

Blumira's New Editions

*Automated Detection & Response
Designed For SMBs*

Free

Set up cloud security in minutes -- easy to evaluate.

Unlimited Users

Sign Up Free

- ✓ 1 Cloud Integration - Microsoft 365
- ✓ Unlimited Users & Data Ingestion*
- ✓ 1 Week Data Retention
- ✓ Detections & Response
- ✓ Basic Reporting
- ✓ Dashboard Summary
- ✓ Rule Insights

Microsoft 365

Access full support & longer data retention.

\$8/User, Per Month

Sign Up Today

- ✓ 1 Cloud Integration - Microsoft 365
- ✓ Unlimited Data Ingestion*
- ✓ 30 Days Data Retention
- ✓ Detections & Response
- ✓ Advanced Reporting
- ✓ Security Dashboards
- ✓ Rule Insights
- ✓ 24/7 Security Operations Team Support**

Cloud

Expand to cover popular cloud applications.

\$12/User, Per Month

Sign Up Today

- ✓ 3 Total Cloud Integrations - Microsoft 365, Duo Security, SentinelOne
- ✓ Unlimited Data Ingestion*
- ✓ 1 Year Data Retention
- ✓ Detections & Response
- ✓ Advanced Reporting
- ✓ Security Dashboards
- ✓ Rule Insights
- ✓ 24/7 Security Operations Team Support**

Advanced

Full coverage across your entire environment.

\$16/User, Per Month

Sign Up Today

- ✓ Coverage For All On-Premises and Cloud Integrations
- ✓ Unlimited Data Ingestion*
- ✓ 1 Year Data Retention
- ✓ Detections & Response
- ✓ Advanced Reporting
- ✓ Security Dashboards
- ✓ Automated Response (Dynamic Blocklists)
- ✓ Rule Insights
- ✓ Honeypots
- ✓ 24/7 Security Operations Team Support**

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

The Value of Blumira's Free Edition

Cloud security monitoring for Microsoft 365 with unlimited users & data



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

- 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

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

- **Free cloud SIEM** for your Microsoft 365 integration
- **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
- **1 week 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

Set up cloud security in minutes -- easy to evaluate.

Unlimited Users

Sign Up Free

- ✓ 1 Cloud Integration - Microsoft 365
- ✓ Unlimited Users & Data Ingestion*
- ✓ 1 Week Data Retention
- ✓ Detections & Response
- ✓ Basic Reporting
- ✓ Dashboard Summary
- ✓ Rule Insights

