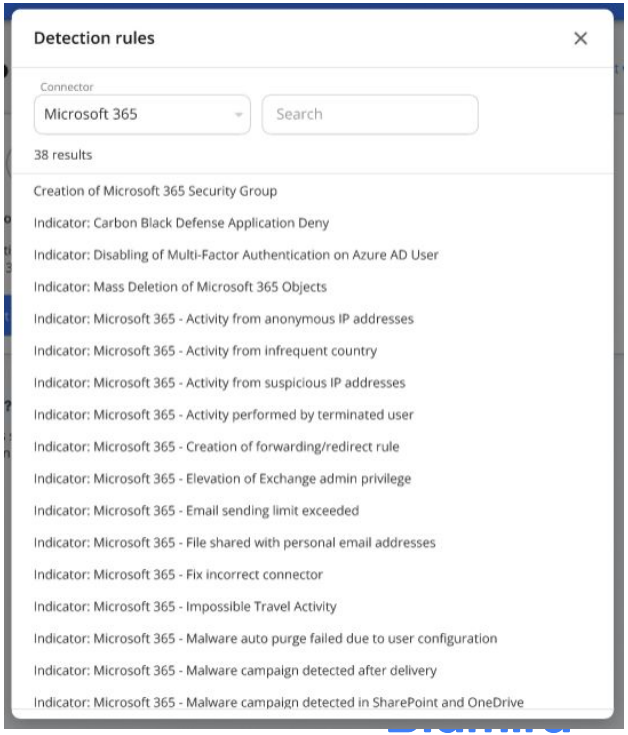
Free: Automated Detection Rules

Detect & respond to Microsoft 365 threats early to stop attacks

Blumira automatically applies fine-tuned rules to eliminate noise for your IT team. Our platform helps you respond to critical, threat-based detections for M365:

- Anomalous user logins
- Malicious email activity
- Password changes and resets
- Disabled MFA
- Malware campaigns
- Misconfigurations

And more! We update and add new rules every two weeks to keep you protected against the latest threats.



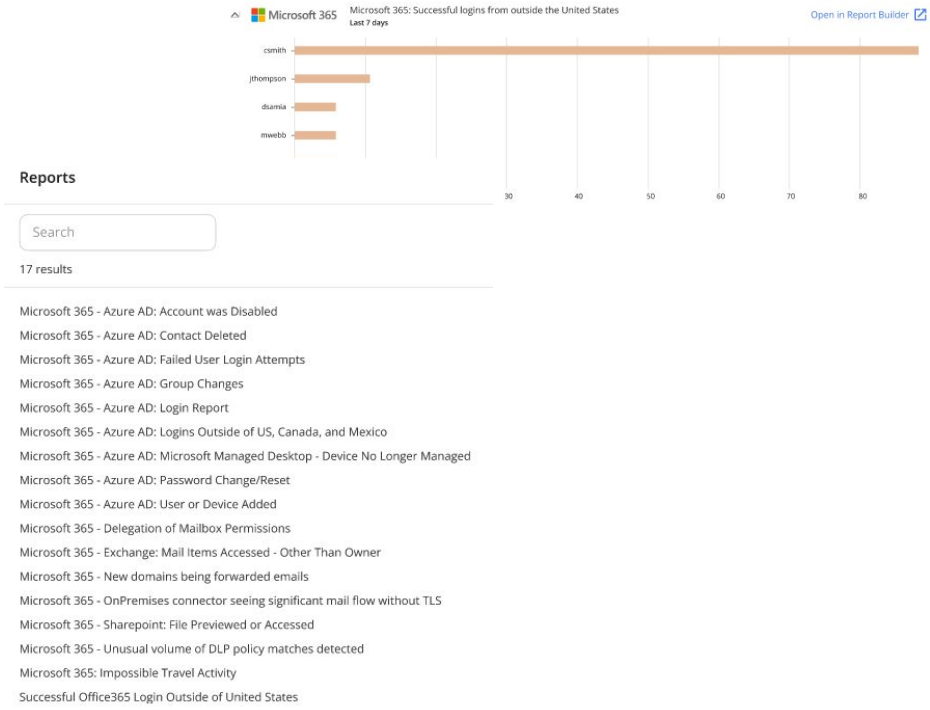
Free: Basic Security Reporting

Get basic reporting for deeper M365 visibility

Get pre-built (global) reports with the click of a button:

