Blumira

# Easy, Effective SIEM + XDR for Lean IT Teams

# Agenda

01

**Blumira's Value**
How Blumira solves customer challenges.

02

**How Blumira Works**
Easy, effective and efficient detection and response.

03

# 01

# Blumira's Value

**CHALLENGES**

# Small & medium-sized businesses struggle to protect their organization against ransomware and breaches

## Time-Strapped

Managing security tools can require many manual tasks – threat hunting, managing rules, parsing data, developing integrations and more.

## No 24/7 Team

Small IT teams can't be fully staffed around the clock due to costly enterprise solutions, talent shortage and lack of security expertise.

## Complexity

Too many disparate solutions results in redundancies and lack of visibility into remote endpoint risks.

*"**I don't have the staff** dedicated to sit and read logs all day or with the **skillset to analyze our data**."*
*– Jim Paolicelli, IT Director, Atlantic Constructors*

Blumira

BLUMIRA'S VALUE

# Blumira's open XDR platform simplifies advanced detection and response for small and medium-sized businesses

## EASY

### Free up time & refocus efforts

Reduce reliance on humans to complete manual security tasks to achieve faster time to security

## EFFECTIVE

### Faster time to security

Accelerate breach prevention and ransomware protection with automated response

## EFFICIENT

### Satisfy compliance & gain more visibility

All-in-one open XDR + SIEM platform simplifies workflows & satisfies more compliance controls

*"I feel comfortable now that we don't have unknown activity happening on our network -- we now have **full visibility of our infrastructure**." – John Hwee, Director of IT, Duraflame*

Blumira

# Blumira delivers unique value to meet SMB needs:

Microsoft Azure · DUO SECURITY · SentinelOne

## ✓ FLEXIBILITY OF AN OPEN XDR

Open platform supports multiple vendors for hybrid coverage of cloud, endpoint, identity, servers and more

## ✓ AUTOMATION ACCELERATES SECURITY

Deploy in minutes; stop threats immediately with automated response to isolate devices and block malicious traffic

PCI DSS COMPLIANT · NIST · Federal Financial Institutions Examination Council · HIPAA COMPLIANCE

## ✓ MANAGED PLATFORM SAVES TIME

Blumira's team manages the platform to do threat hunting, data parsing and analysis, correlation and detection at scale

## ✓ SATISFY MORE COMPLIANCE CONTROLS

Get more in one – SIEM w/1 year of data retention, endpoint, automated response & 24/7 SecOps support*

