HMD

Endpoint Protection via an AI Engine

HMD

Endpoint Protection via an AI Engine

Deploy HMD (Host-based Malware Detection) on each endpoint host to leverage our patternless AI-based malware detection engine which continuously monitors overall endpoint health, detects anomalies, and alerts about software vulnerabilities.

Empower staff to quickly detect Advanced Persistent Threat (APT) infections, determine the source, and take appropriate response measures. HMD integrates EDR (endpoint detection and response), GCB (Government Configuration Baseline), and software vulnerability alerts to deliver a comprehensive endpoint security solution.
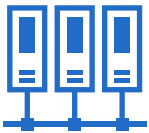
Endpoint Protection

HMD goes beyond regular AVS to detect Advanced Persistent Threat (APT) infections by assessing threat level of endpoints in your systems, from networks to files and programs to memory. HMD continuously assesses risk and immediately alerts staff when abnormalities are found.

Protection via Compliance

- Verify GCB and other government and industry configuration compliance at the OS level to reduce information security risks.
- Detect software vulnerabilities and understand the system's protection status at-a-glance.

Incident Response

When an incident is detected, the host is reported for further analysis while all other endpoints in the system are scanned under the same detection rules to track spread.

Multi-faceted Threat Detection

Our cybersecurity professionals created a patternless AI-based malware detection engine which automatically detects malicious programs and effectively assists management in cleaning system infections.

HMD

HMD (Host-based Malware Detection) adds critical endpoint security protection to your network. Get summaries on the risk levels for each endpoint and take immediate action.

Anomaly Detection	AI Algorithms & Digital Forensics
Detect Suspicious Files	Monitor Programs & Settings
Multiple Host Deployment	Endpoint Risk Alerts

Powered by Gorilla Technology