Blumira

Automated Threat Detection and Response

Blumira: Automated Detection & Response

Blumira's affordable cloud SIEM helps organizations of all sizes:

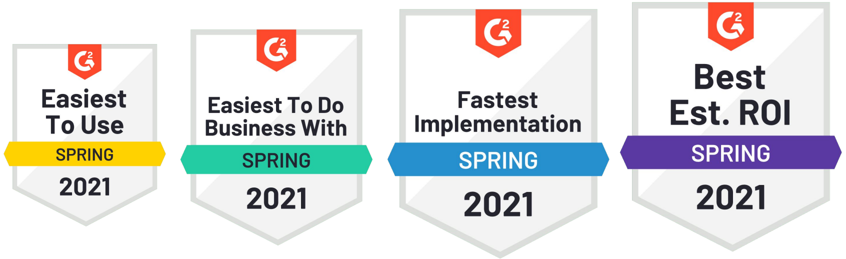
- Prevent, detect & respond to threats
- Deploy quickly with easy implementation
- Integrate broadly across an existing tech stack

Quick facts:

- Founded in 2018 in Ann Arbor, MI by CEO Steve Fuller & CTO Matt Warner
- Team of experienced security professionals (formerly Duo Security, NSA, LogRhythm, Censys)
- High-growth SaaS startup focused on ease of use

Blumira makes enterprise-level security accessible to all, enabling small teams *with limited resources & security expertise.*

Rated #1 SIEM in North America on G2



"Blumira provides expertise in understanding alerts. With a limited staff, it's important that someone has my back – Blumira's team has a real commitment to its customers."

- Kevin Hayes, CISO, Merit Network

Blumira

Agenda

01

Challenges

Addressing the biggest challenges in SecOps.

02

How Blumira Works

How we handle threat detection and response.

03

Setting Up Blumira

Blumira's integrations and deployment.

01

Current Challenges in SecOps

Security Challenges Today

Ransomware

- Everyone is a target, including SMB/MM.
- Rising ransomware & breach costs reach avg. of $2-4 million

Remote Work

- Move to cloud has created security challenges
- Lack of confidence & visibility to secure orgs

Security Shortage

- Security expertise is expensive, difficult to find
- Existing solutions too resource-intensive for SMB/MM, ripe for displacement in enterprise

Rising breach costs, cloud security risks & talent shortage converge to create a cybersecurity market gap.

Anatomy of a Data Breach

207 Days

Average Time to Detect

73 Days

Average Time to Contain

# Employees	Cost*
<500	$2.35 million
500-1k	$2.53 million
1k+	$4.72 million

Data breach costs continue to rise, year over year.

**Source: Ponemon & IBM's Cost of a Data Breach 2020 Report*

Blumira

The Business Impact of Ransomware

▶ **$4.44 million**

Cost of Ransomware Breach

Ransomware data breaches cause ongoing damage, disruption & costs.

Factored Into Total Cost:

- ✓ Ransomware payment
- ✓ Lost revenue due to downtime
- ✓ Damage to company reputation
- ✓ Forensics, investigation, remediation
- ✓ Legal fees, if customer data leaked
- ✓ Credit monitoring, identity protection
- ✓ Compliance violation fines

Blumira

Security Challenges Today

Most organizations lack detection & response capabilities - why?

Limited Teams

Companies can't afford security operations teams - current staff have limited security expertise.

Complex Tools

Maintaining & getting real security value out of SIEMs is a very slow & manual process.

Too Many Alerts

With over 10k alerts a day, how can analysts analyze and investigate every alert?

Lack of real security insights results in the inability to focus on the things that matter.