*For critical priority issues

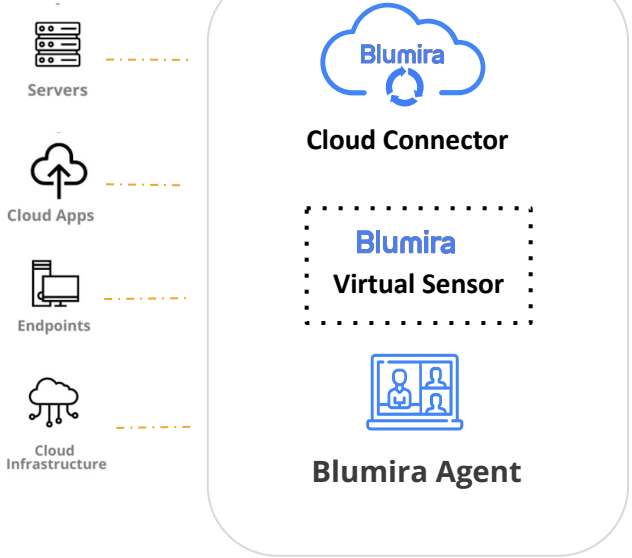
Blumira

# 02

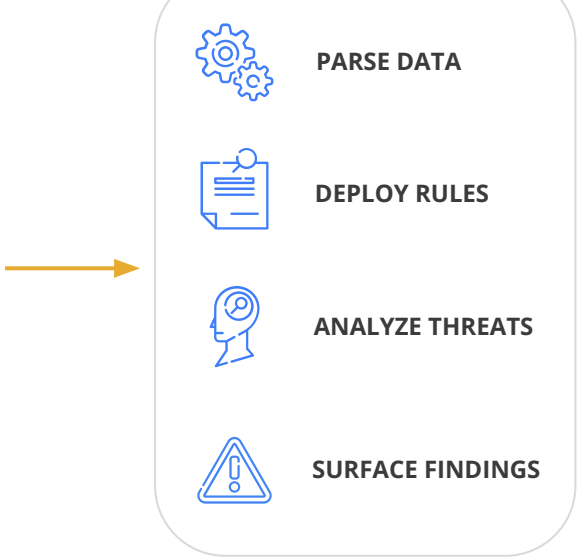
# How Blumira Works

## HOW IT WORKS

### 1. TECH CONNECTION + LOG COLLECTION




### 2. DATA TRANSFORMATION




### 3. AUTOMATED RESPONSE + SUPPORT


---

**One Year Data Retention**
*Satisfy compliance controls; extended retention available*

**Managed Detections**
*Pre-built detections identify advanced threats early; notifies in under a minute*

**24/7 SecOps Support**
*Extend your team with SOC support for critical priority issues*

**Response Playbooks**
*Simple step-by-step instructions for your IT team*

**Automated Response**
*Isolate threats immediately & automatically, at any time*

## Fast, Easy & Automated

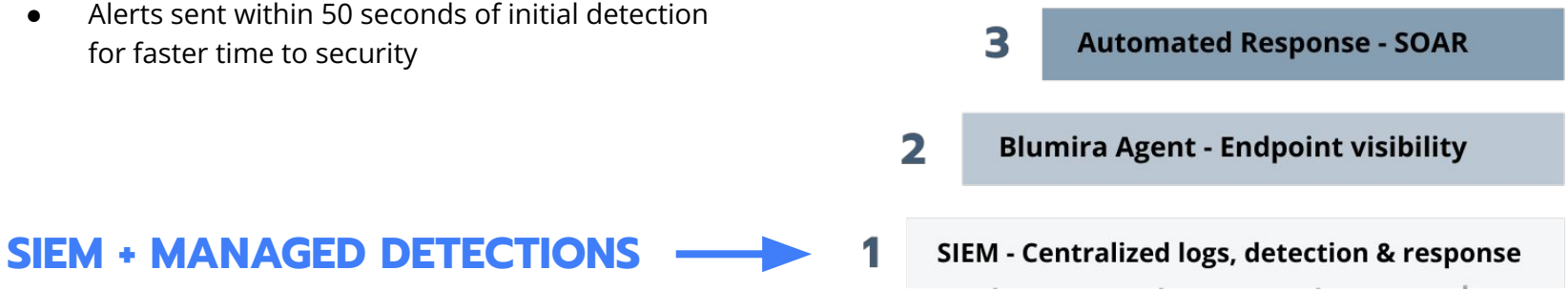
- Deployment is 5x faster than the industry avg.*
- Data is parsed, normalized, retained for 1 year
- Logs are automatically analyzed for threats

## Reduce Alert Fatigue

- All findings are prioritized by level of criticality (P1-P3)
- All correlated data are consolidated under initial findings and tuned or adjusted to reduce fatigue
- Alerts sent within 50 seconds of initial detection for faster time to security

## Fully Managed Detections

- Blumira engineers tune and develop new detections to automate threat hunting
- Platform updated regularly to protect against new threats
- Customers can filter alerts based on known safe activity to reduce noise



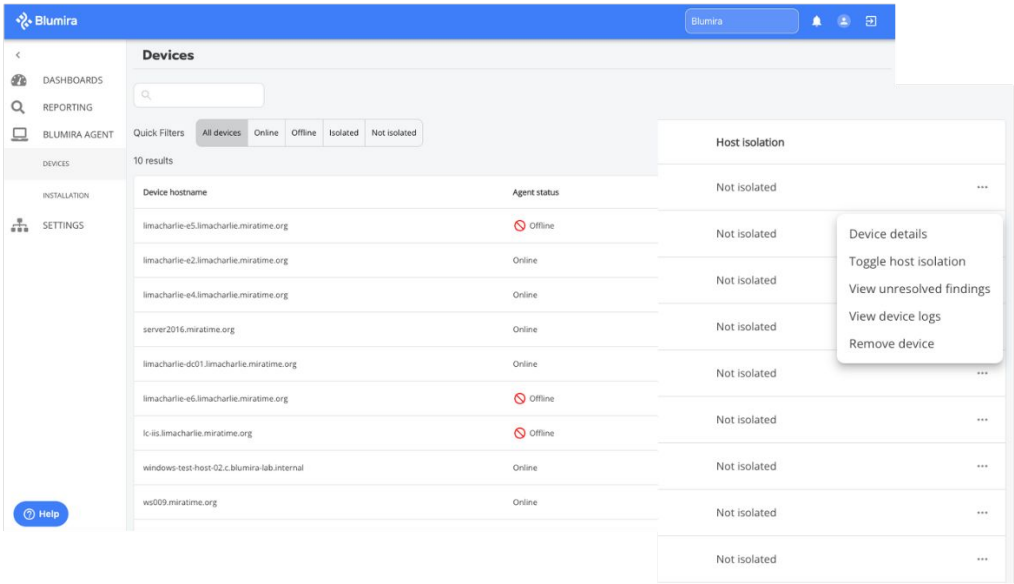

Blumira

## Support Remote Work

- Blumira Agent extends coverage to Windows endpoints located anywhere
- Fast, easy to deploy in minutes – no infrastructure required
- Lightweight, minimal impact to your environment

