



Blumira

**Automated Threat
Detection & Response**

Agenda

01

Blumira Security Value

Addressing the biggest challenges in infosec.

02

3-Step Rapid Response

How Blumira enables faster response times.

03

How Blumira Works

Blumira offers fast time to security with wide coverage.



MISSION

Only Blumira makes threat detection and response **easy & effective for SMBs and the mid-market.**

01

Blumira Security Value



Blumira

MARKET CONDITIONS

Breaches & ransomware increase, as SMBs struggle to both acquire defenses and meet compliance requirements



Rising Breaches

SMB attacks are increasing - **breaches rose 68% in 2021**, with threats going undetected for months



Slow Response

Average time to detect & contain a breach is 287 days, resulting in **35% higher costs overall**



Stricter Compliance

New data regulations, including cyber insurance, require SIEM and 1 yr of log retention

SMB PROBLEMS

SMBs need SIEM, detection & response to meet compliance – but tools today fail them.



TOO COMPLEX

Security solutions are built for large enterprises with big teams



LIMITED RESOURCES

Require add'l infrastructure, security skills, months to get operational

Small teams stretched too thin between IT & security tasks



TIME CONSTRAINTS

Too many logs and alerts to comb through to find real threats delays critical response time

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

*"We can't **monitor** all of our logs — we would need a team of 100 to go through all of these logs manually."*

*"Other **tools** are noisy; we don't have time to dig through layers and layers of data."*

BLUMIRA SOLUTION

Blumira delivers unique value specifically suited to SMB needs, differentiating from competitors with:

✓ FASTEST TIME TO SECURITY

Easy deployment by IT admins in minutes to hours; not weeks or months

✓ REDUCED NOISE, FOCUS ON CRITICAL THREATS

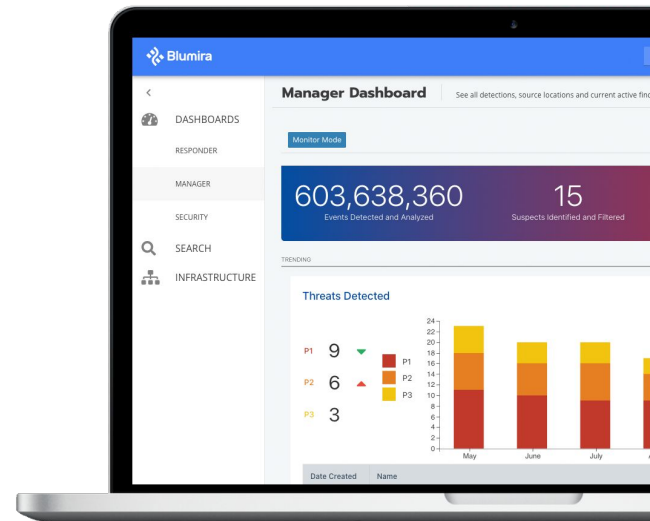
Behavior-based detections reduce noisy alerts; catch threats other tools miss

✓ EFFECTIVE THREE-STEP RESPONSE

Automated response, playbooks & SecOps support; competitors lack response

✓ DOES ALL THE HEAVY LIFTING

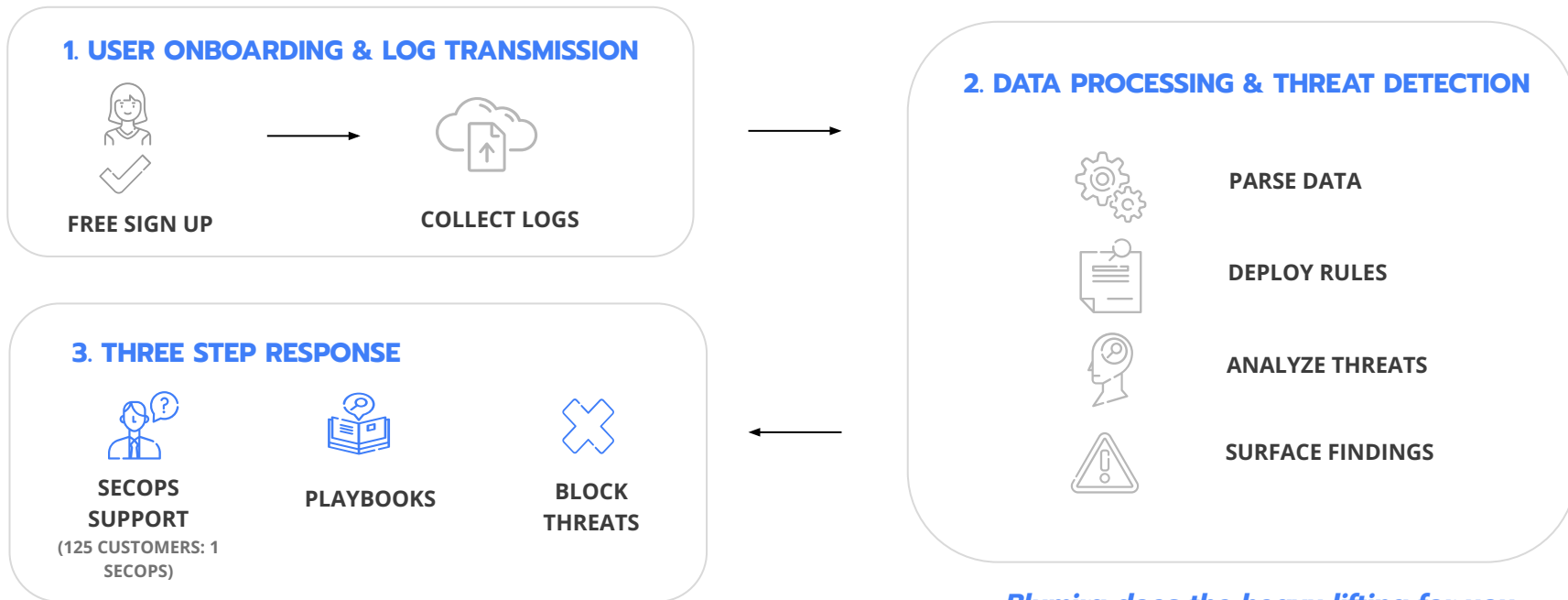
Parsing, integrations, correlation, analysis, rule tuning; Blumira takes care of it all