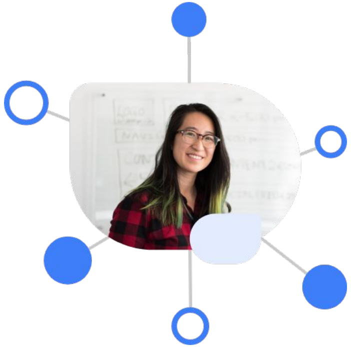
Blumira

02

How Blumira Works

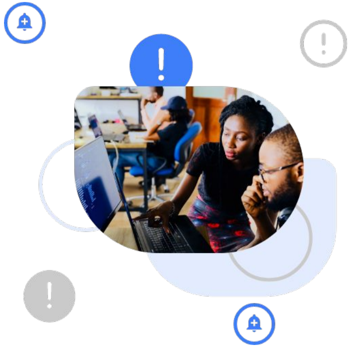
Blumira

Blumira Enables IT/Security Teams



Deploy in Hours

Cloud-delivered, small
teams can deploy



Detect Real Threats

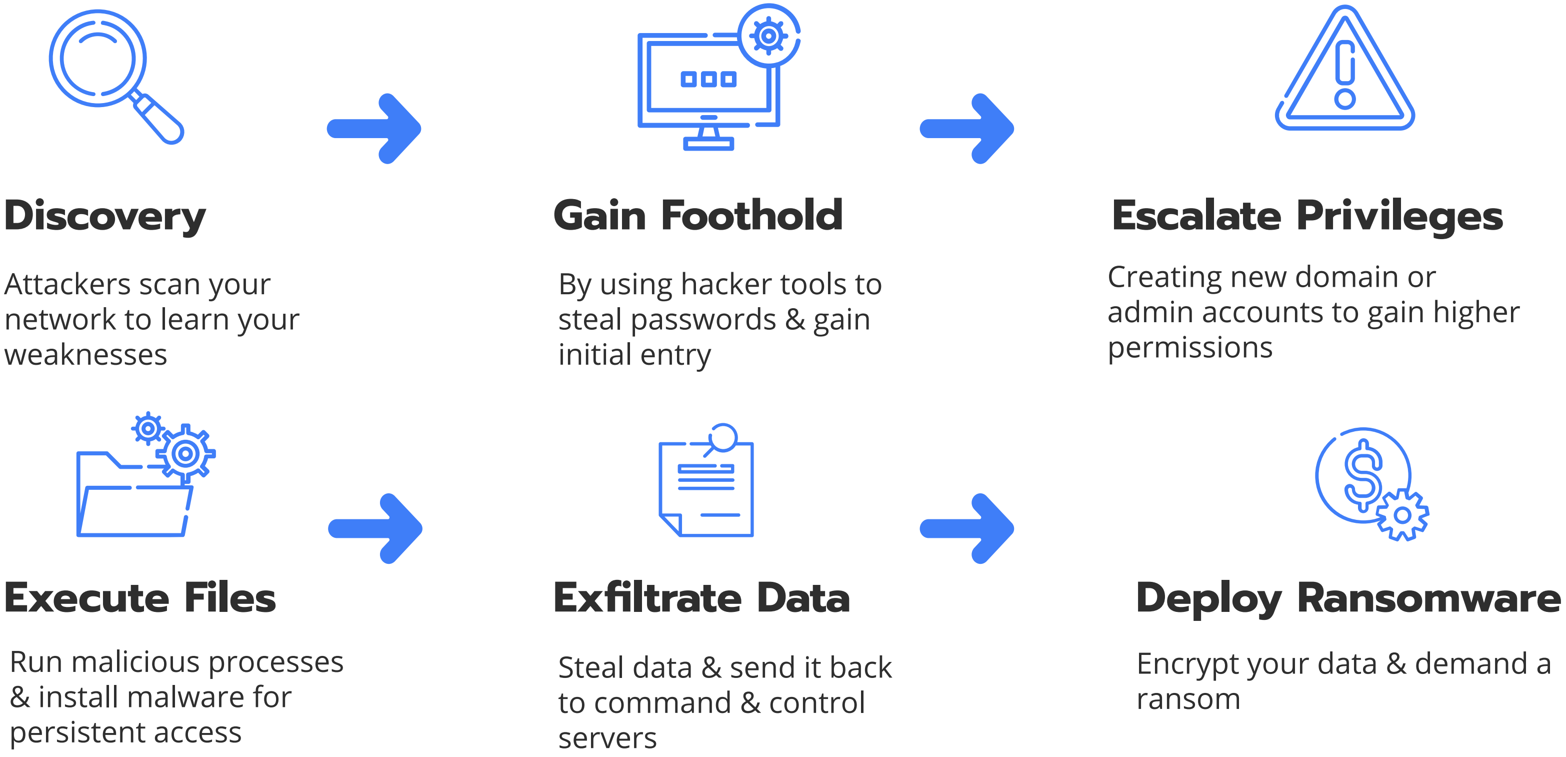
Prioritizes real security
threats & risks