## Detect & Contain Threats Immediately

- Device/host isolation to automatically contain an identified threat
- Protect your network from a ransomware attack




**ENDPOINT VISIBILITY WITH BLUMIRA AGENT**

3 **Automated Response - SOAR**

2 **Blumira Agent - Endpoint visibility**

1 **SIEM - Centralized logs, detection & response**

Blumira

## Automated Host Isolation

- Blumira Agent immediately isolates an endpoint from your network when a critical threat is identified

## Automated Blocking

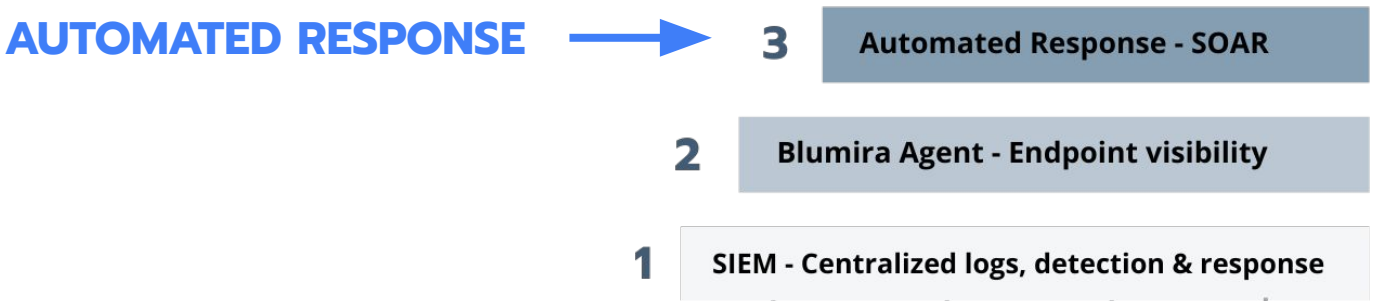
- Automatically block traffic from known malicious IP addresses
- Dynamic blocklists use updated threat feeds integrated with your firewall to identify threat sources

## Response Playbooks

- Automatically sent with every finding
- Guide your IT team through easy remediation steps

## 24/7 SecOps Support

- Access to a responsive security team for critical priority issues
- Get security guidance, onboarding help and answer any questions about findings