"Blumira provides expertise in understanding alerts. With a limited staff, it's important that someone has my back." – Kevin Hayes, CISO, Merit Network

HOW IT WORKS *"The perfect SIEM; up & running in one hour"*

Blumira analyzes threats with faster resolution to prevent a breach



Blumira does the heavy lifting for you.

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

Time to Detect

212 days

Industry avg. time to detect a breach



Blumira

99.4% faster

32 min

Blumira's average time to detect a finding



Blumira's platform is highly effective, resulting in better security outcomes vs. competitors

Time to Respond

75 days

Industry avg. time to respond to a threat



99.4% faster

6 hours

Average time to respond (customer closed a finding)



Resources – staff, cost, infrastructure, time – required to set up and maintain it are lower than competitors

(Source: 2021 Cost of a Data Breach)

(Source: Blumira's 2021 dataset)

Blumira

BLUMIRA IMPACT

With Blumira, SMBs realize greater security benefits:

✓ TIME & RESOURCES SAVED

On deployment, onboarding, integration setup, parsing, writing detection rules and manual security tasks; more time spent on strategic initiatives

✓ BETTER RESPONSE TIMES

Real-time detections delivered in 50 sec; prioritized alerts & 3-step response stop attacks in progress faster to prevent ransomware & breaches

✓ IMPROVED THREAT DETECTION

Blumira's detection engineers focus on threats other tools miss, researching and updating the platform regularly so SMBs don't have to

✓ EASILY MEET COMPLIANCE & CYBER INSURANCE

Faster deployment, less resources and headcount needed to meet compliance & cyber insurance policy requirements for SIEM, log review, data retention, etc.

"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, Chief
Information Officer
Greenleaf Hospitality*

PRODUCT CAPABILITIES *"Automated detection & response game changer!"*

All-in-one solution for easy detection & response

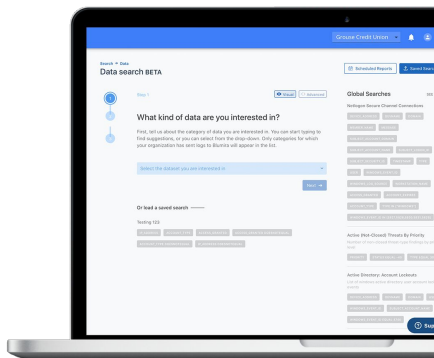
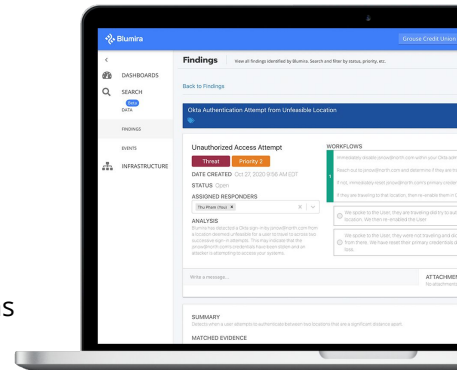
50+ INTEGRATIONS

- Hybrid coverage for on-prem & cloud
- Ideal for Microsoft environments
- Easy setup for IT



SIEM + DETECTION & RESPONSE

- Centralize all log data from different sources (endpoint, servers, identity) into one platform
- Logs are analyzed for real attacker behavior to surface meaningful findings
- All relevant data and playbooks guide small teams through fast, easy threat response



REPORTS & SECOPS SUPPORT

- One year of log data retention to meet compliance & cyber insurance policies
- Pre-built global reports; ability to customize & schedule
- Manager, Responder & Security dashboards
- 24/7 SecOps team support for critical issues

02

Rapid Response in 3 Steps



Blumira

Security Outcome: Rapid Response



The faster you resolve an incident, the lower the impact.