Take Action

Automated response with
security playbooks

Blumira

The Many Stages of an Attack



Discovery

Attackers scan your network to learn your weaknesses

Gain Foothold

By using hacker tools to steal passwords & gain initial entry

Escalate Privileges

Creating new domain or admin accounts to gain higher permissions

Execute Files

Run malicious processes & install malware for persistent access

Exfiltrate Data

Steal data & send it back to command & control servers

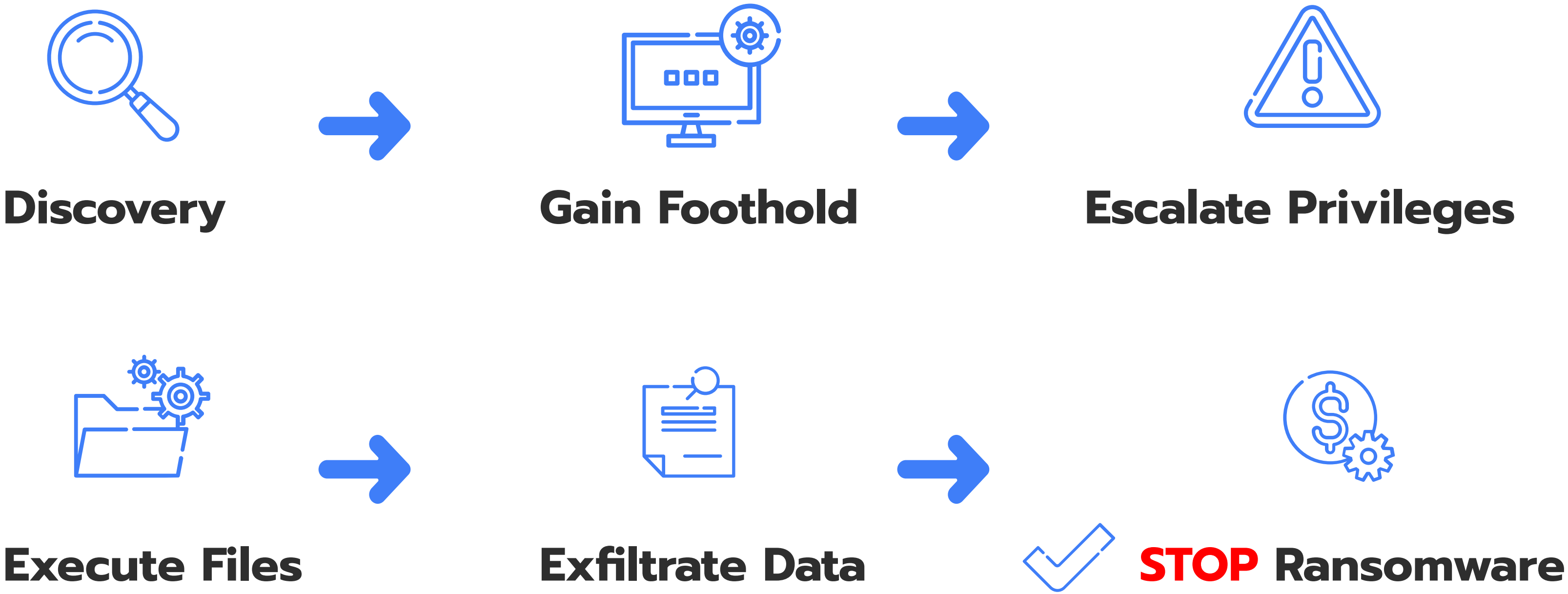
Deploy Ransomware

Encrypt your data & demand a ransom

Blumira

Blumira

Detects All Stages of a Ransomware Attack - Enables You to Respond Early to Stop Infection



Discovery → Gain Foothold → Escalate Privileges

Execute Files → Exfiltrate Data → ✓ STOP Ransomware

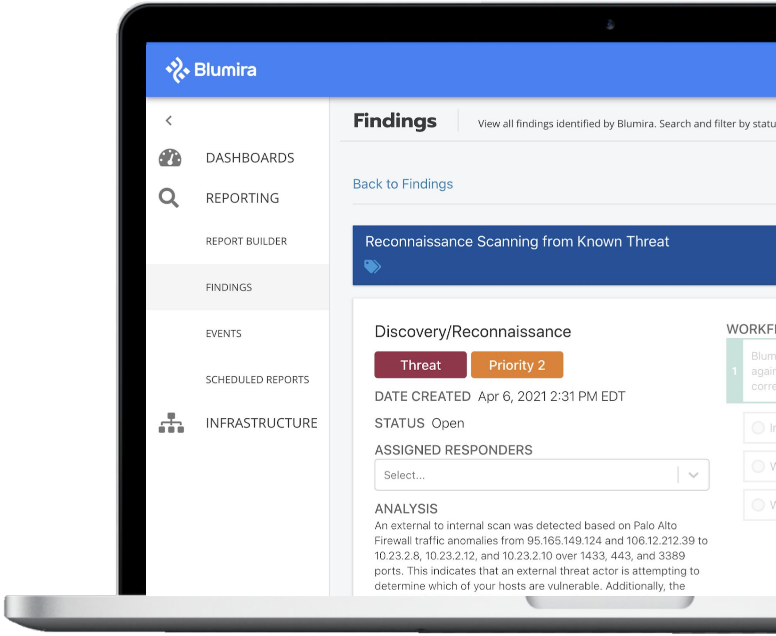
Blumira

Detect & Prevent Ransomware Attacks Early

Discovery

Scanning is one way attackers seek out vulnerable spots of your network to attack – a tactic used in the Discovery stage of attack.

By detecting source IPs running port scanning tools on your network, Blumira can detect and alert you to an attacker early in the stages of an attack, before ransomware infection.



Findings

View all findings identified by Blumira. Search and filter by statu

Back to Findings

Reconnaissance Scanning from Known Threat

Discovery/Reconnaissance

Threat Priority 2

DATE CREATED Apr 6, 2021 2:31 PM EDT

STATUS Open

ASSIGNED RESPONDERS

Select...