Blumira

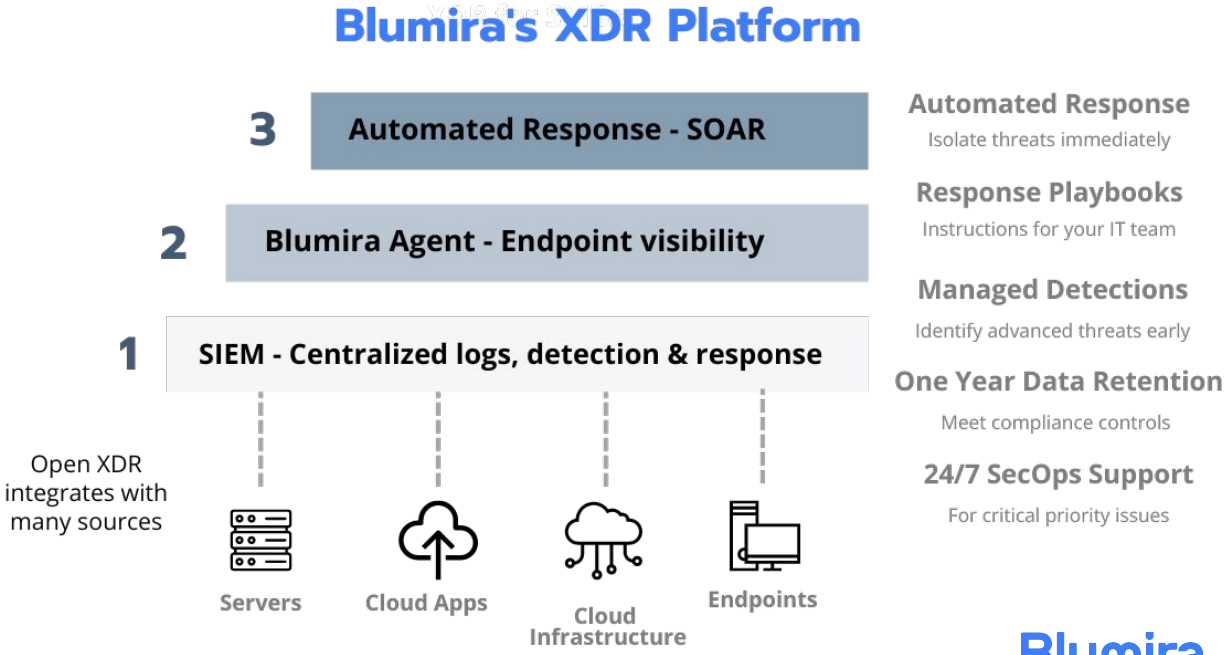
**BLUMIRA XDR PLATFORM**

# Blumira's open XDR platform simplifies detection & response, accelerating ransomware and breach prevention.

## EASY
Free up time & refocus efforts

## EFFECTIVE
Faster time to security

## EFFICIENT
Satisfy compliance & gain more visibility




Blumira

| Features | Free SIEM | SIEM Pro | SIEM + Endpoint Visibility | XDR Platform |
|---|---|---|---|---|
| **Data retention** | 14 days | 30 days | 1 year | 1 year + |
| **Cloud integrations** | Pick 3 | ✓ All | ✓ All | ✓ All |
| **Sensor integrations** | | ✓ All | ✓ All | ✓ All |
| **Logging & analysis** | ✓ | ✓ | ✓ | ✓ |
| **Managed detections & playbooks** | ✓ | ✓ | ✓ | ✓ |
| **Filter detections for noise** | | ✓ | ✓ | ✓ |
| **Blumira Agent / manual isolation** | | | ✓ 1/user + | ✓ 1/user + |
| **Automated host isolation / blocking** | | | | ✓ |
| **Honeypots** | | | ✓ | ✓ |
| **Dashboards & reporting** | Only basic | ✓ | ✓ | ✓ |
| **24/7 support critical issues** | | ✓ | ✓ | ✓ |

# 03

# Blumira Teams

# Blumira Dedicated Success Model

*Most onboarding takes between 2-8 hours; on average, 4 hours**

## Activate

- Host kickoff call
- Understand objectives, environment
- Provision / start deployment

## Onboarding

- Install sensors & agent
- Configure log sensors
- Validate installations
- 24/7 SecOps coverage begins

## Training

- Product training
- Dashboards & reporting
- Findings & playbooks
- Contacting support

## Follow-Ups

- Ongoing questions
- Scheduled sessions
- New log sources & integrations
- New contacts or changes

## Auto-Updates

- Release/tune new detection rules
- New feature & integration updates
- Continued improvements

## 24/7 SecOps

- Reach out with questions
- After hours help for critical priority issues
- Create reports, tune rules, etc.

*May vary depending on customer's environment

Blumira

# Blumira Dedicated Onboarding

*Blumira deploys 5x faster than other SIEM vendors (hours vs. months)*

| | Stage 1 | Stage 2 | Stage 3 | Operational |
|---|---|---|---|---|
| **Onboarding Stages** | **Discovery**<br>*60 minutes* | **Configuration**<br>*Time varies based upon requirements* | **Validation & Training**<br>*60-90 minutes, split into multiple meetings* | **Follow-Ups**<br>*30-60 minutes* |
| **Goals** | Determine what your top priorities are and what logging settings are needed | Begin configurations for log forwarding and API integrations | Validate configurations are working as intended; troubleshoot if needed | Provide ongoing support and answer product questions. Suggest Blumira feature requests or other product needs |

*Our dedicated Solution Architects (SAs) are with you every step of the way through deployment, validation and ongoing use.*

Blumira

# Blumira Customer Testimonials

*Our happy customers love Blumira's responsive & high-quality support*

The team has a lot to do with my satisfaction…your entire support team has been awesome. They are willing to go out of their way for you. Every time I open a ticket or have any other type of interaction – the experience has been great. **Blumira is at the top of the list when it comes to customer support.**

*Frank DeLuca, President, CTO Agency*

**Your support team has been fantastic** and will follow through until the ticket is closed. **They are very responsive, genuine, and understanding**. Even if it's something on my side, they are still willing to lend a hand. That means a lot – that means keeping a customer as well.