\$1.12 million

*Saved if breach is detected & contained in less than 200 days**



**Best
Results**

Mid-Market

**SPRING
2022**

Blumira delivers fast resolution in three steps:

1. **Automated response**
2. **Playbooks for every alert**
3. **A live security expert**

1. Automated Response

Block threats immediately

Get the fastest response times by blocking known threats automatically through Blumira's platform, reducing manual remediation.



Best Results

Mid-Market

SPRING
2022

Merit uses Blumira's automated blocklists paired with their Palo Alto firewall integration to protect against malicious activity.

"There's a few checks and balances in Blumira's platform to ensure that you have some control, in addition to providing **automated threat response.**"

- CISO Kevin Hayes, [Merit Network](#)

merit

NETWORK. SECURITY. COMMUNITY.



The screenshot shows the 'Blocklists' management page in the Blumira interface. At the top, there's a blue header with the title 'Blocklists' and a subtitle 'Manage your organization's blocklists and threat feeds.' Below this is a 'Configure' button. A green dot indicates the feature is 'Enabled' since August 2022. The main content area lists three blocklists: 'Blumira Domain Blocklist', 'Blumira IP Blocklist', and 'Blumira URL Blocklist', each with a corresponding URL input field containing 'https://storage.googleapis.com/blumira...'. At the bottom, there's a search bar and an 'Add IP Entry' button. A table below shows a list of IP addresses with columns for 'IP', 'Negating', 'Automated', and 'Community'. The first row shows the IP '144.76.109.56'.

Blumira

2. Playbooks

Guided, faster response

Get playbooks for every finding written by security experts for step-by-step instructions on how to respond -- easy for anyone to understand.



Easiest
To Use

SPRING

2022

"I like that you not only provide good details on findings, but also **suggestions on what to do about them**. With our previous solution, it would often be 24 hours before we would receive alerts from our partner and we had to do a lot of manual analysis."

- Senior Systems Analyst Bryan Allen, [LTU](#)

Lawrence
Technological
University



WORKFLOWS

1

Immediately disable user within your G Suite admin console.

Reach out to user and determine if they are traveling.

If not, immediately reset user's primary credentials.

If they are traveling to that location, then re-enable G Suite.

We spoke to the User, they are traveling and have not yet authenticated from that location. We then spoke to the User

We spoke to the User, they were not traveling. We had them not try to authenticate from there. We have reset their primary credentials due to likely credential compromise.

3. Security Experts

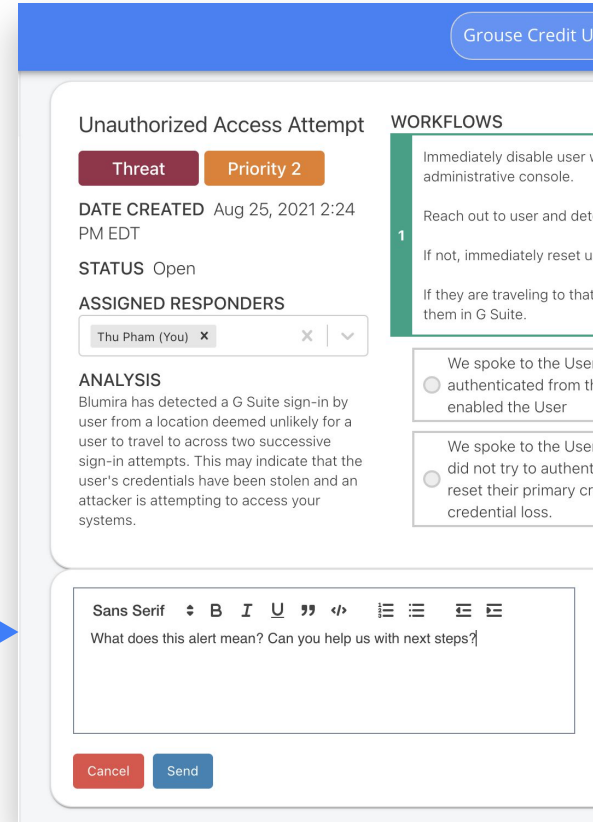
Extend your security team

Our experienced and responsive security team is on standby to help answer questions, triage and assist with incident response. We continuously help improve your overall security posture.



"To be able to pay for a service and have pretty much a **SOC team behind you** to support you -- it definitely gives me a good night's sleep."