ANALYSIS

An external to internal scan was detected based on Palo Alto Firewall traffic anomalies from 95.165.149.124 and 106.12.212.39 to 10.23.2.8, 10.23.2.12, and 10.23.2.10 over 1433, 443, and 3389 ports. This indicates that an external threat actor is attempting to determine which of your hosts are vulnerable. Additionally, the

Blumira

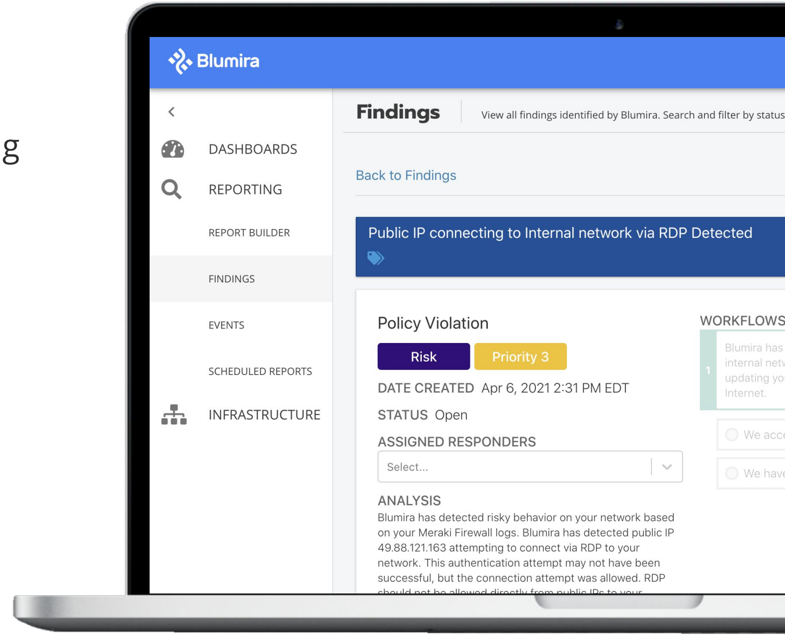
Detect & Prevent Ransomware Attacks Early

Gain Foothold

Attackers can gain a foothold to your network by stealing passwords, brute-forcing RDP credentials, or with password spraying.

Blumira can detect password spraying, account lockouts, RDP connections, open ports and more.

Blumira also provides security playbooks to guide you through next steps, such as updating firewall policies to block inbound connections from the internet.



