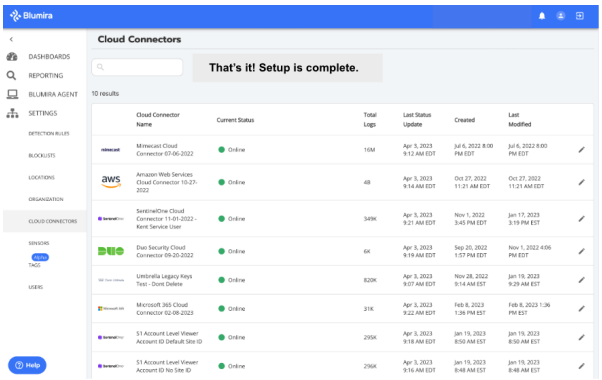
# Sales/Marketing Demo Talking Points - XDR

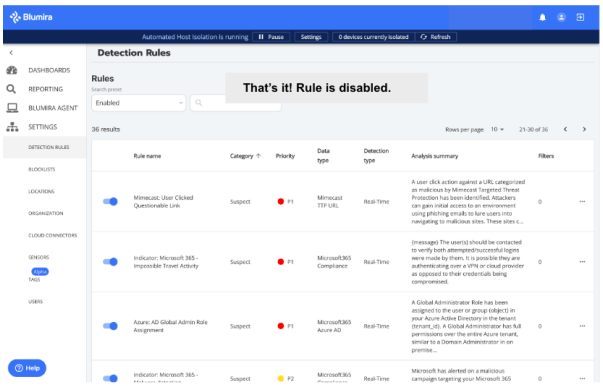
## 1. Cloud Deployment




**Easy SIEM deployment** – Blumira is 5 times faster to deploy than the average SIEM provider (according to G2) – it only takes minutes to set up a cloud integration via API and start sending logs to Blumira for threat analysis, detection and response. Traditional SIEMs normally take weeks to months to set up.

**Broad coverage for hybrid environments** – We also provide additional integrations available to set up via sensors – see blumira.com/docs for full list of third-party integrations we support (including Windows, Microsoft Cloud, endpoint, firewall, identity providers, and more).

## 2. Detection Rules

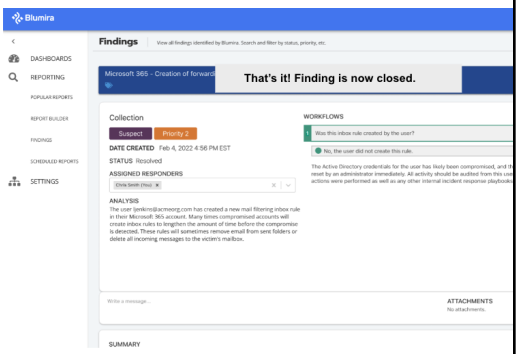



**Detection Rules** – See all rules enabled in your account and managed by Blumira's security engineers.

- Our engineers do the work for you - researching, developing, tuning and automatically rolling out new rules to the platform on a regular basis to do threat hunting at scale for your team.
- Blumira's engineers keep up to date with the latest vulnerabilities, threat research, understanding what's critical, and tracking patterns of attacker behavior

**Here, you can manage your own rules** by toggling them on and off easily, or customize them using **Detection Filters** to allow known safe activity and further reduce the noise of alerts for your team.

## 3. Findings & Playbook



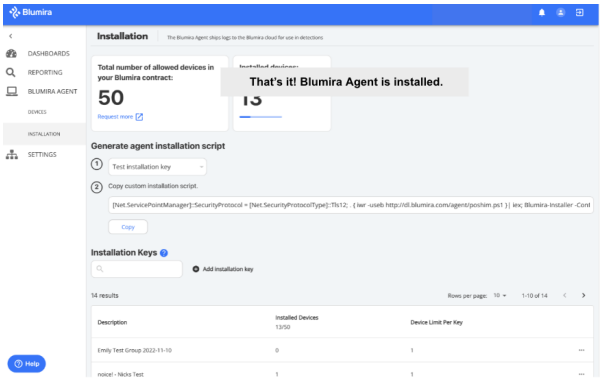

**Time to Security**: Findings are sent to you within 50 seconds of initial detection, prioritized by criticality so you know what's important to respond to right away.

- See all correlated data related to the finding, stacked below, saving you time on gathering information for investigation.
- From right within the app, you can assign a help desk tech the ticket for fast and easy triage.

**Easy to Respond**: Every finding comes with a pre-built playbook written by our security engineers to walk you through how to respond quickly.

**Message Support**: Need more help? Message our 24/7 SecOps team directly within the app (or call or email).

## 4. Endpoint Visibility



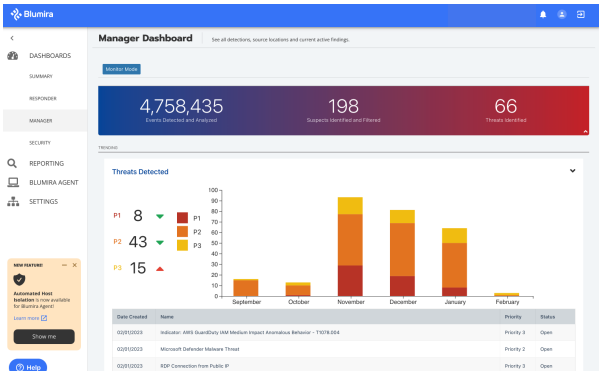

**Endpoint visibility** – Install a lightweight agent on Windows endpoints for detection and response. You can easily isolate an endpoint manually through our platform.

As part of our XDR platform, Blumira provides automated response for endpoints and malicious traffic:

- **Automated Host Isolation** – Set up auto-isolation for P1 and P2 threats to immediately contain compromised endpoints from your network to protect against spread of ransomware and attacker lateral movement. We cut off access from the endpoint to your network.

- **Automated blocking** – Block traffic from malicious sources (IP addresses) with Dynamic Blocklists – after integrating your firewall with Blumira, we can detect and automatically block malicious traffic (this requires sensor setup)

## 5. Dashboards & Reports




**Visibility** – See our at-a-glance dashboards:

- **Security** – Get a summary of your events, findings, users and endpoints
- **Manager** – See all detections prioritized by criticality, source locations, current active findings and more
- **Responder** – See all security findings and respond to priority alerts

**Reporting**

- **Report Builder** – Get access to your log data using Report Builder
- **Global Reports –** Use pre-built global reports to quickly populate and schedule to send reports of your log data.
- **Scheduled Reports** – See a list of your schedule reports, useful for investigation and compliance