- IT Manager Ronnie Baker, [Burcham Hills](#)



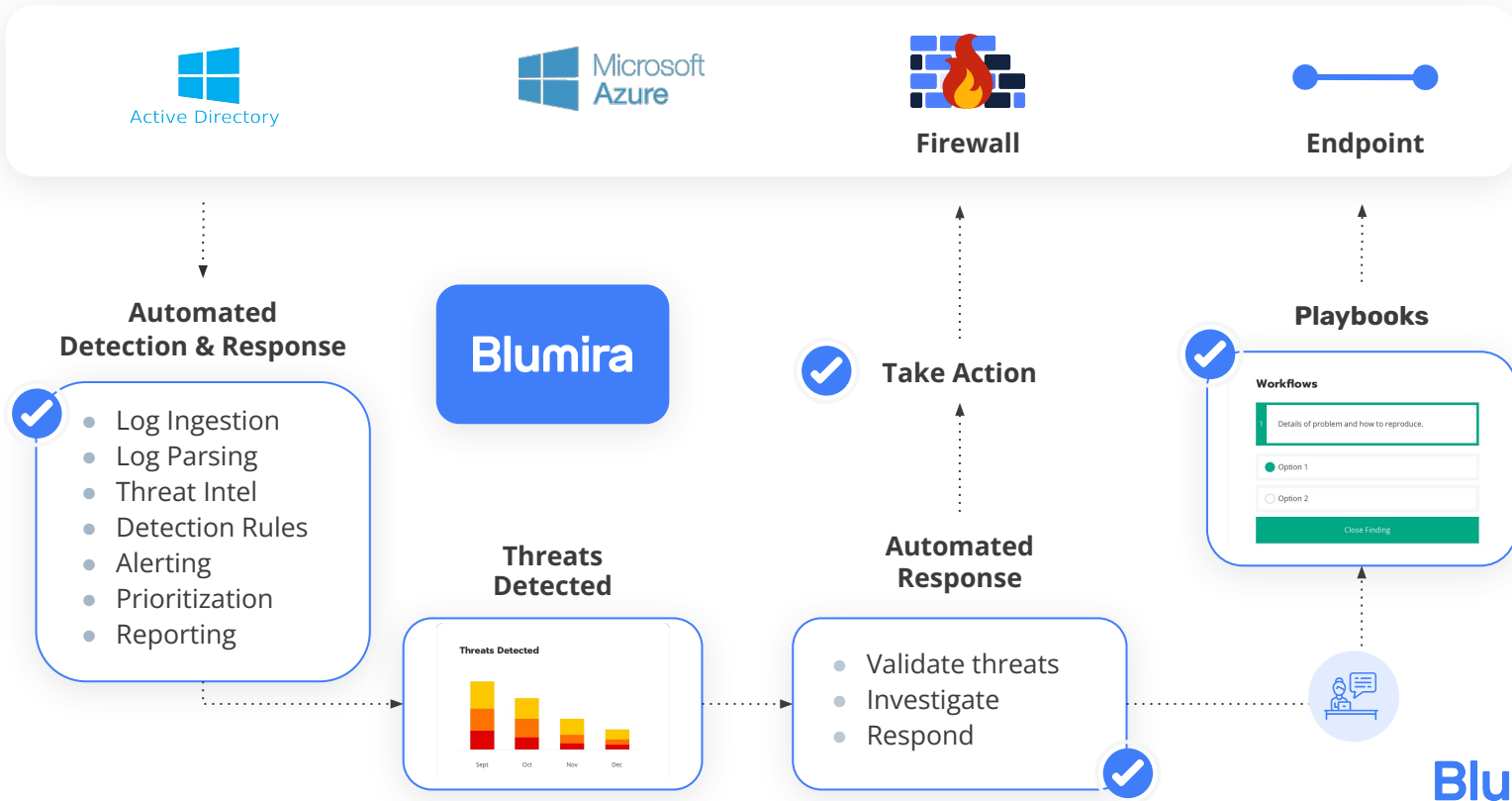
03

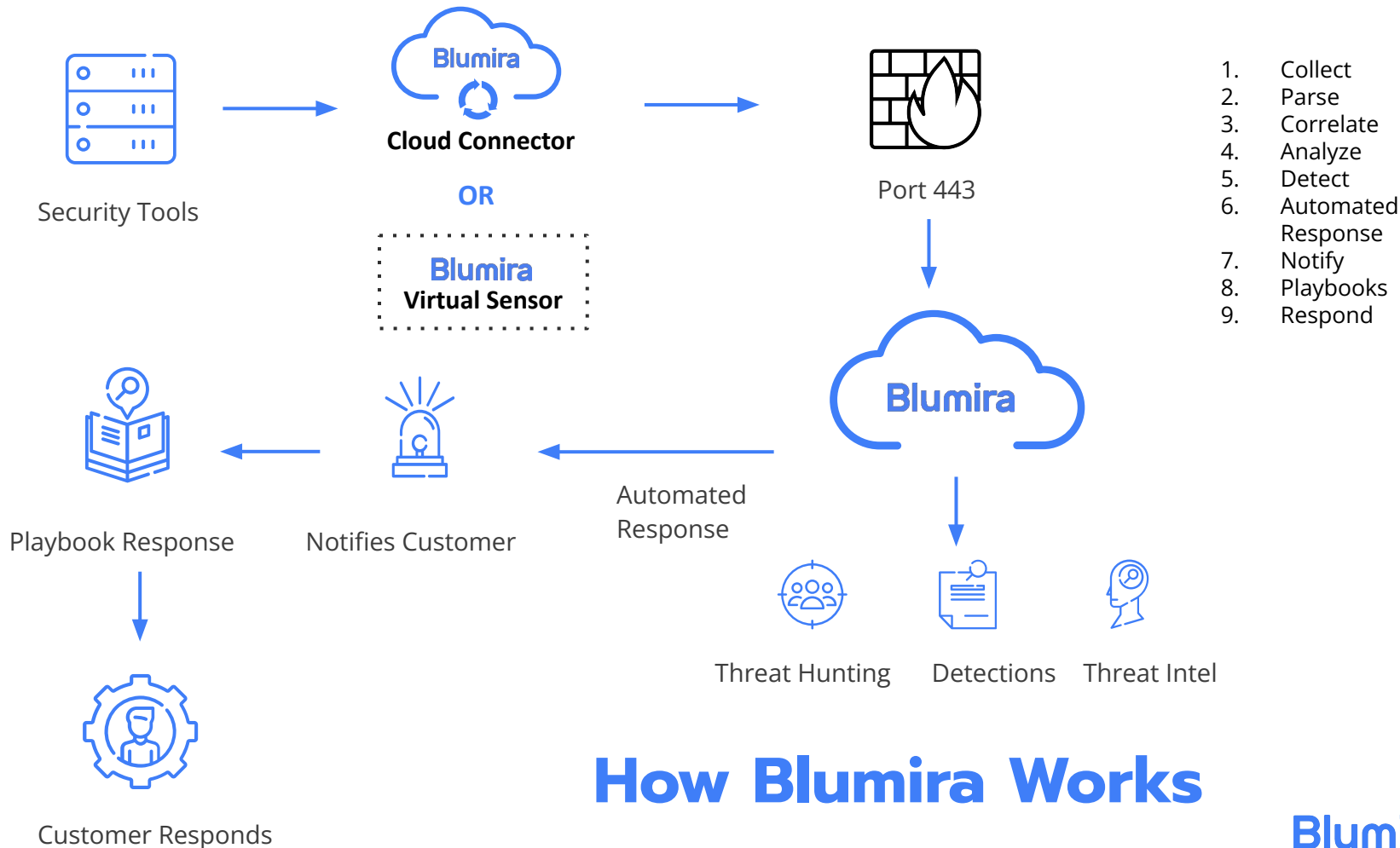
How Blumira Works



Blumira

Blumira's Detection & Response





1. Collect
2. Parse
3. Correlate
4. Analyze
5. Detect
6. Automated Response
7. Notify
8. Playbooks
9. Respond

How Blumira Works

Fast, Easy Security Made for IT Teams

Blumira is 5x faster than industry average to deploy – set up in minutes vs. months.

We take care of all SIEM setup, automating tasks for our customers:

- Data parsing across integrations
- Fine-tuning to reduce noise & alert fatigue
- Rule development for latest threats
- Finding analyses & gathering data
- Prioritizing findings by severity (P1-P3)

“Blumira’s demo and free trial period **gave us a lot of value and was pretty easy** to do. The total process took 3-4 hours to get fully functional.”

– John Hwee, Director of IT, [Duraflame](#)

duraflame



Blumira











Blumira 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.  FORCEPOINT  cisco. 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/docs