*Christopher Reddekopp, Level 2 Support, TUA*

I was able to [deploy Blumira] myself about 90% within an afternoon – and then **Dave (Blumira's dedicated Solution Architect) stepped in to help** tweak things as well. It was easy to set up our integrations using Blumira's excellent documentation.

*Jim Paolicelli, IT Director, Atlantic Constructors Inc.*

It's easy to use the portal, and **Blumira's team is quick and helpful to add rules and help with detection.** I like that I can get text notifications of higher risk findings. Being on a small team without the time to watch the application constantly, that can be helpful.

*Ethan Shutika, Director of IT & Security, Nittany Oil*

Blumira

# The Blumira Teams That Work as an Extension of Your Own

*Blumira is dedicated to your security success*

## Security Operations Analysts (SecOps)

**The SecOps team is a dedicated group of security experts who are on standby** to help you tailor Blumira security detections for your specific needs, help you understand the security findings that Blumira generates for your review, and support you 24/7 in the event of a critical security issue.

## Technical Support Analysts

**Our Technical Support Analysts support you in troubleshooting** any issues you may experience with the Blumira platform and work with our Product and Engineering teams to advocate for Blumira feature additions and usability enhancements, based on the insights you share with us.

## Dedicated Solutions Architects (SAs)

**Your Solutions Architect is a dedicated partner who sets you up for success** with Blumira. They support you with your product integrations and onboarding and then check in with you on an ongoing basis to ensure that you're learning about new features as they're added to your package and looking for opportunities to improve your security.

## Incident Detection Engineers

**The incident detection team at Blumira writes detection rules** that power Blumira's platform to help identify indicators of compromise early and often for our customers.

Lead Incident Detection Engineer Amanda Berlin is a highly accomplished network defender, author of "Defensive Security Handbook: Best Practices for Securing Infrastructure" with Lee Brotherston, published by O'Reilly Media.

Blumira

# Additional Product Information

# A Typical Day in the Life

*Of an IT Person Using Blumira for Detection and Response*

## 24/7 Monitoring

After deployment and integration with your tech stack, Blumira is monitoring and analyzing your logs, 24/7.

## Detect An Attack

The platform detects something unusual in your environment and sends an alert in under a minute of initial detection.


## Fast Notification

Your IT person gets pinged immediately through their choice of notification – email, text or phone call.

## Prioritized Alerting

The finding is prioritized by level of criticality (P1-P3), so your IT person knows how to respond accordingly.