Findings View all findings identified by Blumira. Search and filter by status

Public IP connecting to Internal network via RDP Detected

Policy Violation

Risk Priority 3

DATE CREATED Apr 6, 2021 2:31 PM EDT

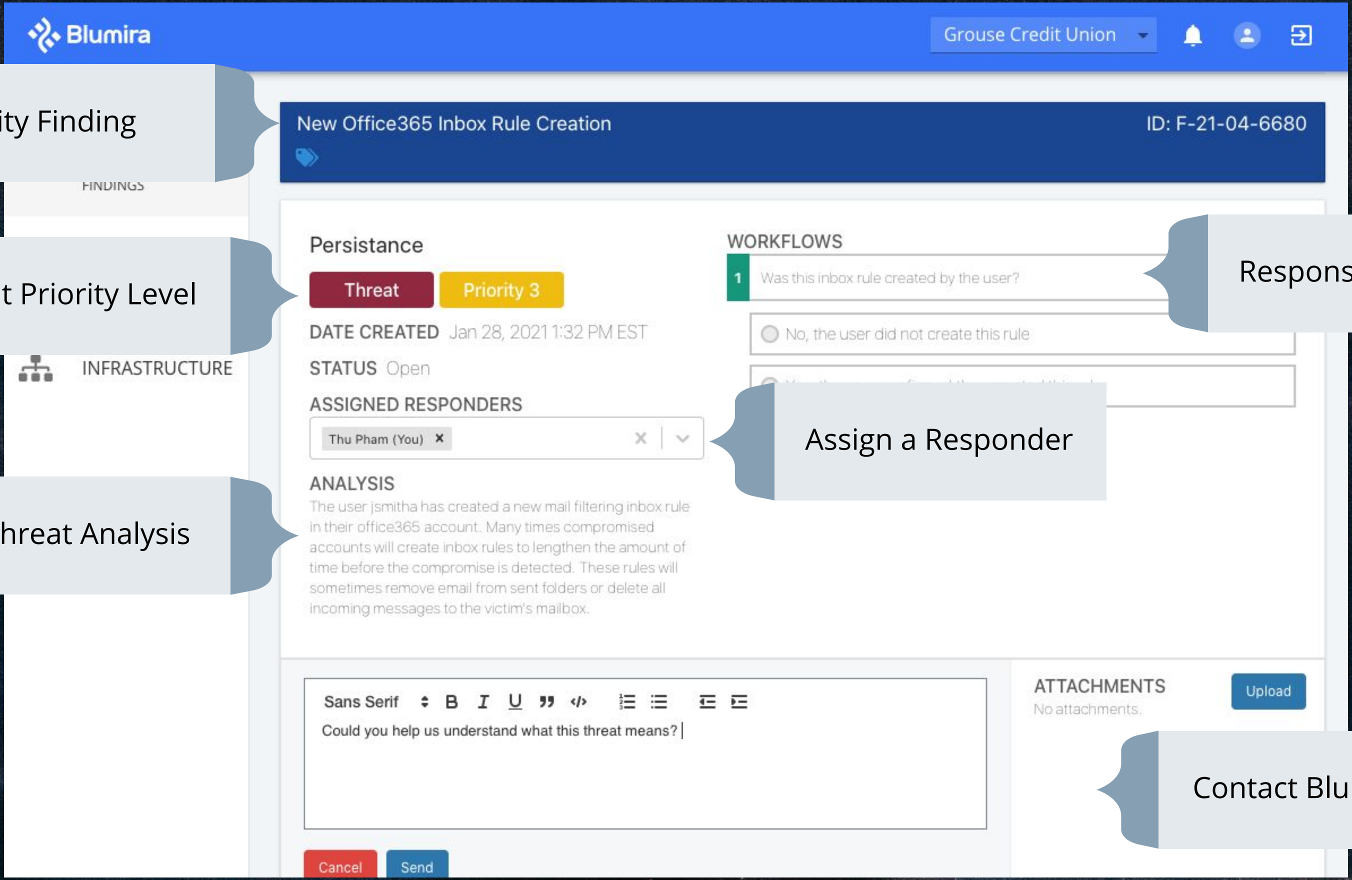
STATUS Open

ASSIGNED RESPONDERS

Select...

ANALYSIS

Blumira has detected risky behavior on your network based on your Meraki Firewall logs. Blumira has detected public IP 49.88.121.163 attempting to connect via RDP to your network. This authentication attempt may not have been successful, but the connection attempt was allowed. RDP should not be allowed directly from public IPs to your



New Office365 Inbox Rule Creation

ID: F-21-04-6680

Persistance

Threat Priority 3

DATE CREATED Jan 28, 2021 1:32 PM EST

STATUS Open

ASSIGNED RESPONDERS

Thu Pham (You) ×

ANALYSIS

The user jsmitha has created a new mail filtering inbox rule in their office365 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.

WORKFLOWS

1 Was this inbox rule created by the user?

○ No, the user did not create this rule

Could you help us understand what this threat means?

ATTACHMENTS

No attachments.