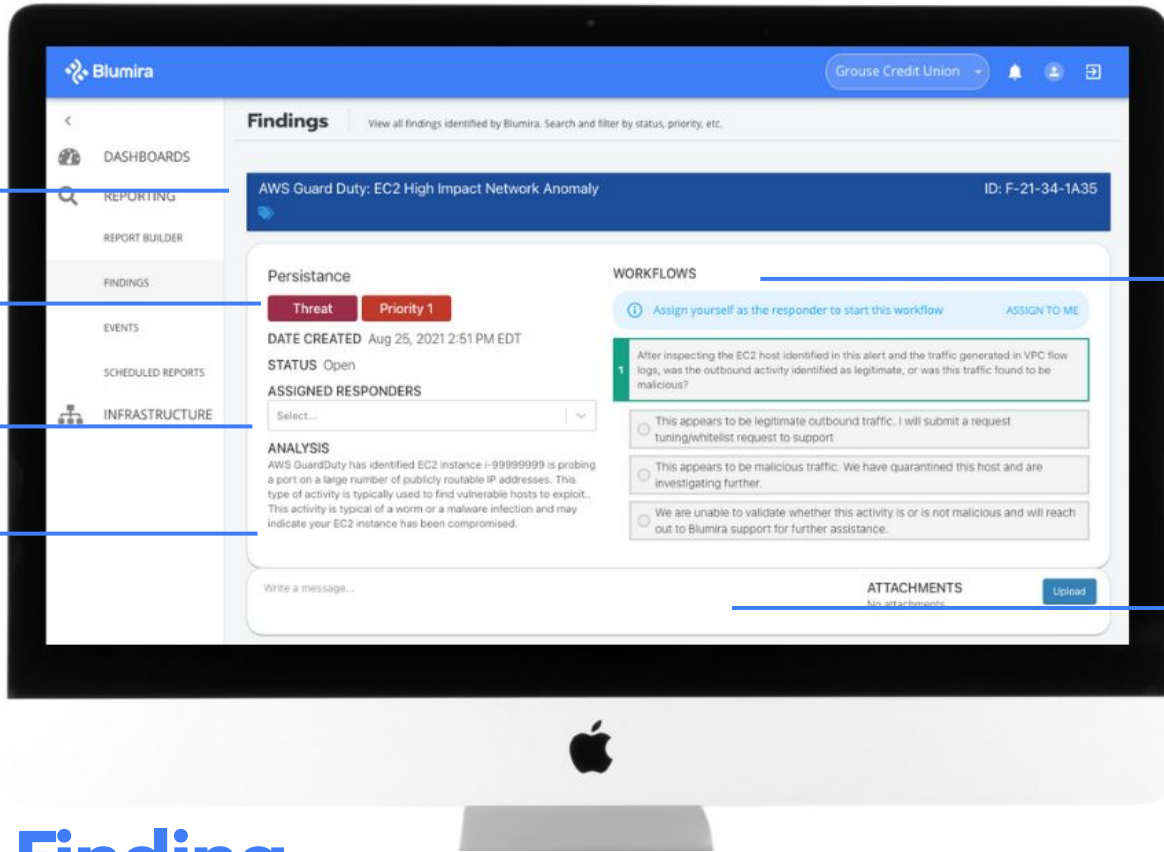
Blumira

Blumira Integrates With Any Service

Additional Integrations	 osquery  APACHE 
	 MacOS  FORESCOUT 
	 proofpoint 
	 logstash  LastPass 

See complete list of integrations at blumira.com/docs

Blumira



Security Finding

Threat Level

Assign Responder

Threat Analysis

Response Playbooks

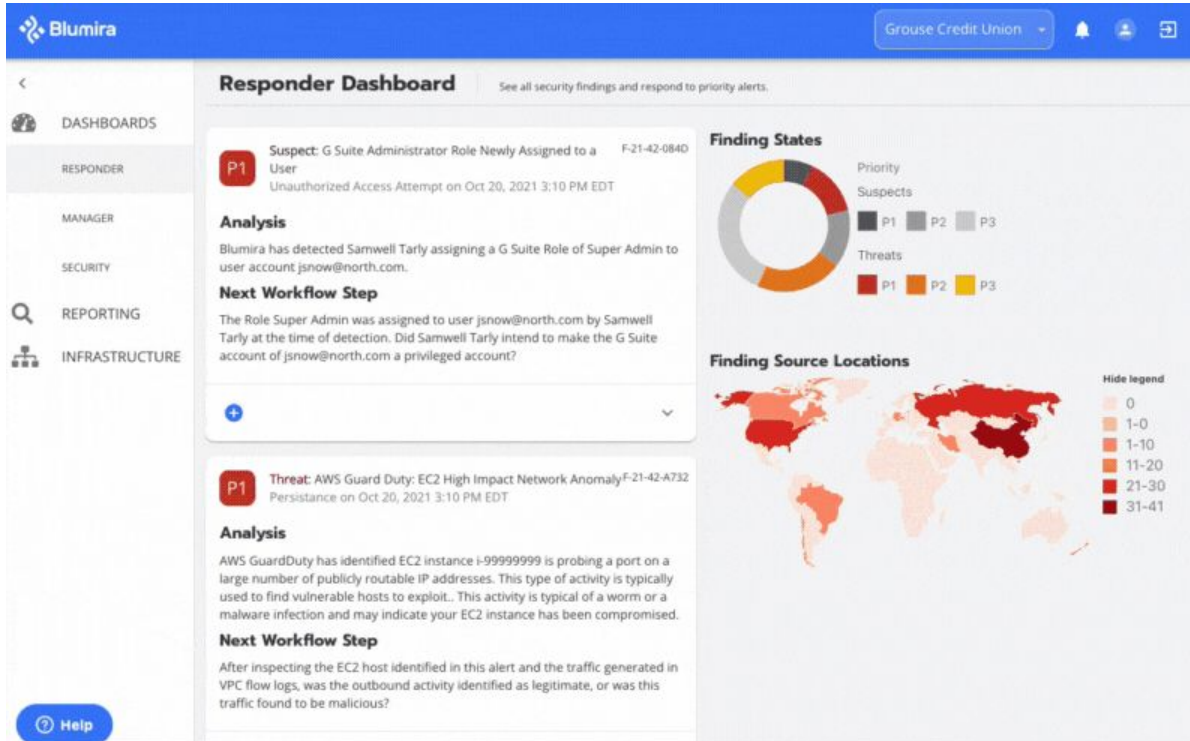
Ask an Expert

Example Finding

Blumira

See Blumira in Action

Actionable, automated threat detection & response



- Meaningful findings give you a full analysis of the threat
- Workflows for every finding tell you how to respond
- Matched evidence gives you related information to help with investigation