Free Edition: How It Works

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

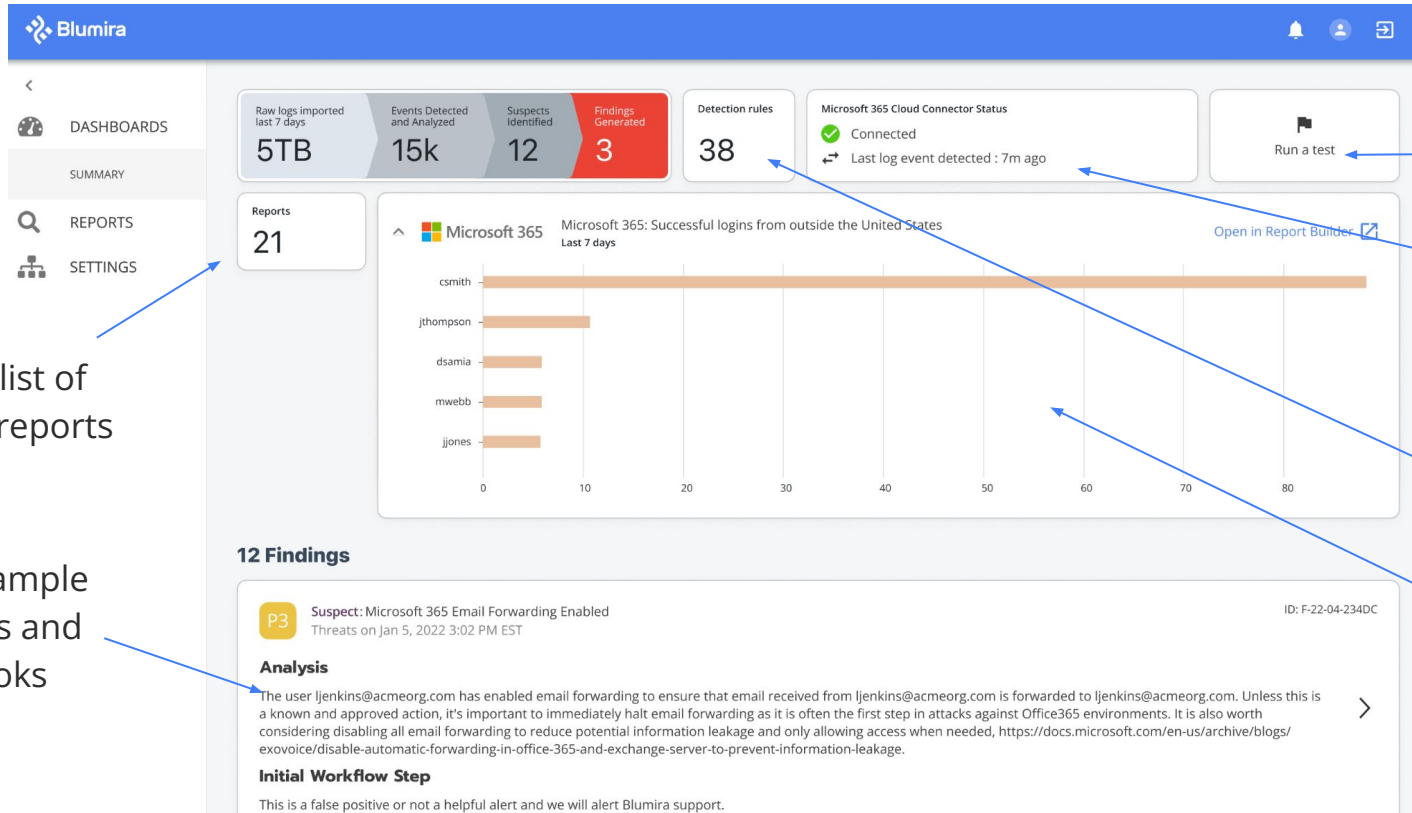


Watch the explainer video to learn:

- 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.

Free Edition: Summary Dashboard



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

See a list of basic reports

See example findings and playbooks

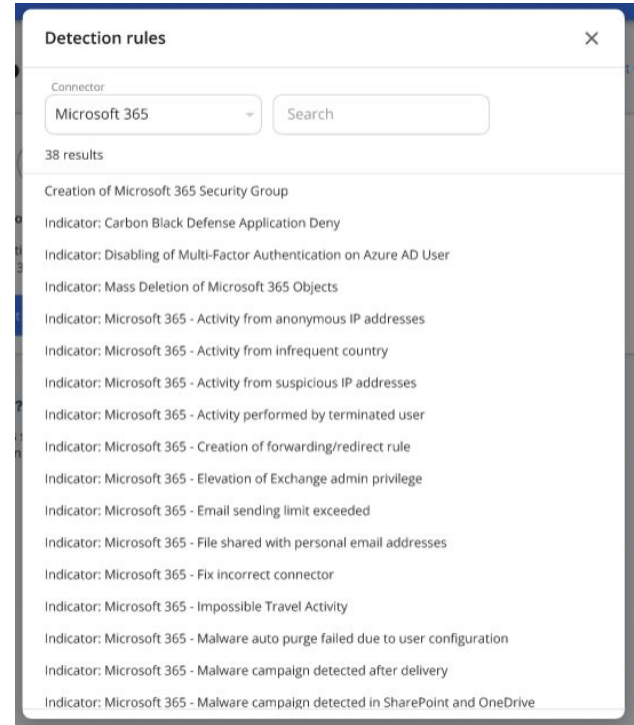
Free: Automated Detection Rules

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.



