Blumira

Blumira Agent

Blumira Agent is a lightweight endpoint agent that identifies and notifies you of threats on your devices. Blumira Agent automatically contains devices remotely, preventing the spread of ransomware and cutting off attacker access to protect your environment from affected devices.

WHY DO I NEED BLUMIRA AGENT IF I ALREADY HAVE AN EDR IN PLACE?

Avoid attacker's EDR evasion methods. Many attackers use evasive maneuvers to avoid detection by major EDRs. They can remove agents or disable event tracing for Windows (ETW), which helps hide detection of their activity. EDRs use multiple sources to collect information from a Windows operating system; ETW is one of those sources.

Blumira Agent's technology does not rely on the same methods or any third-parties to collect data from a device. The events are generated first party from user and kernel mode to ensure we can accurately detect attacker behavior that may be missed by an EDR (source: LimaCharlie).

Faster & more advanced detections

Blumira Agent sends notifications within a minute of initial detection. Paired with Blumira's SIEM, you can detect an attack in progress earlier than using an EDR alone. Blumira Agent's detections are behavior-based, written and tuned by security engineers to focus your attention on critical early signs of an attack. Without experts to write detections or tune a noisy EDR, you may miss early signs of attack.

Meet compliance

Most EDRs keep your logs for less than 90 days, which is not enough to meet compliance regulations or provide enough historical evidence for incident response or investigation. Blumira's SIEM+ and XDR Platform editions bundle in Blumira Agent, giving you one year of data retention in addition to meeting many other compliance and cyber insurance requirements.

Save money on incident response

In the event of a breach, Blumira Agent continuously sends logs, even after a device is isolated. Combined with your other logs collected by Blumira's platform, you get a complete picture of what happened, saving you time and money on incident response. Without logging, cyber insurance is not enough to cover your incident response costs in the event of an incident.

Ensure recovery

After an event, the protected logs collected by Blumira will help ensure your company can recover. By analyzing the logs, you'll be able to trace an attacker's footsteps and know if they're still in your systems or not. This helps you actually close up security holes and prevent another incident.

Blumira

DETECT & RESPOND EARLY TO PREVENT A BREACH

Identify signs of an attacker, respond quickly and contain a device significantly earlier than your EDR. Taking a layered approach to security ensures you don't miss critical signs of an attack in progress, including:

- **External access attempts**: Attackers can use external-facing remote services to initially access and/or persist within a network. Blumira Agent detects whenever a public IP address attempts to connect via SMB, RDP or FTP to your network and can automatically isolate associated devices via Automated Host Isolation.

- **Credential access attempts**: Using brute-force attempts, attackers can try to guess a legitimate user's login credentials to gain access to your network. Blumira Agent detects incidents of password spraying (programmatically testing passwords with a username) to alert you to early signs of an attacker.

- **Hidden malware commands**: Attackers may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Blumira Agent detects command and control traffic related to known malware families, and can immediately contain any affected devices.

- **Lateral movement & privilege escalation**: Attackers use different methods and tools to move throughout your environment. Blumira Agent can detect the use of PowerShell post-exploitation tools that can indicate an attacker is getting ready to exploit an Active Directory infrastructure.

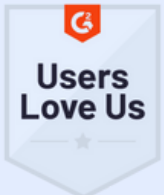
And much more – our incident detection engineers continually update and release new detection rules to keep you protected against the latest vulnerabilities and exploits.

> Overall the agent is pretty slick. It definitely has a lot of value to the customer as far as installing it on every endpoint in the environment, as it allows us to put it everywhere rather than just the server environment, which is what we have now.
>
> Michael Amado, IT Program Admin, City of Murrieta

TRIAL XDR TODAY

Blumira Agent is part of our SIEM + Endpoint Visibility and XDR Platform editions. Contact us for a demo or to try it out free yourself and get:

- Cloud SIEM you can deploy in hours
- Blumira Agent to detect and respond automatically to endpoint threats
- One year of data retention to meet compliance requirements



Visit blumira.com