

## Blumira's Detection & Response

### BUILT FOR SM(ALL) TEAMS

Breaches and ransomware are increasing, as small teams struggle to acquire defenses and meet compliance requirements



#### RISING RANSOMWARE

Ransomware attacks have doubled in the past two years, increasingly targeting SMBs\*



#### SLOW RESPONSE

Average time to detect & contain a breach is 287 days, resulting in 35% higher costs -- on average, \$4.8 million\*\*



#### STRICTER COMPLIANCE

New data regulations, including cyber insurance, require SIEM and one year of log data retention

*SMBs need security to meet compliance & reduce risk – but traditional tools today fail them.*



#### TOO COMPLEX

Security solutions today are built for large enterprises with big budgets and big teams with advanced security expertise



#### LIMITED RESOURCES

Require add'l infrastructure, security skills, months to get operational – teams stretched too thin between IT & security tasks



#### TIME CONSTRAINTS

Too many alerts to comb through to find real threats delays critical response time – threats go unnoticed, resulting in breaches

## THE BLUMIRA VALUE

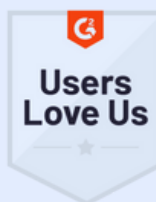
Get easy, effective security your team can actually use to defend against breaches and ransomware, while meeting compliance and cyber insurance requirements.

Blumira's **all-in-one** SIEM combines logging with automated detection and response for better security outcomes.



**Blumira does the heavy lifting** to pare down the overwhelming amount of data from logs into actionable events. That allows us to focus on revenue-enhancing activities.

Michael Cross, CIO  
Greenleaf Hospitality



VOTED #1 SIEM ON G2

- MOMENTUM LEADER
- BEST ROI
- EASIEST TO USE
- LIKELY TO RECOMMEND

# Blumira

## HOW DO WE DO THINGS DIFFERENTLY?

Meet compliance controls, save time on security tasks, focus on real threats and protect against a breach faster than ever -- with Blumira.



### AUTOMATE TASKS FOR YOU

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.



### 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.



### EASILY MEET COMPLIANCE

With a year of data retention and deployment that takes minutes to hours, we help you meet cyber insurance and compliance easily and quickly with the team you have today.

COMPARED TO THE INDUSTRY AVERAGE, BLUMIRA'S PLATFORM HELPS YOU DETECT AND RESPOND TO THREATS 99.4% FASTER, HELPING YOU SUCCESSFULLY AVOID A BREACH.\*

*Easy setup  
in hours!*

#### 1. USER ONBOARDING & LOG TRANSMISSION



FREE SIGN UP



COLLECT LOGS

#### ALL-IN-ONE SOLUTION: SIEM + DETECTION & RESPONSE

#### 3. THREE-STEP RESPONSE



BLOCK THREATS



PLAYBOOKS



SECOPS SUPPORT

*Blumira does  
all the heavy  
lifting for you.*

#### 2. DATA PROCESSING & THREAT DETECTION



PARSE DATA



DEPLOY RULES



ANALYZE THREATS

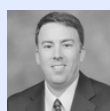


SURFACE FINDINGS



I don't have the staff dedicated to sit and read logs all day or with the skillset to analyze our data. **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



## BLUMIRA FREE EDITION

Protect your Microsoft 365 environment in minutes!  
Sign up free (no credit card required) to get:

- Cloud SIEM with detection & response
- Automated detection rules applied
- Playbooks on how to respond to threats
- Security reports to see risk trends

**SIGN UP FREE**