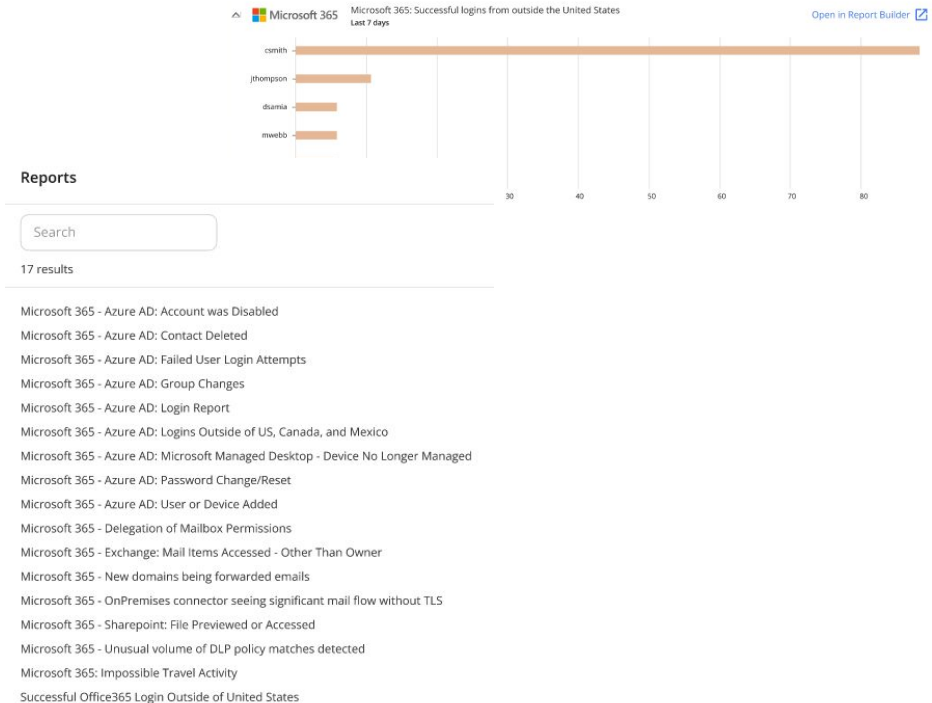
Free: Basic Security Reporting

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.



Free: Findings & Playbooks

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

The screenshot displays the Blumira interface. At the top, the Blumira logo is on the left, and notification, user, and help icons are on the right. A left sidebar contains navigation options: DASHBOARDS, REPORTING, POPULAR REPORTS, REPORT BUILDER, FINDINGS, SCHEDULED REPORTS, and SETTINGS. The main content area is titled "Findings" and includes a subtitle: "View all findings identified by Blumira. Search and filter by status, priority, etc." Below this, a finding card is shown with the title "Microsoft 365 - Creation of forwarding/redirect rule" and ID "F-22-04-234DC". The finding details include: "Collection" with tags "Suspect" and "Priority 2"; "DATE CREATED" as "Feb 4, 2022 4:56 PM EST"; "STATUS" as "Resolved"; "ASSIGNED RESPONDERS" as "Chris Smith (You)"; and "ANALYSIS" text: "The user ljenkins@acmeorg.com has created a new mail filtering inbox rule in their Microsoft 365 account. Many times compromised accounts will create inbox rules to lengthen the amount of time before the compromise is detected. These rules will sometimes remove email from sent folders or delete all incoming messages to the victim's mailbox." To the right of the finding details is a "WORKFLOWS" section with a single step: "1 Was this inbox rule created by the user?" with a selected response: "No, the user did not create this rule." Below the workflow is a detailed response instruction: "The Active Directory credentials for the user has likely been compromised, and therefore should be force reset by an administrator immediately. All activity should be audited from this user to verify no other actions were performed as well as any other internal incident response playbooks should be followed."

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

Paid: Detection Rule Management

Manage/choose which rules are right for your organization

The image shows the Blumira web interface for managing detection rules. On the left is a navigation sidebar with categories like DASHBOARDS, REPORTING, SETTINGS, and DETECTION RULES. The main area displays a table of 38 detection rules. Two overlays are present: a "Confirm detection rule change" dialog box asking for confirmation to disable a rule, and a "Detection rule details" dialog box showing information for a specific rule, including its data source, condition name, and analysis summary.

Condition name	Analysis summary
<input checked="" type="checkbox"/> Creation of Microsoft 365 Security Group	The user ljenkins@acmeorg.com is forwarded to ljenkins@acmeorg.com as a result of this action, it's important to immediately halt email forwarding as a result of this action.
<input checked="" type="checkbox"/> Indicator: Carbon Black Defense Application Deny	The user ljenkins@acmeorg.com is forwarded to ljenkins@acmeorg.com as a result of this action, it's important to immediately halt email forwarding as a result of this action.
<input checked="" type="checkbox"/> Indicator: Disabling of Multi-Factor Authentication on Azure AD User	The user ljenkins@acmeorg.com has enabled email forwarding for ljenkins@acmeorg.com as a result of this action, it's important to immediately halt email forwarding as a result of this action.

