

Faster Detection & Response

Time to security is more critical than ever to quickly detect and contain threats. Blumira's platform enables you to respond to threats faster to prevent ransomware and data breaches.

Simplify & Automate Threat Protection

With Blumira's SIEM & XDR platform, you can get up and running 5x faster than the industry average — using your existing team and infrastructure. Get complete security coverage in hours to rapidly detect and stop attacks.

Benefits of Blumira:

- ▶ **Faster time to security** - deploy in minutes, 5x faster than industry average
- ▶ **Replace your legacy SIEM** (security incident event management) - automate manual triage and response
- ▶ **Lower TCO** (total cost of ownership) - all-in-one platform priced per user (not data or endpoints)
- ▶ **Custom and Scheduled Reporting** - On demand access to all data for reporting and investigation purposes

Detection

Monitor and detect real threats

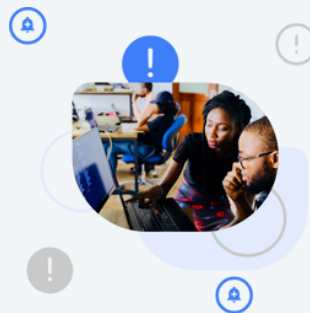
- Get meaningful findings on real threats to reduce alert fatigue
- Easy-to-understand threat analyses
- Gain wide coverage across on-premises and cloud; track trends with security reports



Response

Enable your team to quickly respond

- Block known threats with automated responses
- Easily remediate with playbooks for every finding
- 24/7 Blumira SecOps support for further assistance



Expertise

Gain access to security expertise

- Get security advice from Blumira's responsive security team
- Get help with onboarding, deployment, integrations and rule management
- Get advanced support for incident response, triage and investigation



Easy for SMBs

"SIEMs have been unreachable for small or medium-sized companies for far too long, and we are glad to say that with Blumira, that's not the case anymore."

-- David S. CISO, SMB

Comprehensive Coverage of Real Threats

Blumira leverages threat intelligence and behavioral analytics to detect patterns of attack, alerting you to high priority threats such as:

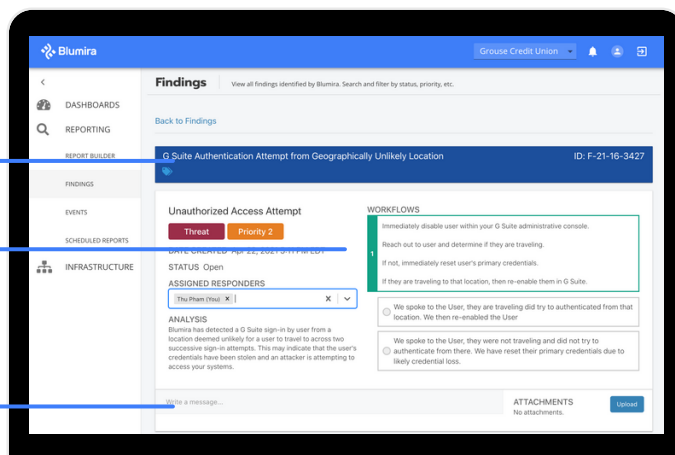
- ▶ **Cloud infrastructure threats** - Common misconfigurations, modified security groups, malware indicating a compromised cloud instance, attempts to connect with C2 (attacker-controlled) servers
- ▶ **Identity-based attacks** - Attempts to log in to your systems, including geo-impossible logins and fraudulent login attempts that could indicate the theft of usernames and passwords
- ▶ **Email & document risks** - Anomalous access attempts, external document sharing, email forwarding and new inbox rules created by attackers
- ▶ **Endpoint security threats** - Malware, unknown or blocklisted applications, malicious executables, and compromised processes running on devices within your network
- ▶ **Ransomware-related risk** - Blumira detects indicators of a ransomware attack through any of the threats listed above, then enables you to respond faster to prevent infection and a data breach

Actionable Findings, Automated Response & Access to Experts

Threat Analysis

Playbooks For Response

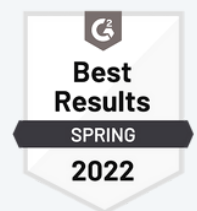
Direct Message a Security Expert



Blumira's XDR Edition

Benefits include:

- 1 year log retention for unlimited data
- 24/7 Security Operations Support for Critical Issues
- Detection rule management, allowlisting, customization
- Automated Blocking of threats with Dynamic Blocklists
- Automated Host Isolation to immediately contain device threats
- Honeypots
- Support for Firewall and Windows/Linux logs
- Custom and scheduled reporting
- Over 60 integrations included at no additional cost



Simple Security For IT Admins

"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