Security Finding

Threat Priority Level

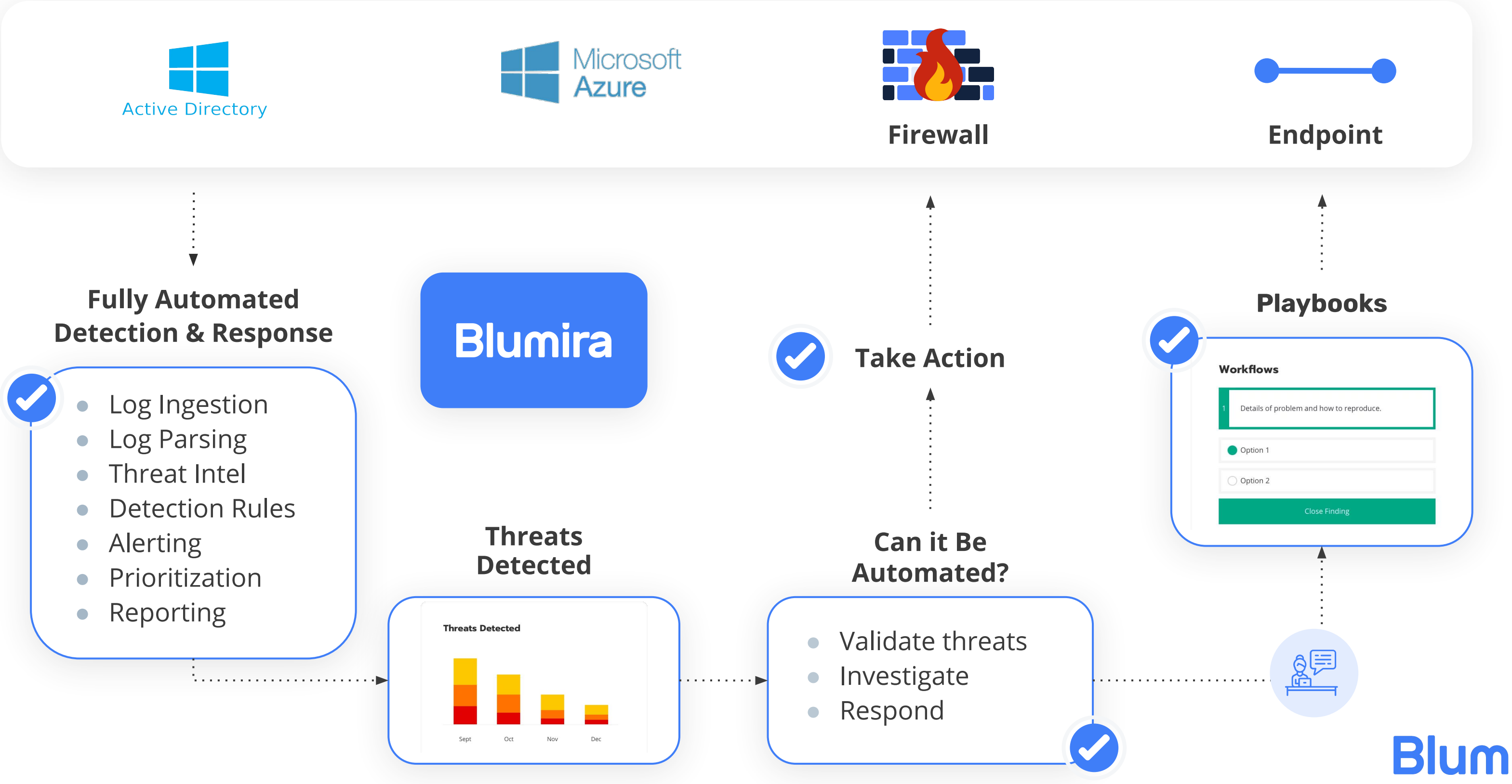
Our Threat Analysis

Response Playbooks

Assign a Responder

Contact Blumira

End-to-End Threat Detection



Fully Automated Detection & Response

- Log Ingestion
- Log Parsing
- Threat Intel
- Detection Rules
- Alerting
- Prioritization
- Reporting

Threats Detected

Can it Be Automated?

