

Vision

This Service (“Vision”) may also be referenced as: Vision EDR, Vision Agent, BDVision, EDR Software

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the **Vision** offering (“Services”) provided by Binary Defense. Vision is a managed endpoint detection and response (EDR) solution designed to provide clients with threat detection, investigation, and response support across endpoint environments, all in the quantities and volumes defined in, and subject to, your quote through which you purchased the Services. The Service includes access to the BD Platform, deployment of the Vision Agent, 24/7/365 monitoring, and a range of managed support functions, all as described below.

2. Scope of Services

The Services provided under this Service Description include the following core components:

- Deployment of the Vision Agent to Client endpoints (with the quantity identified in the applicable quote)
- Access to the Vision Server platform for agent management
- Access to the BD Platform for investigation management, service requests, and reporting
- Ongoing updates to Vision Agent and detection rulesets
- 24/7/365 monitoring and detection for endpoints
 - Detection and Escalation service levels are outlined in the [Detection and Escalation SLA](#).
- Access to investigation output through the BD Platform
- Configuration of dashboarding and reports for relevant log sources and events
- Binary Defense will notify Clients of new investigations and respond to service tickets via the BD Platform
- Binary Defense will tune rules to minimize false positives and suppress noise as needed
- **Overage Handling:** Endpoint quantities are as defined in your quote. If Client exceeds 5% over the defined endpoint limit, overages will be billed pro rata through the remaining term.

2.1. Service Definitions and Parameters

- **BD Platform (“BDP”):** The primary portal for investigation review, reporting, and service ticket management.
- **Vision Server Platform:** Platform currently used for Vision Agent deployment and management. Client must use this interface to configure endpoints.
- **Endpoint:** Any physical or virtual device with internet access where the Vision Agent is installed.

- **Detection:** A rule or logic set designed to trigger alerts upon identification of suspicious or malicious behavior on an endpoint.
- **Investigation:** The analytic review of an alert, leading to evidence gathering and determination of whether response or remediation is warranted.
- **EOL (End-of-Life):** The status of software no longer actively supported by its vendor. Binary Defense supports OS versions up to one year post-vendor EOL.
- **Monitoring & Investigation Limits:** Monitoring and investigations are performed up to the count of endpoints specified in the Client's quote. Clients who exceed the monthly threshold of deployed endpoints for three consecutive months may be subject to additional charges.
- **False Positives & Low-Value Alerts:** Binary Defense reserves the right to suppress, disable, or convert to reports any high-volume, low-fidelity events.
- **Supported OS:** An OS on an endpoint that BDVision is intended to function on. A supported OS means that BD makes a good faith effort designed to ensure BDVision will work as expected, including testing for new releases and bug fixes. BDVision is supported on Windows, Mac, and select Linux operating systems. We support an OS for one calendar year past their provider's end-of-life date.
- **OS:** Operating system

2.1.1. Options

N/A

No opt-in/opt-out modules are defined under this offering. Service customization is managed through detection tuning and platform access.

2.2. Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties:

N/A

2.2.2. Governance Activities:

N/A

2.2.3. Implementation Activities:

- **Agent Deployment:** The Vision Agent must be deployed on all in-scope endpoints
- **Platform Access Setup:** Client users must be provisioned with access credentials for the BD Platform and Vision Server
- **Dashboard/report configuration and initial tuning of detections** (as applicable)

2.3 Client Obligations & Assumptions

The below shall not limit or diminish Client's obligations under the Agreement.

2.3.1. Obligations:

- Deploy Vision Agent onto all in-scope endpoints
- Provide access credentials and contact information for authorized users of the BD Platform and Vision Server
- Maintain endpoint availability and ensure supported OS versions are in use

2.3.2. Assumptions

- Service is delivered remotely
- English is the default language of delivery
- Client is responsible for licensing and maintenance of their endpoint infrastructure
- Binary Defense is not responsible for Vision Server deprecation timing or roadmap transitions

2.4.1. Exclusions

Unless specifically set forth in this Service Description or reasonably related thereto as jointly determined by the parties, such activities are excluded, including, for example:

- Onsite support and endpoint deployment
- Custom agent development or third-party EDR integration
- MSSP-style active blocking or remediation services
- Forensic-level endpoint analysis beyond standard alert-based investigation
- Any legal support or expert witness work
- Real-time alerting configuration outside platform capabilities
- Access to internal Sentinel correlation instance

3. Terms and Conditions

The Services described herein are subject to the [Binary Defense Terms and Conditions](#), unless you have a separate written agreement in place with Binary Defense (“Agreement”). In the event of a conflict, this Service Description shall control unless otherwise expressly agreed in writing.