- Successful logins from outside the U.S.
- Failed Azure AD user login attempts
- Disabled Azure AD accounts, deleted contacts, password changes/resets
- Delegation of mailbox permissions

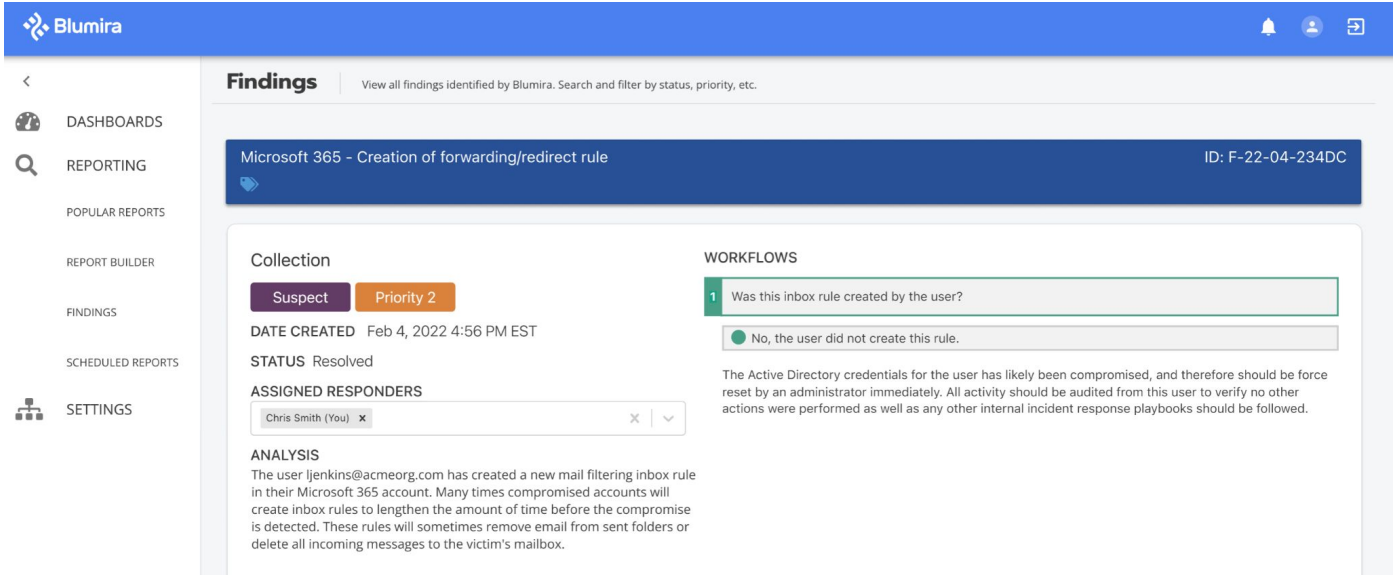
And more! Upgrade to access Scheduled Reports.