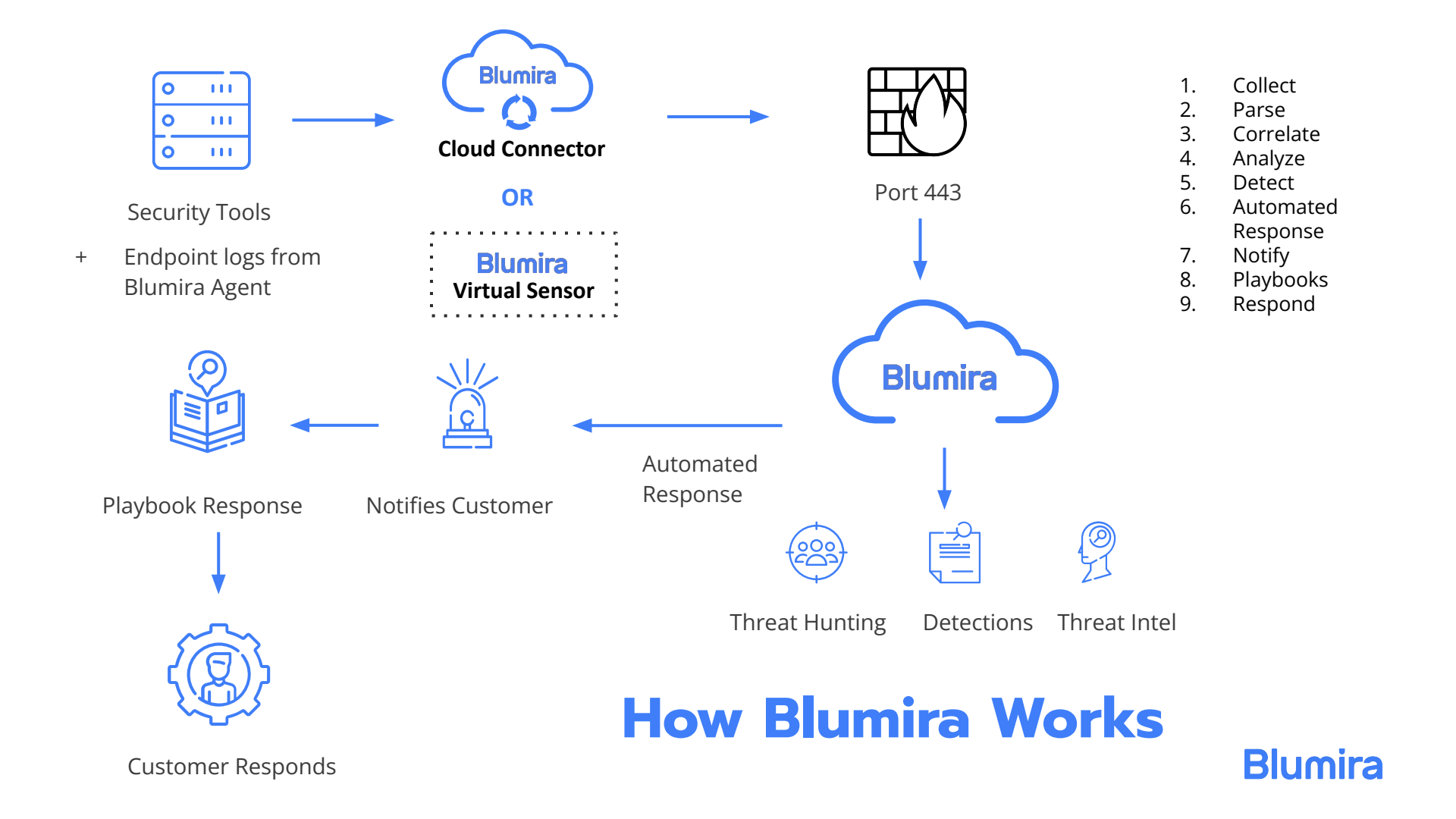
## Guided Response

Within the finding, Blumira provides a description of what happened and a playbook to guide your IT person through response.

## 24/7 SecOps

If your IT person has a question, they can send a message in-app to Blumira's SecOps team 24/7 to help with critical priority issues.

Blumira




# How Blumira Works

Blumira

# Open XDR Integrates With Any Service

| | |
|---|---|
| Cloud Infrastructure | Microsoft Azure, Azure Active Directory, okta, DUO SECURITY, aws |
| Endpoint | Carbon Black., SentinelOne, CROWDSTRIKE, SOPHOS, Malwarebytes, TREND MICRO, eset, Symantec, BlackBerry CYLANCE |
| Productivity | Microsoft 365, G Suite, proofpoint, Cisco Umbrella |
| Host | Windows Server, Windows, Active Directory, Linux |
| Firewall | paloalto NETWORKS, FORTINET, cisco, Meraki, Check Point SOFTWARE TECHNOLOGIES LTD., SOPHOS, CITRIX, WatchGuard |

*See complete list of integrations at [blumira.com/integrations](blumira.com/integrations)*