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

Upgrade For Greater Security Coverage & Support

- **Additional integrations** across on-prem & cloud
- **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)
- **Advanced reporting & dashboards** to see security trends and send scheduled reports

Microsoft 365	Cloud	Advanced
Access full support & longer data retention.	Expand to cover popular cloud applications.	Full coverage across your entire environment.
MSP Price	MSP Price	MSP Price
Sign Up Today	Sign Up Today	Sign Up Today
<ul style="list-style-type: none">✓ 1 Cloud Integration - Microsoft 365✓ Unlimited Data Ingestion*✓ 30 Days Data Retention✓ Detections & Response✓ Advanced Reporting✓ Security Dashboards✓ Detection Rule Management✓ 24/7 Security Operations Team Support**	<ul style="list-style-type: none">✓ 3 Total Cloud Integrations - Microsoft 365, Duo Security, SentinelOne✓ Unlimited Data Ingestion*✓ 1 Year Data Retention✓ Detections & Response✓ Advanced Reporting✓ Security Dashboards✓ Detection Rule Management✓ 24/7 Security Operations Team Support**	<ul style="list-style-type: none">✓ Coverage For All On-Premises and Cloud Integrations✓ Unlimited Data Ingestion*✓ 1 Year Data Retention✓ Detections & Response✓ Advanced Reporting✓ Security Dashboards✓ Automated Response (Dynamic Blocklists)✓ Detection Rule Management✓ Honeypots✓ 24/7 Security Operations Team Support**

Paid: Microsoft 365 Edition

Get everything in Free, plus:

- **24/7 security operations team support** for urgent priority issues
 - Full security & tech support
 - Webinar access for M365 and Report Builder
 - Video tutorials & log ingestion troubleshooting article
- **Advanced reporting & dashboards** to see security trends (Responder, Manager & Security view) and send scheduled reports
- **30 days of data retention**, useful for a historical overview and investigation
- **Detection rule management** to see detailed rule analyses and toggle rules on/off to suit their organization's needs

Microsoft 365

Access full support & longer data retention.

MSP Price

Sign Up Today

- ✓ **1 Cloud Integration - Microsoft 365**
- ✓ Unlimited Data Ingestion*
- ✓ 30 Days Data Retention
- ✓ Detections & Response
- ✓ Advanced Reporting
- ✓ Security Dashboards
- ✓ Detection Rule Management
- ✓ 24/7 Security Operations Team Support**

Paid: Cloud Edition

Get everything in Microsoft 365, plus:

- **3 key cloud integrations** - Microsoft 365, Duo Security & SentinelOne
- **24/7 security operations team support** for urgent priority issues
 - Full security & tech support
 - Webinar access for M365, Duo, SentinelOne and Report Builder
 - Video tutorials for M365, Duo, SentinelOne
- **1 year of data retention**, ideal for meeting compliance & cybersecurity insurance requirements

Cloud

Expand to cover popular cloud applications.

MSP Price

Sign Up Today

- ✓ **3 Total Cloud Integrations - Microsoft 365, Duo Security, SentinelOne**
- ✓ Unlimited Data Ingestion*
- ✓ 1 Year Data Retention
- ✓ Detections & Response
- ✓ Advanced Reporting
- ✓ Security Dashboards
- ✓ Detection Rule Management
- ✓ 24/7 Security Operations Team Support**

Paid: Advanced

Get everything in Cloud, plus:

- **Unlimited integrations** for on-premises and cloud, including infrastructure (AWS), endpoint security, firewalls, servers, and more
- **1 year of data retention** for compliance, meeting cybersecurity insurance requirements & investigation
- **Dynamic blocklists** to immediately block threats
- **Honeypots** to detect lateral movement and unauthorized access attempts
- **24/7 security operations team support** for urgent priority issues
- Full security & tech support
 - Periodic network scanning via Shodan
- 3 one-on-one onboarding sessions with a TAM (Technical Account Manager)
- Webinar access for Microsoft 365, Duo, AWS, SentinelOne, Report Builder and troubleshooting log ingestion
- Video tutorials
- 1 network attack surface assessment
- Executive Sponsorship Program (ESP) only: Quarterly business reviews

Advanced

Full coverage across your entire environment.

MSP Price

Sign Up Today

- ✓ Coverage For All On-Premises and Cloud Integrations
- ✓ Unlimited Data Ingestion*
- ✓ 1 Year Data Retention
- ✓ Detections & Response
- ✓ Advanced Reporting
- ✓ Security Dashboards
- ✓ Automated Response (Dynamic Blocklists)
- ✓ Detection Rule Management
- ✓ Honeypots
- ✓ 24/7 Security Operations Team Support**