Blumira

Free: Findings & Playbooks

Get meaningful findings and easy-to-follow workflows for response

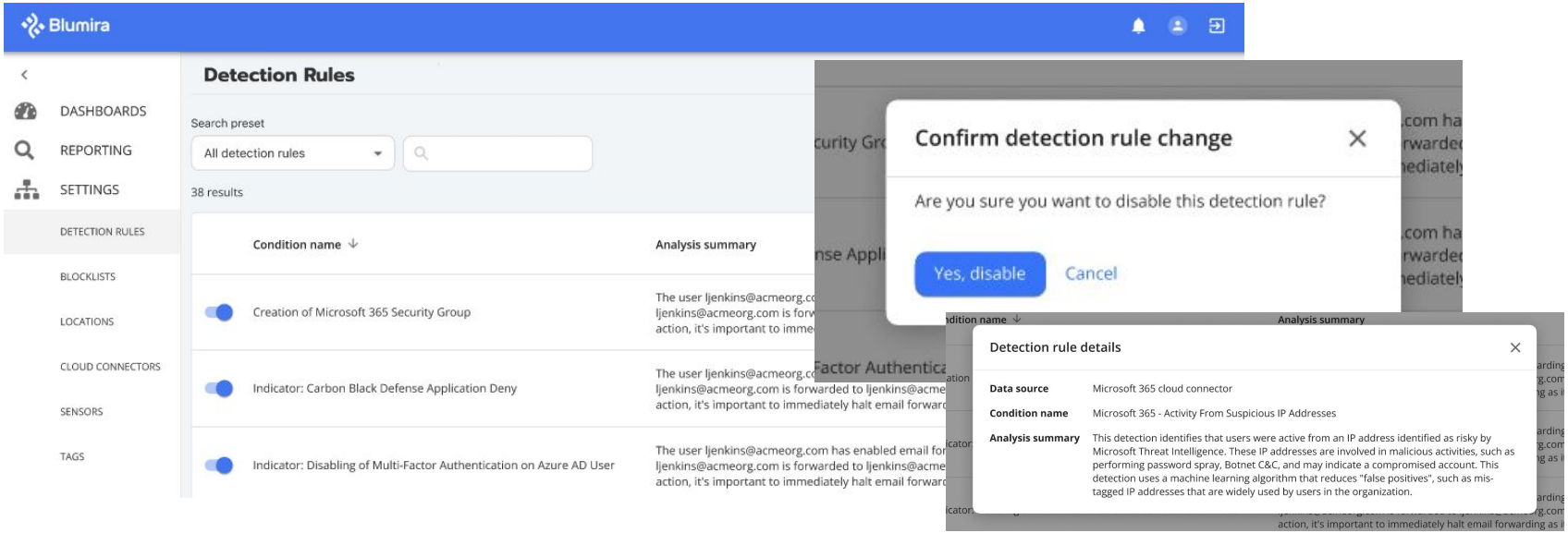


Need more help? Upgrade to paid to get access to Blumira's security operations team support.

Blumira

Paid: Detection Rule Management

Manage/choose which rules are right for your organization

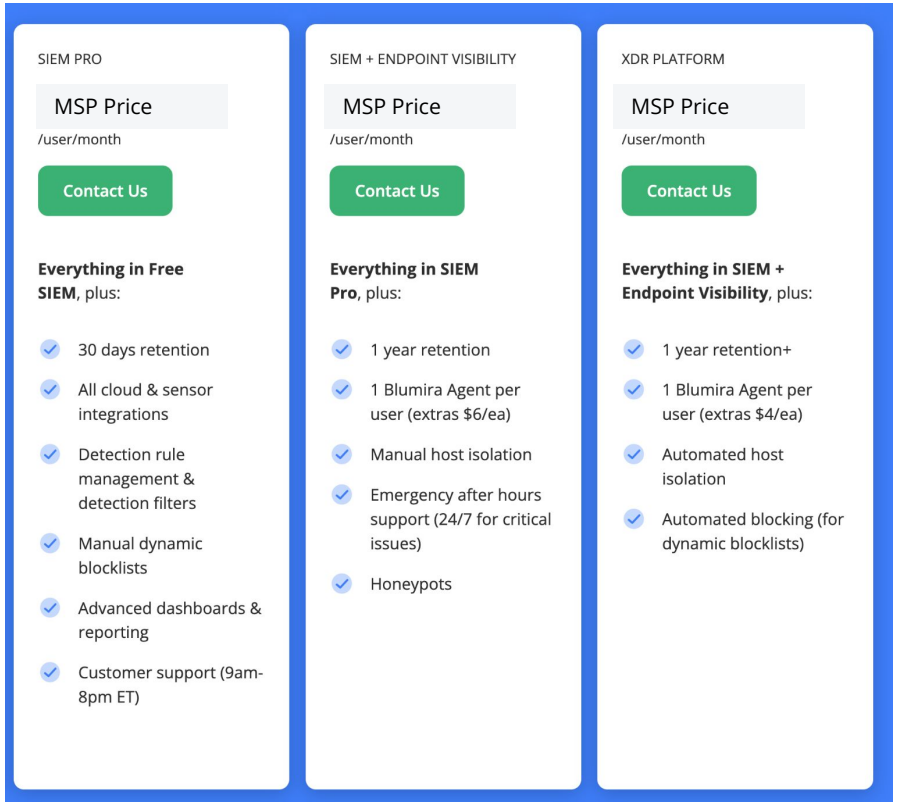


See all active detection rules automatically applied to your account and easily turn them on/off as needed.