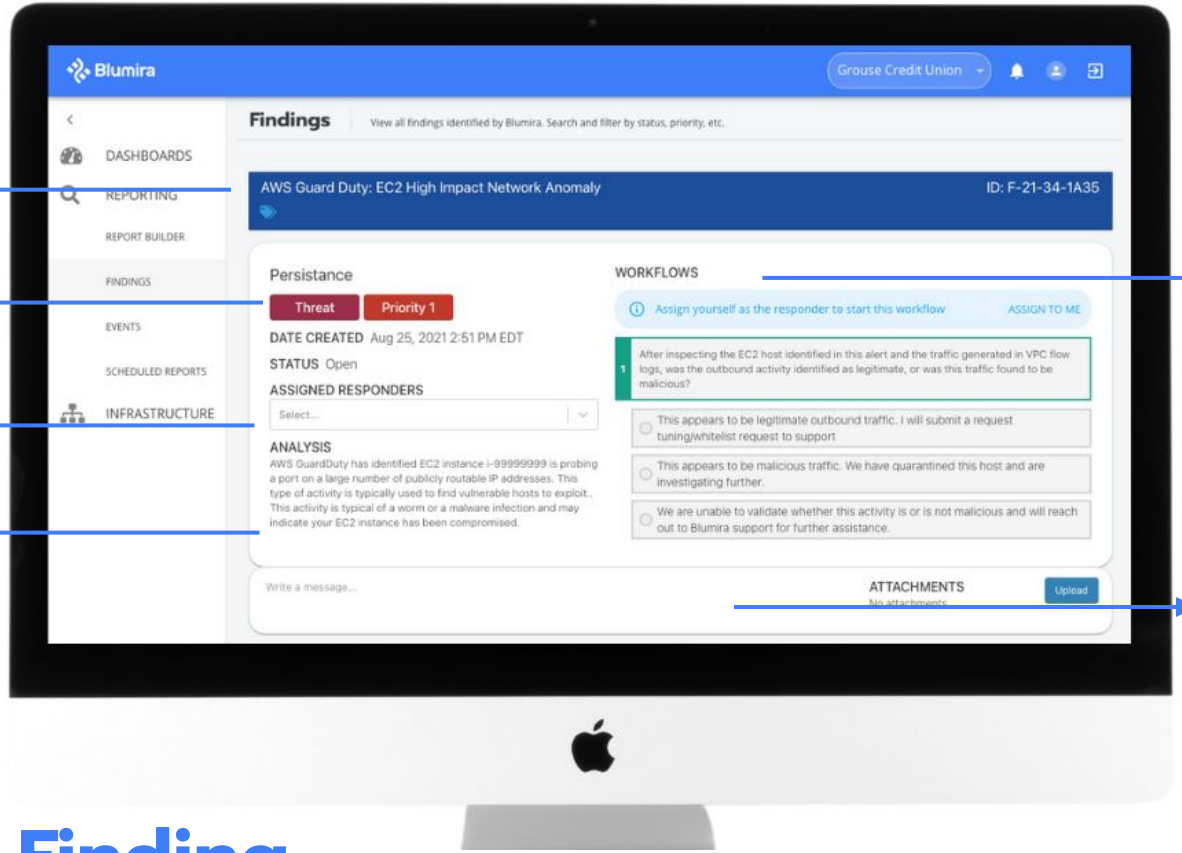
Blumira

# Open XDR Integrates With Any Service

| | |
|---|---|
| Additional Integrations | osquery, APACHE, NGINX |
| | MacOS, FORESCOUT, PhishER |
| | mimecast, vmware® |
| | logstash, LastPass, Windows Defender |
| | |

