

Blumira Agent: Endpoint Security

REMOTE WINDOWS ENDPOINT MONITORING

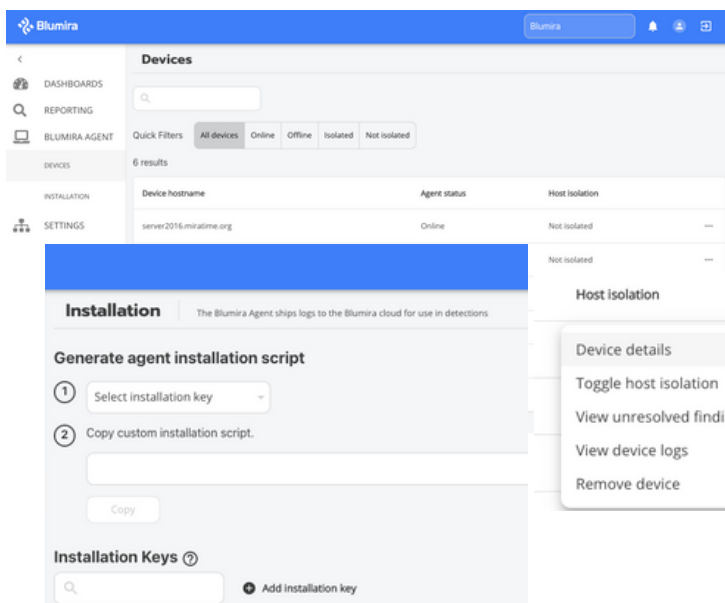
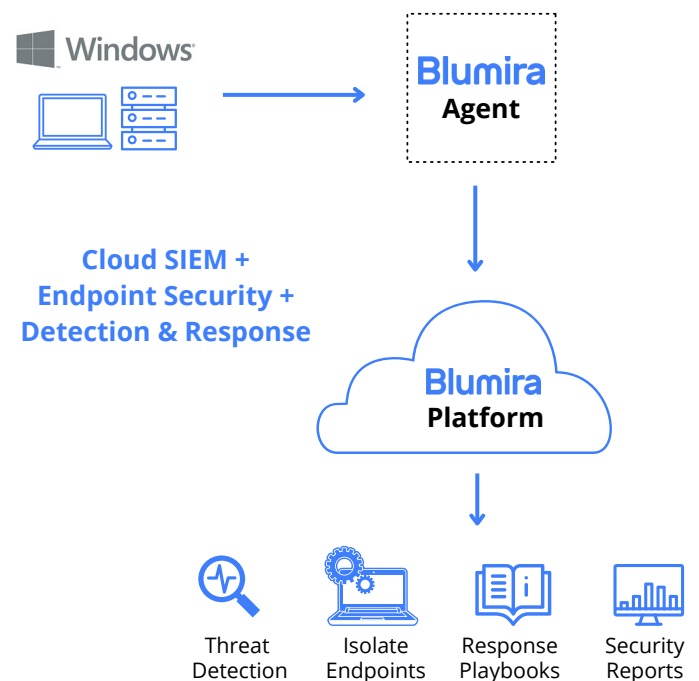
Secure Windows devices from remote locations with **Blumira Agent**: easy-to-use endpoint security designed for SMBs. Blumira Agent collects Windows endpoint logs, sending them directly to Blumira's cloud platform for analysis, detection and threat response -- no infrastructure required.



With Blumira Agent's host isolation, small IT teams can quickly contain threats to prevent the spread of ransomware and data breaches.

BLUMIRA AGENT BENEFITS

- ✓ **Frictionless agent installation** takes minutes to enroll new devices; requires no sensor or on-premises infrastructure
- ✓ **Detect remote Windows endpoint security risks** & remediate quickly using playbooks
- ✓ **Contain threats** immediately to prevent ransomware -- but continue collecting logs, critical for incident response



WHAT YOU CAN DO

- **Isolate an endpoint** with a just few clicks
- **Easily manage all devices** & see their agent status (off/online/isolated)
 - Add, remove and delete devices
- **Drill down further** to see additional device details (see pg. 2 for more info)
- **Access all associated logs** & any unresolved findings within Report Builder

DEPLOY IN MINUTES

Easily install Blumira Agent on a device using the Blumira-provided script and PowerShell

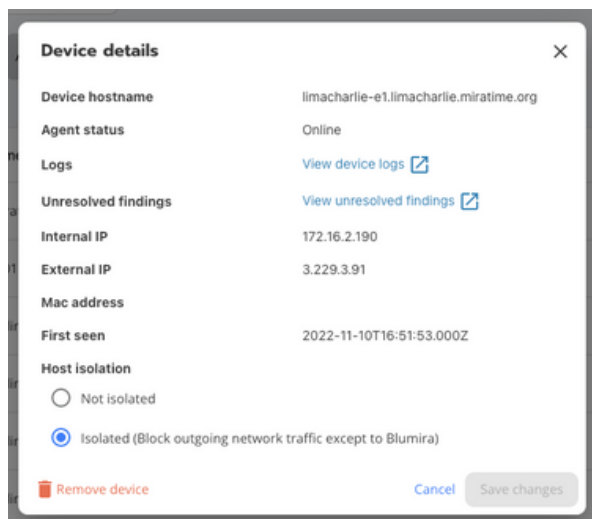
LEARN MORE: [BLUMIRA.COM/AGENT](https://blumira.com/agent)

Blumira Agent: Managed Detections

DETECT & RESPOND TO:

- Anomalous access attempts
- Exploitation of known vulnerabilities
- Malicious processes running on Windows
- Unusual PowerShell activity
- Elevation of privileges to domain admin
- Brute-force (unauthorized access) attacks
- Attempted lateral attacker movement
- Tools used by ransomware threat actors
- Clearing of logs or other attacker intrusion coverups
- **And many more -- Blumira adds new detections every two weeks for the most up-to-date coverage**

SEE DEVICE DETAILS



Windows detection rules come pre-tuned, ready out of the box



Blumira Agent is cloud-based and extremely lightweight, resulting in minimal impact to your network for greater security coverage.

Blumira Agent works well with other agents and processes running on your systems.

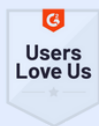
It provides advanced Windows logging for remote endpoints directly to Blumira's cloud -- no sensor required.

Note: Blumira Agent can be installed on Windows machines that are running Windows XP 32 bit or higher

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 and endpoint security with automated detection and response for better security outcomes.



VOTED #1 SIEM ON G2

- MOMENTUM LEADER
- BEST ROI & EASIEST TO USE

[LEARN MORE: BLUMIRA.COM/AGENT](https://blumira.com/agent)

THE BLUMIRA DIFFERENCE:

✓ UNIFY YOUR SECURITY TOOLS

Our platform unifies EDR capabilities, SIEM logging, detection & response to identify threats other security tools may miss, sending you alerts in under a minute of detection to help you respond to threats faster than ever.

✓ AUTOMATE MANUAL TASKS

We do all the heavy lifting for your team to save them time -- parsing, creating native third-party integrations, testing and tuning detection rules to reduce noisy alerts. Our SecOps team is available 24/7 for critical priority issues.

✓ SATISFY COMPLIANCE & INSURANCE

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.