- Validate threats
- Investigate
- Respond

Take Action

Playbooks

Workflows

1 Details of problem and how to reproduce.

● Option 1

○ Option 2

Blumira

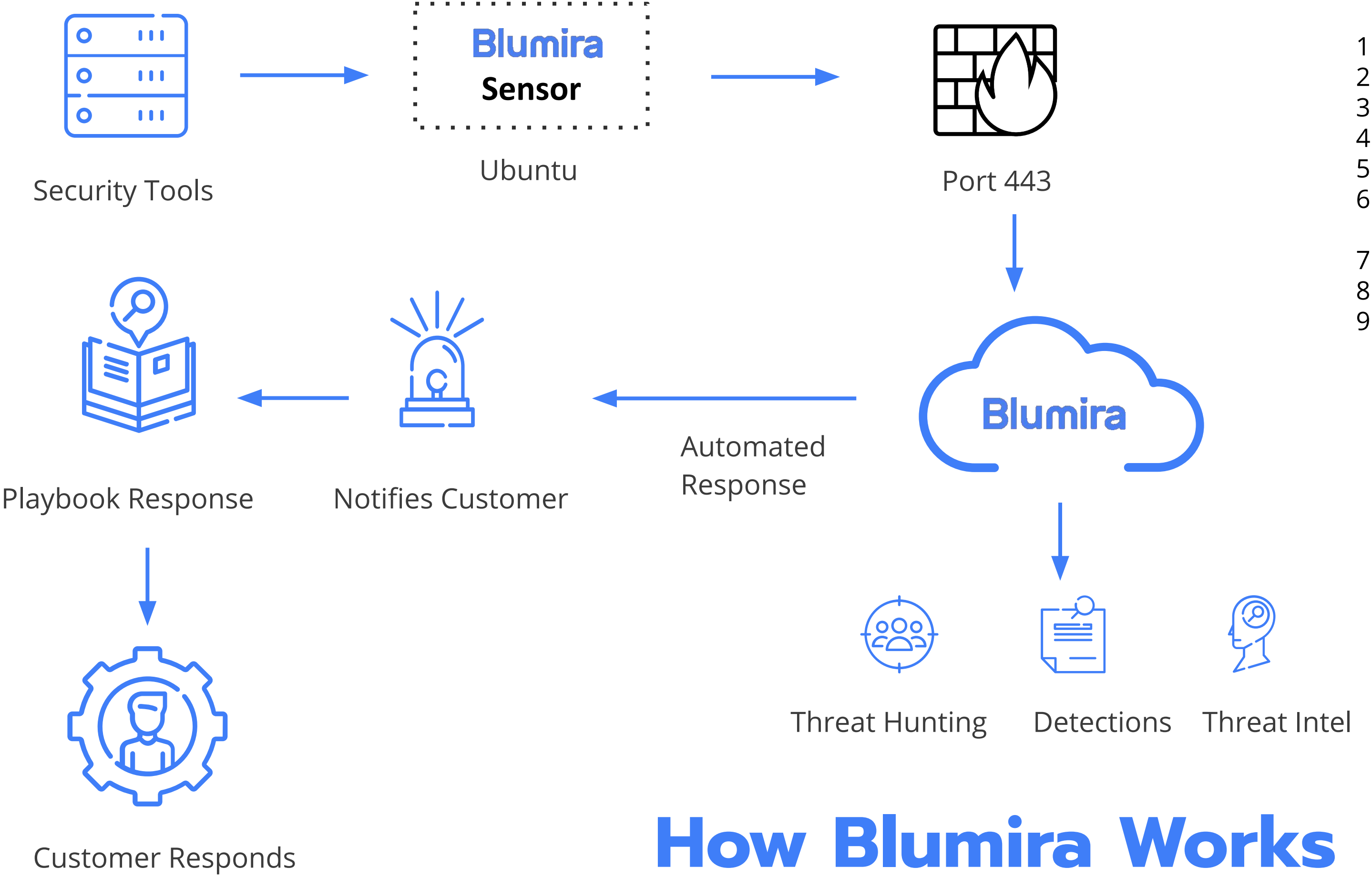
03

Setting Up Blumira

Blumira Integrates With Any Service

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

How Blumira Works



Security Tools

Blumira Sensor

Ubuntu

Port 443

Blumira

Automated Response

Notifies Customer

Playbook Response

Customer Responds

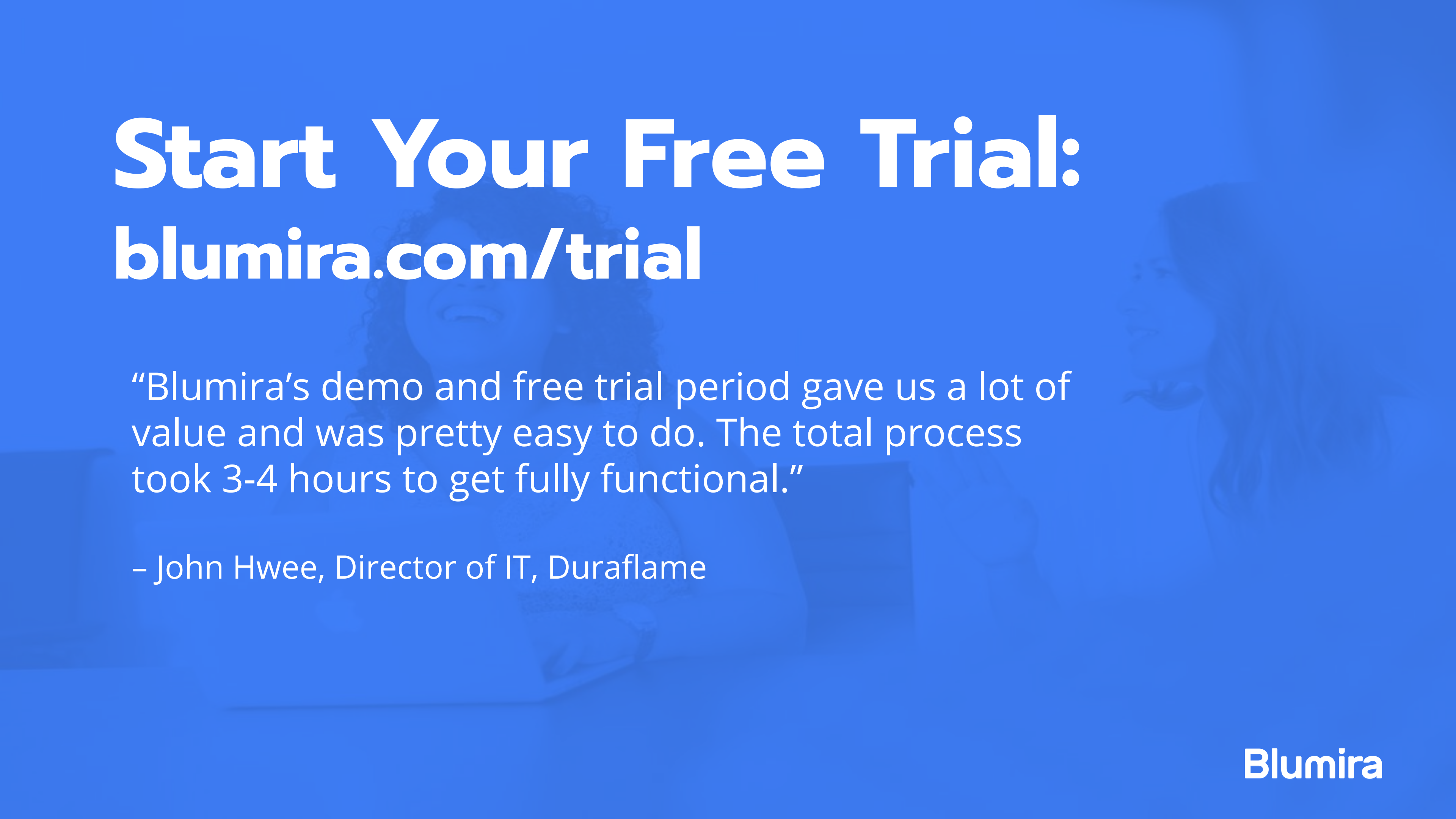
Threat Hunting

Detections

Threat Intel

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

Blumira



Start Your Free Trial:

