securitybox powered by CyberHunter™

One simple box:

200,000 times faster hunting, 99.999% shorter malware lifespan*

securitybox by CyberHunter

- 100% Automated
- Silent Hunting
- No Agents
- Deploys in Minutes
- C-Level Reporting

- The securitybox powered by CyberHunter runs inside your network, silently and rapidly hunting for malware that can sit quietly, hiding for months before traditional solutions can find it.

- Like a skilled human hunter, the securitybox AI engine quickly learns its environment and takes automatic action to locate its prey, wherever it may be hiding.

- No software to install, nothing to maintain. securitybox deploys in minutes and will immediately generate executive-level reports with all the right details to prove you are running clean.

- securitybox is available as a managed service. Quarterly and Annual service terms are available

*Based on average malware dwell time of 8 months in typical enterprise networks.

securitybox configurations

The securitybox comes in three configurations and can meet the scalability needs of any enterprise threat-hunting requirement:

Alpha: Focusing exclusively on the endpoints (Windows and Linux systems and servers) using agentless technology, this securitybox configuration is for those who want to manually launch large-scale, on-demand (or scheduled) cyber threat hunts within their network.

Bravo: Designed for those enterprise customers looking for a zero-touch automated cyber threat hunting experience, the Bravo configuration of securitybox adds an advanced packet analysis engine that monitors network traffic 24/7 looking for anomalous endpoint communication activity (e.g. beaconing, protocol tunneling, exfiltration, etc.). Upon detection of the suspicious network traffic activity, it will immediately launch an agentless endpoint cyber threat hunt that will analyze and validate the suspicion with no false positives.

Charlie: Designed for security analysts and cyber threat hunters who require a full-stack situational awareness of their network, Charlie configuration expands the securitybox capability by adding API functionality and access to a visually rich Cyber Intelligence Portal. The Charlie configuration allows analysts to easily explore and query their data, taking cyber threat hunting to the next level.

Screenshots of securitybox Charlie