See Blumira in Action

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

The screenshot displays the Blumira dashboard interface. At the top, there is a blue header with the Blumira logo and a search bar containing the text 'Blumira'. Below the header, a navigation sidebar on the left lists various sections: DASHBOARDS, REPORTING, POPULAR REPORTS, REPORT BUILDER, FINDINGS, EVENTS, SCHEDULED REPORTS, and INFRASTRUCTURE. The main content area is titled 'Popular Reports' and includes a 'Time Range' filter set to 'Custom' for the period 10/3/2021, 3:59 PM - 11/2/2021, 3:59 PM. Three report cards are visible, each with a dropdown arrow and a brief description of the data it contains:

- Active Directory: Account Lockouts**
List of windows active directory user account lockout events
- Active Directory: Failed User Account Login**
List of windows active directory failed user account logins (i.e., windows_event_id 4625)
- Successful Office365 Login Outside of United States**
List of Office365 logins originating from outside of United States

A 'Help' button is located at the bottom left of the sidebar.

- 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

Sign Up Free!

*Sign up for Blumira's Free edition for Microsoft 365:
Unlimited users and data, no credit card or special
licensing required.*

Visit blumira.com/free to start.



Blumira

Security Gap Assessment

A woman with curly hair is sitting at a desk, smiling, with her arms crossed. She is wearing a light-colored top. In the background, another person is standing and talking, but they are out of focus. The entire image has a blue overlay.

Before vs. After Blumira













Scoring your current security posture - where are your gaps today?

Before Blumira	Score
Logging	0/6
Threat Detection	4/12
Alerting	1/6
Audit / Compliance	0/7
Response	0/4
Monitoring	0/3















Blumira	Score
Logging	6/6
Threat Detection	12/12
Alerting	6/6
Audit / Compliance	7/7
Response	4/4
Monitoring	3/3









Assessment: Logging

Current	Blumira	Capability
		Centralized security/audit log repository
		Security/audit log retention for 365 days
		Logs are automatically parsed and correlated
		Windows hosts have verbose security logging enabled
		Security logs are centrally collected for on-premises applications
		Security logs are centrally collected for cloud applications













Assessment: Threat Detection

Current	Blumira	Capability
		Central monitoring for threats across your environment
		Endpoint detection capabilities
		Correlated third-party threat intelligence to detect threats
		Automated matching of event and threat information
		Lateral movement detection through a honeypot
		Active detection of threats at border gateways & firewalls
		Detection of common misconfigurations (internet-accessible RDP or SMB)















Assessment: Threat Detection, Cont.

Current	Blumira	Capability
		Active detection for indicators of data exfiltration
		Active detection for identity attacks such as password spraying and/or credential compromise
		Phishing / DNS site detection









Assessment: Alerting

Current	Blumira	Capability
		Alerts are provided from your existing security tools
		Alerting is centralized and stacks evidence to reduce alert fatigue
		Only actionable threats are surfaced to reduce the noise of non-actionable information
		Alerts are prioritized cross-platform, based on severity
		Responders are notified out of channel (phone call/SMS) in case a communication system is compromised
		Alerts provide direct link back to evidence, threat details and actionable playbooks on how to respond







Assessment: Audit/Compliance

Current	Blumira	Capability
		Easily generate audit reports
		Access to pre-built reports available for audit / compliance purposes
		Scheduled delivery of recurring audit/compliance reports
		Offsite retention of your security/audit logs
		Audit new domain administrator account creation
		Ability to export logs to CSV or JSON
		Logs can't be modified by administrators

Assessment: Threat Response

Current	Blumira	Capability
		Guided response playbooks can be easily followed to remediate the threats identified
		Automated blocking of security threats on your internet gateway
		Response playbooks can be used with basic IT helpdesk skills
		Role-based administration for responders to enable IT and/or third party providers to interact and respond with the security team

Assessment: Monitoring

Current	Blumira	Capability
		Detection solution has high availability
		Detection solution has 24x7 automated detection
		Detection solution queue logs in the event of an internet outage and resume once connectivity is re-established?

Appendix



Complete Security Coverage

Detect & prevent every stage of an attack in progress with Blumira



Discovery

- Recon Scanning (Internal & Known Threat)