Blumira

Upgrade For Greater Coverage & Support

- **Additional integrations** across on-prem & cloud
- **24/7 security operations team support** for urgent priority issues
- **1 year of log data retention + option for longer**, ideal for compliance & cybersecurity insurance
- **Automated response** to block threats & isolate devices immediately
- **Advanced reporting & dashboards** to see security trends and send scheduled reports

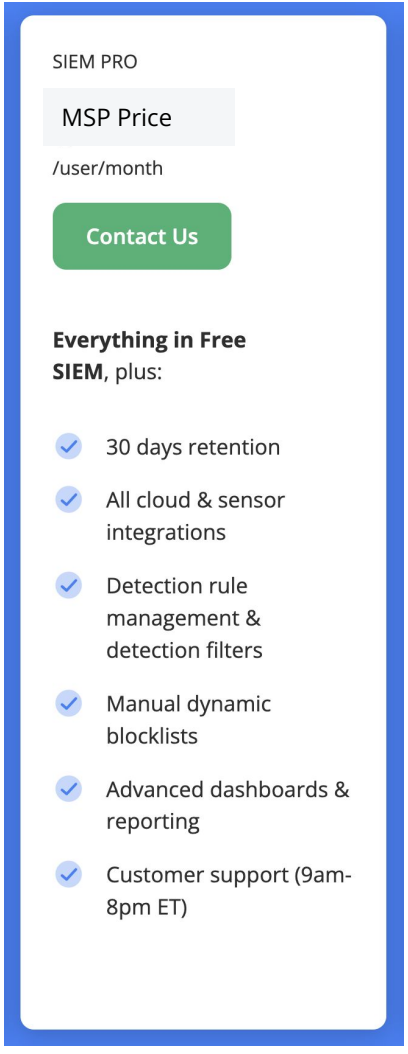


Blumira

Paid: SIEM Pro

Get everything in Free SIEM, plus:

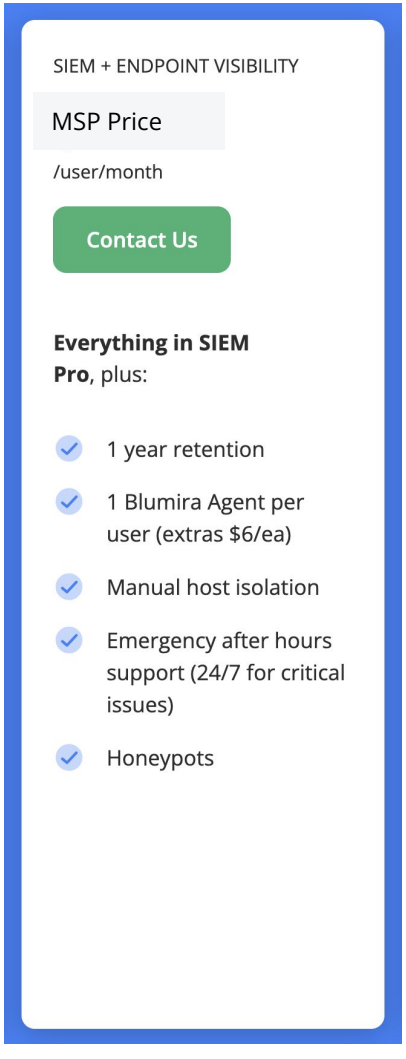
- **All cloud & sensor** integrations
- **Customer support (9am-8pm ET)**
- **Advanced reporting & dashboards** to see security trends and send scheduled reports
- **30 days of data retention**, useful for a historical overview and investigation
- **Detection rule management and detection filters** to see detailed rule analyses, toggle rules on/off, and customize detection rules to fit their organizations' needs
- **Manual dynamic blocklists** to notify your responders of known malicious sources of traffic attempting to access your environment



Paid: SIEM + Endpoint Visibility

Get everything in SIEM Pro, plus:

- **Blumira Agent for endpoint visibility -** 1 agent per user to give you coverage for remote Windows endpoints; option to purchase extras at $6/agent
- **Manual host isolation** with the option to isolate endpoints from your network when a threat is identified by Blumira
- **Emergency after hours support** for urgent priority issues
- **1 year of data retention**, ideal for meeting compliance & cybersecurity insurance requirements
- **Honeypots** - a decoy tool to lure attackers & identify unauthorized access attempts



Paid: XDR Platform

Get everything in SIEM+, plus:

- **1 year of data retention** for compliance, meeting cybersecurity insurance requirements & investigation
- **Blumira Agent for endpoint visibility -** 1 agent per user to give you coverage for remote Windows endpoints; option to purchase extras at $4/agent
- **Automated host isolation** to immediately contain affected devices, when a P1-P3 threat is triggered
- **Automated blocking (thru dynamic blocklists)** to immediately block sources of known threats