

VISION MDR AGENT

Elevate your defense instantly with Binary Defense Vision - where advanced detection meets rapid response for unparalleled security resilience.



Why Vision MDR Agent:

The minute you install Vision, you harness decades of our detection engineering, threat intelligence, deception, and response capabilities, expanding your detection program to protect against modern threats. Experience unprecedented observability and immediate contextual feedback on events happening in your organization's environment. Vision provides a robust layer of detection even when conventional tools are being attacked or evaded.

Deployment:

Install in minutes with zero user impact through our **nano-agent** enabling strategic deployment on critical servers, infrastructure, high-value targets or enterprise-wide.

Key Features:

Detection Engineering Expertise: Benefit from a dedicated detection engineering team that correlates data from our Threat Intelligence, Counterintelligence teams, Threat Hunters, and Researchers to build seamless detections

Deception Technology: With the click of a button, generates diverse simulated environments and exposures to deceive attackers. These deceptive measures attract and mislead attackers, triggering critical alerts for immediate response.

Identity Lockout: Strengthen access control measures by disabling compromised accounts on domain controllers.

Containment Playbooks: Deploy playbooks for swift containment and response to mitigate threats effectively.

Immediate Behavioral Baselining: Quickly establish behavioral-based indicators of compromise across your enterprise for early threat detection.

Key Benefits of Vision Agent

Deception Technologies: Use deception to disrupt cyber threats. Incorporate layered deception in each phase of an attack to confuse attackers and trigger low false positive alerts. Protect your assets and data by staying ahead of adversaries with advanced deception capabilities.

AI Learning Models for Advanced Threat Detection: Employ cutting-edge learning models to identify subtle indicators of compromise and emerging attack vectors. Vision utilizes machine learning algorithms to detect anomalies and potential threats, empowering you to stay one step ahead of attackers.

Vision automatically analyzes programming languages through generative AI and can determine high confidence scoring on potentially malicious code execution or suspicious indicators of compromise.

Additional Identity Safeguards: During a compromise, one of the most crucial steps is identifying the compromised identity. Vision allows you to seamlessly respond and disable compromised accounts to prevent further malicious activity.

Continual Behavioral Detection Engineering: Protect your environment from evolving threats with continual behavioral detection engineering. Vision, analyzes and adapts to emerging threat patterns in real-time. As Vision learns your network and gathers more data over time, it can accurately identify unusual behaviors and indicators of compromise that would often go unnoticed.

Detection of EDR Bypass: Detect and respond to threats even when other Endpoint Detection and Response solutions are bypassed. Vision provides an additional layer of defense, actively monitoring for signs of evasion and ensuring comprehensive threat coverage across your environment.

Integration with Managed Detection and Response: Seamlessly integrated with Binary Defense's MDR services to augment your security posture. Benefit from expert SOC analysts, deep forensic analysis, triage, rapid incident response, and threat hunting capabilities.

OS

Supported Version

Debian (x64)

Debian 11

macOS (x64/M1)

macOS 10.15 (x64,) 11 (x64/M1,)12 (x64/M1)

Red Hat Enterprise Linux (x64)

Red Hat 7, 8, 9

Ubuntu (x64)

Ubuntu 18.04, 20.04, 22.04

Windows Server

Windows Server 2012, 2016, 2019, 2022

Windows Desktop (x86)

Windows 8.1, 10

Windows Desktop (x64)

Windows 8.1, 10, 11