BINARY DEFENSE

1-800-BINARY2 | info@binarydefense.com

ENDPOINT DETECTION AND RESPONSE

Detection

Hacker-tested, superior detection to any solution available, both on and off premise. Combines attack intelligence and machine learning to identify abnormal patterns of behavior. Additionally, hunting capabilities allow rapid detection of edge cases.

Deception

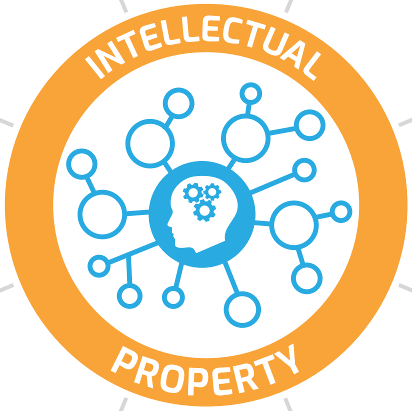
Creates multiple methods for tricking attackers along the kill-chain in order to create simulated areas and exposures for hackers to go after on each endpoint and server with Vision installed.

Protection

Blocks the attackers' tactics, techniques, and procedures (TTPs) with application control and advanced protection methods.

Response

Accelerated investigation and collapsed detection time via immediate alarming and detection. Additionally, our SOC triages for you to reduce your work and time for compromise.



Simplicity

Simple deployment and the ability to detect both commodity and advanced threats immediately with little to no resource impact to systems in a single agent.

24x7x365 Monitoring

We have analysts and eyes on your endpoints around the clock, investigating threats towards the enterprise.

Active Threat Hunting

The team focuses on identification of new groups, techniques, command and control infrastructure, and more in order to provide updated and automatic ingestion of new threats towards an organization.

Attack Intelligence

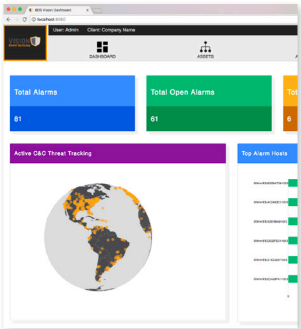
With researchers, penetration testers, and the security community contributions, Binary Defense is the leading attack intelligence company in the world.

Collapsing many technologies into one platform, so you don't have to buy or manage them individually. Our goal for you: Less Work, More Results!

Address the Most Targeted Attack Vector in Your Organization!

Endpoints and Servers are the most attacked surfaces within an organization. At the same time, adversaries no longer use the traditional hacking methods once caught by Anti-Virus (since renamed to Endpoint Protection Platforms). EPP provides little visibility and doesn't provide the protection program you need. Targeted attacks, adversaries, organized crime, and traditional hackers leverage similar behavior to establish maintained access and then move laterally in an environment. Binary Vision is the next generation of detection based on attack patterns.

A True Extension of Your Team for Managed Detection & Response



User: Admin Client: Company Name

Total Alarms 81

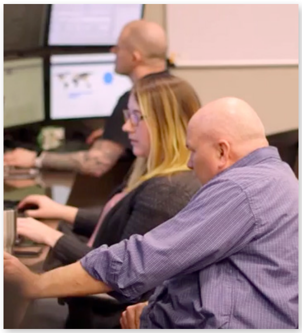
Total Open Alarms 61

Active C&C Threat Tracking

Top Alarm Hosts

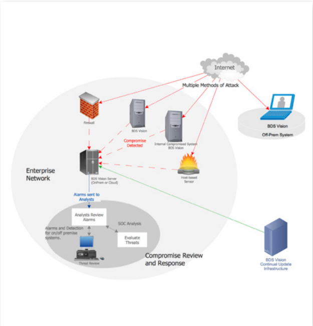
Technology

- Detection
- Deception
- Incident Management
- Containment
- Process Automation
- Machine Learning
- Application Control
- Threat Intelligence



Expertise

- Security Architects
- Security Analysts
- Threat Intel Researchers
- Penetration Testers
- Software Engineers
- Infrastructure/Operations Integration Specialists
- Security Program Managers


Internet
Multiple Methods of Attack
Firewall
BDS Vision
Compromise Detected
Internal Compromised System BDS Vision
BDS Vision Off-Prem System
Enterprise Network
BDS Vision Server (OnPrem or Cloud)
Host-based Sensor
Alarms sent to Analysts
Analysts Review Alarms
SOC Analysis
Alarms and Detection for on/off premise systems.
Evaluate Threats
Threat Review
Compromise Review and Response
BDS Vision Continual Update Infrastructure

Process

- Compromise Assessment
- Alerting & Notification
- Investigation/Event Triage
- Incident Response
- Purple-team Support
- Audit Support
- Program Maturity Leadership
- Threat Hunting

Advanced Features:

- **PowerShell injection** – advanced powershell exploitation methods used both on-disk and in-memory
- **Persistence detection** – (registry, service, file-writes, abnormal execution, PowerShell attacks, and more)
- **Abnormal patterns of behavior** – methods for application whitelisting bypasses and other methods for circumventing detection
- **Lateral movement detection** – ability to detect lateral movement in the network
- **Golden Ticket detection** around persistence hook methods in the network
- **Centralized updating** ensures continual support and latest attack pattern understanding
- **Continuously monitors command and control (C2) detection** – behavior around C2 instances and connections to malicious systems
- **Centralized reviews** of event logs and pattern attacks within log analysis
- **Deception** to protect operations technology (OT) and Internet of Things (IoT)
- **Real-time detection** of indicators of compromise (IoCs) within an organization
- **Honeypot creation** turns every endpoint into an active honeypot sensor
- **Active hunt teaming** capabilities looking for existing compromises on systems
- **Application whitelisting** and control for cloud protection

Binary Defense Vision Highlights:

- Installed in minutes with zero user impact
- Over 219,023,388 events analyzed per day
- 4,987 intrusions prevented (on average) every single day
- Instant visibility and protection across an entire enterprise
- Created by understanding the attacker mindset and behavior
- Deployed on hundreds of thousands of endpoints across the globe

Specifications: Vision employs a "nano" agent that only uses:

- 32 megs of RAM
- 0.1 CPU Usage
- 3 MB per asset

Supported Endpoints: Windows 7, Windows 8, and Windows 10, OS X, Linux

Supported Servers: Server 2008 R2 or greater (Server 2008 R2, 2012, 2016)

System Requirements: 200MB of free disk space 70MB of RAM

Network Requirements: HTTPS (443) to central BDS Vision Server

Deployment: Deployed via MSI and uses with GPO or SCCM