Initial Access

- Password Spraying
- Brute-Force Attacks



Escalate Privileges

- Admin Role Changes
- New Admin Accounts



Execute Files

- Compromised Processes
- Malicious Executables



Exfiltrate Data

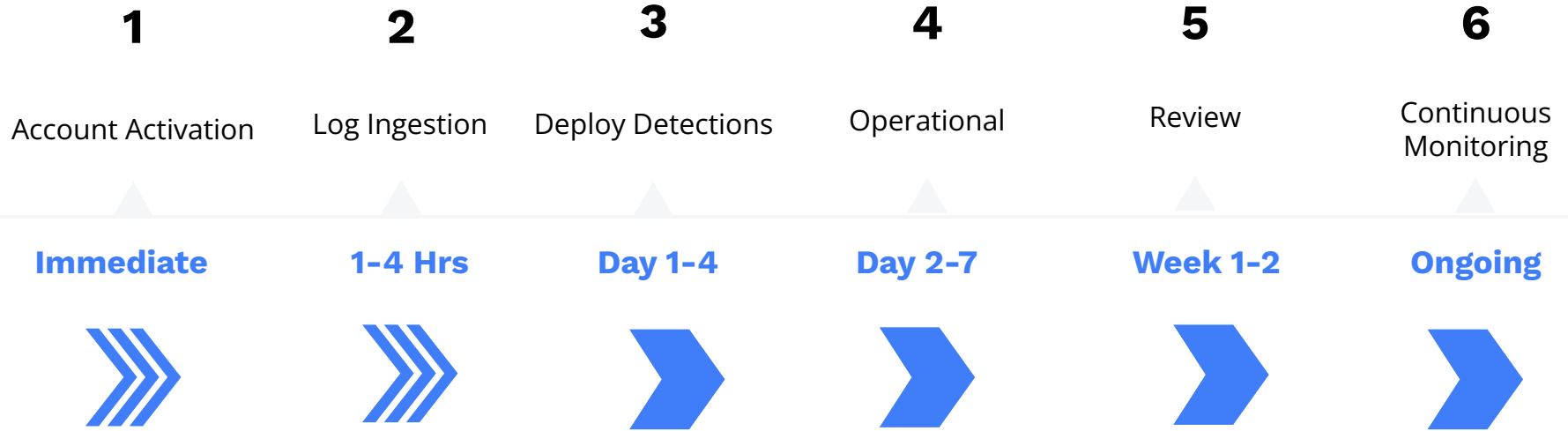
- External Doc Shares
- Outbound Connections



Ransomware

- Malware Applications

Blumira Deployment Timeline



Help Meet Compliance With Blumira

Help meet requirements for logging, audit trails, log retention, threat detection, incident response and more



PCI-DSS 3.2
to protect
payment
info

NIST 800-63
& 800-171

FFIEC for
financial
applications

HIPAA to
protect
patient
health info

CMMC for
federal
agencies

CJIS for
criminal
justice
data

IRS Pub
1075 for
tax data

Blumira Valued Customers & Trusted Partners

Finance



Healthcare



Government



Manufacturing



Retail



And More



Blumira Ranked Highly on G2



Customer Story: Ottawa County



Ottawa County is required by compliance to review logs daily - Blumira saves them time spent monitoring, doing threat hunting and investigation through automation.

Industry: Local government
Employees: 1000

Business Drivers:
Securing cloud; CJIS, IRS Pub 1075 & HIPAA compliance

"We like that Blumira is user-friendly and we don't need a dedicated security analyst to maintain it. For some of the other solutions, it would probably require us to have two security analysts on staff. Blumira is well-worth the money."

- Mike Morrow, Tech Infrastructure Manager



Problems

- Manual log reviews to meet compliance wasting time
- Need to secure complex cloud infrastructure
- Small team struggling to balance IT & security

Solution

- Blumira's solution automates the manual log review process
- Saves time on investigation and threat hunting; walks through remediation
- Provides security coverage for both cloud & on-premises environment

Blumira

Customer Story: Fechheimer



Fechheimer deployed Blumira in less than a week - resulting in shorter time to security & immediate alerts on security findings other tools missed.

Industry: Manufacturing
Employees: 500-1000

Business Drivers:
Poor pentest performance, limited resources

"Other tools are noisy; we don't have time to dig through layers and layers of data. Blumira does a good job summarizing detections and giving us advice on how to remediate."

- Steve Gatton, VP of IT, Fechheimer



Problems

- Too many tools for threat detection & log management
- Lacked visibility, proper alerting and log aggregation
- They needed a better solution for their limited IT/security team.

Solution

- Blumira alerted Fechheimer to incidents that would otherwise go unnoticed (scanning, firewall attacks, etc.)
- Now they have access to Blumira's security team
- Uses playbooks to guide them through remediation

Blumira

Customer Story: TAS United



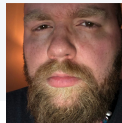
TAS United replaced Splunk with Blumira for usability, easier search, faster deployment and greater visibility.

Industry: Telecommunications
Employees: 51-200

Business Drivers:
Remote workforce support, PCI DSS compliance

"We don't have to go digging to uncover findings, alerts or reports. We're already getting a benefit out of Blumira without spending any time fine-tuning it - that's one thing in the SIEM space you can't say about other offerings."

- Tim Brewer, Systems Analyst, TAS United



Problem

- TAS United needed to secure a fully-remote workforce using personal devices
- Needed to meet PCI DSS compliance, quickly

Solution

- **TAS United replaced their Splunk SIEM** with a more user-friendly one built for lean IT teams with limited resources.
- Turned to Blumira for greater visibility, easier log search/investigation & fast proof of concept

Blumira

Blumira Care

Premium customer experience package to ensure your security success

Complete Coverage:

- **Dedicated Technical Account Manager**
- Customer Onboarding
- Technical Integration
- Deployment Consultation
- Express Rule Customization
- Customized Report Creation
- Quarterly Coverage Review
- Priority Support