blumira.com/trial

"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

Blumira

Appendix

Blumira

Blumira G2 Awards

Best Support
SPRING
2021

High Performer
SPRING
2021

Easiest To Do Business With
SPRING
2021

Best Results
SPRING
2021

Best Est. ROI
SPRING
2021

Best Usability
Mid-Market
SPRING
2021

Users Most Likely To Recommend
Mid-Market
SPRING
2021

Most Implementable
SPRING
2021

Easiest To Use
SPRING
2021

Fastest Implementation
SPRING
2021

Blumira

Blumira Deployment Timeline

1	2	3	4	5	6
Account Activation	Log Ingestion	Deploy Detections	Operational	Review	Continuous Monitoring
Immediate	**1-4 Hrs**	**Day 1-4**	**Day 2-7**	**Week 1-2**	**Ongoing**

Blumira

How Blumira Does It

Automated Security Operations

Log ingestion & parsing

Correlated threat intelligence

Defined detection rules

Alerting & prioritization

Honeypot detections

Automated Detection & Response

Built-in SOAR

Automate SecOps workflow

Enable IT w/ response playbooks

Cloud SIEM

Deploys in hours

100+ pre-built integrations

Scalable SaaS platform

Automated reporting

Product / Security Expertise

Hands-on deployment

Consult on identified threats

In-product interaction

Access to expertise

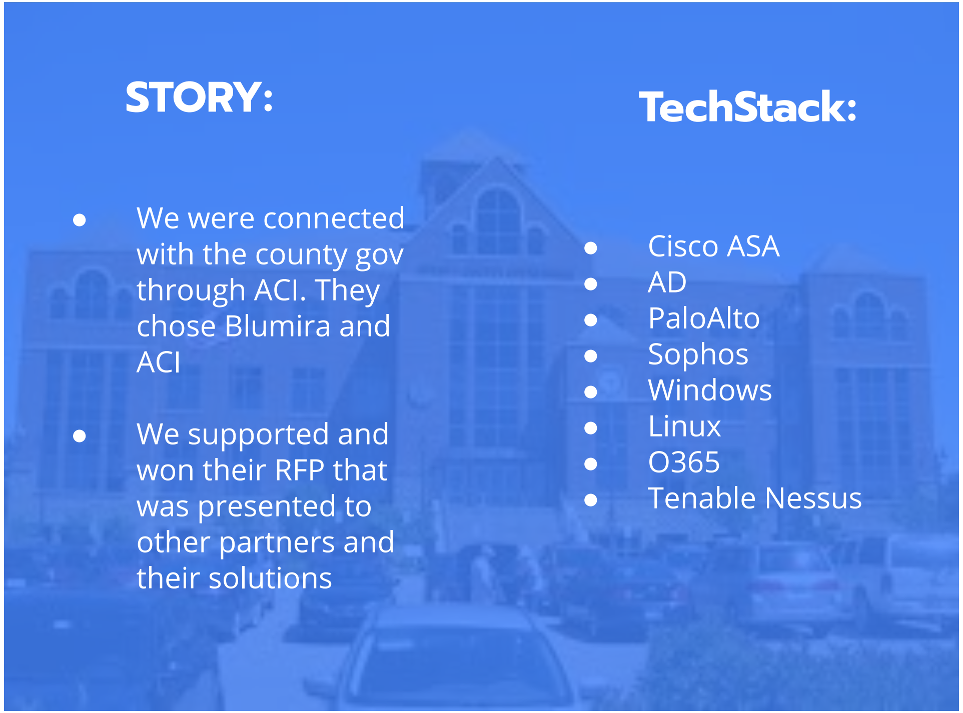
Blumira

Customer: County Government

Industry: County Govt in West Michigan
Employees: 1,000

Business Drivers:
Partner ACI is providing a security solution including Blumira

Competition:
Do Nothing, Other Partners



STORY:

- We were connected with the county gov through ACI. They chose Blumira and ACI
- We supported and won their RFP that was presented to other partners and their solutions

TechStack:

- Cisco ASA
- AD
- PaloAlto
- Sophos
- Windows
- Linux
- O365
- Tenable Nessus

Blumira Care

Our premium excellent customer experience package to help ensure your security success with Blumira's platform.

What You Get:

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

Detection Capabilities Before

Logging

0/6

Threat Detection

4/12

Alerting

1/6

Audit/Compliance

0/7

Response

0/4

Monitoring

0/3

* Please see the attached Appendix for clarity around these figures.

Detection Capabilities With Blumira

Logging

6/6

Threat Detection

12/12

Alerting

6/6

Audit/Compliance

7/7

Response

4/4

Monitoring

3/3

* Please see the attached Appendix for clarity around these figures.

Blumira Meets Compliance Requirements

Every security best practices guide and regulation asks for logging and threat monitoring

Core requirements outlined in PCI-DSS 3.2

Helps meet NIST 800-63 and 800-171

Meet FFIEC requirements for financial applications

Log security events related to PHI access

Meet Federal CMMC Requirements