*See complete list of integrations at [blumira.com/docs](blumira.com/docs)*

Blumira




Security Finding

Threat Level

Assign Responder

Threat Analysis

Response Playbooks

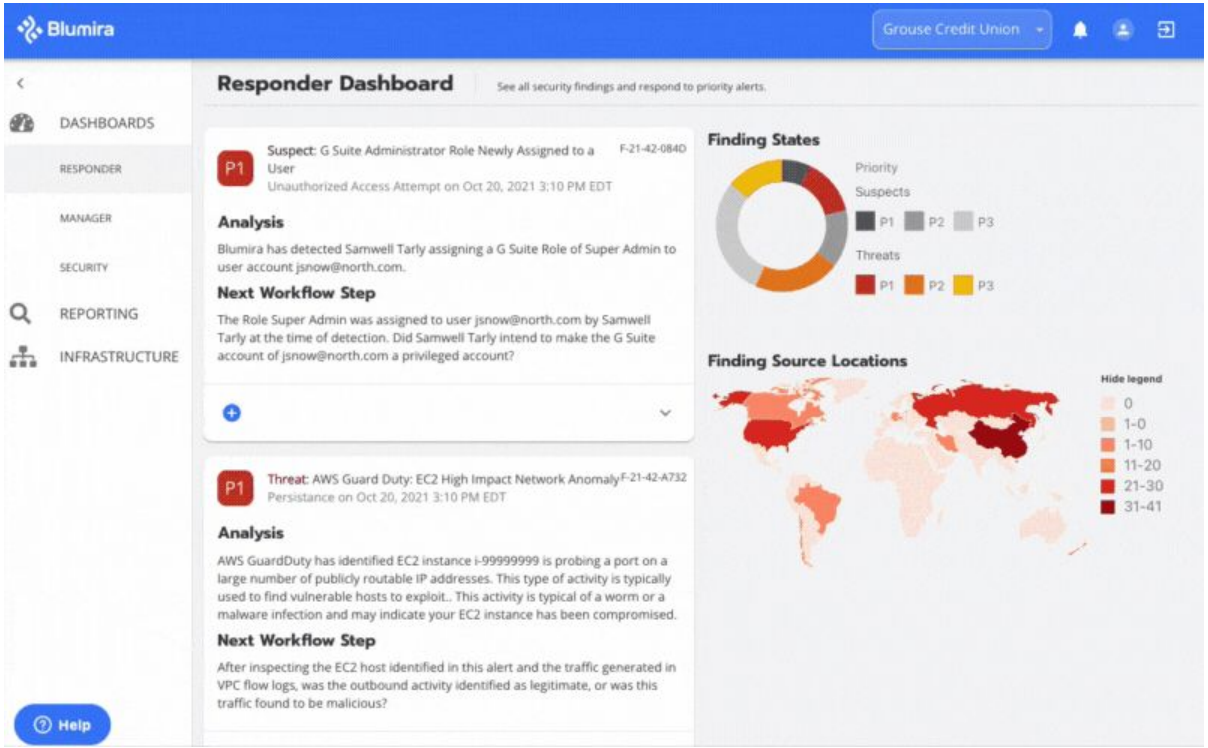
Ask an Expert

# Example Finding

Blumira

# See Blumira's XDR Platform in Action

*Automated extended threat detection & response*

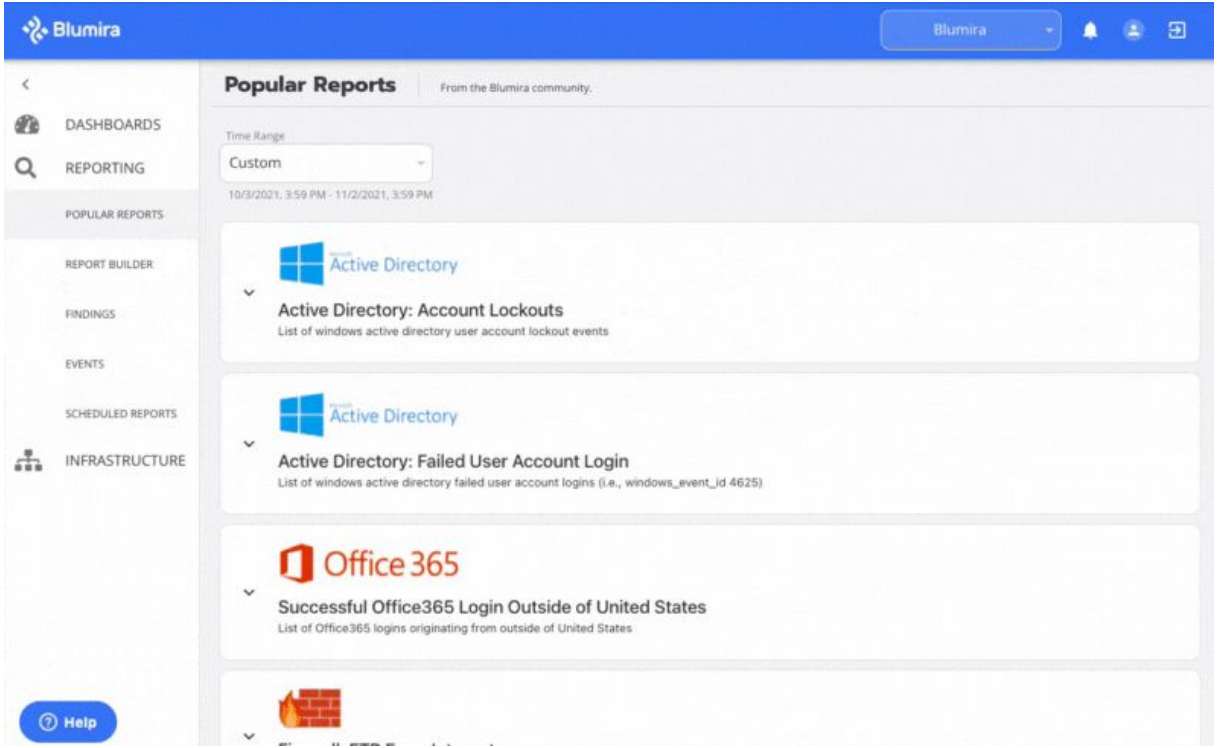



- Prioritized findings give you a full analysis of the threat
- Workflows for every finding tell you how to respond
- Correlated data sent with findings to help with investigation

Blumira

# See Blumira's XDR Platform in Action

*Easy-to-Use Security Reports With Click-Through Dashboards*




- Scheduled security reporting is included
- Drill down into account lockouts, failed user logins and more
- Click-through dashboards provide customizable search through your data, filtered by data source

Blumira

# Try Blumira

***Sign up for Blumira's Free SIEM***
*Unlimited users and data, no credit card or special licensing required.*

***Contact us for an XDR trial***
*Try out the XDR platform today!*

*Visit **blumira.com/free** to start.*




Blumira