CYBERBIT
PROTECTING A NEW DIMENSION

Cyberbit EDR

The Only Platform Built for Air-Gapped Environments
Endpoint protection, response and threat hunting designed for the most highly-targeted organizations.

Is your Security Dependent on IOCs?

"The most critical EDR capability is the ability to detect sophisticated hidden threats, ideally without requiring externally fed IOCs"
(Gartner, Market Guide for Endpoint Protection and Response Solutions, 9 November 2017)
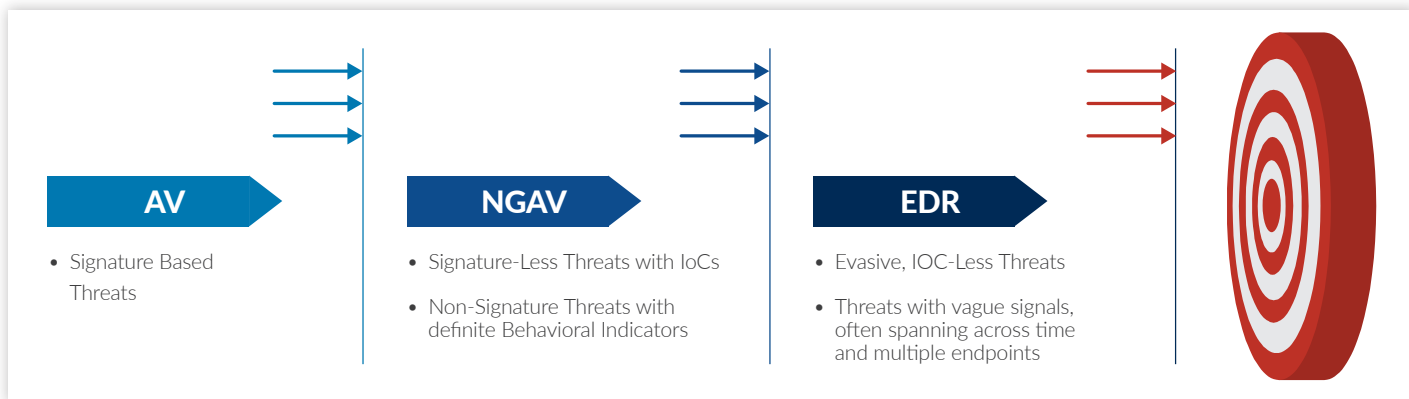
Despite numerous security tools, cyber threats manage to penetrate networks, making detection the key capability to keeping organizations secured. Yet, most detection solutions use signatures or static indicators of compromise (IOCs), detecting only threats that have been seen before. Cyberbit EDR uses machine learning and pure behavioral analytics to detect new attacks and attack permutations that have never been seen before, offering protection against the most evasive, sophisticated and highly-targeted cyber attacks and advanced persistent threats (APTs).

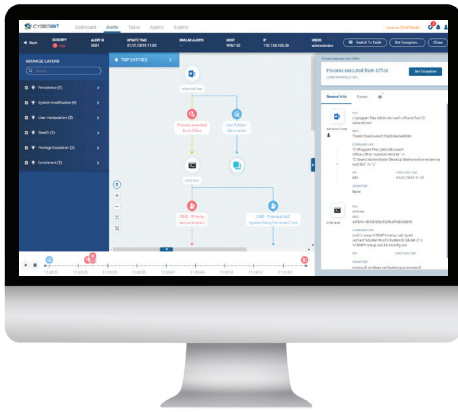## Cyberbit EDR - The Last Line of Defense Against the Most Evasive Threats

Trusted by the world's most heavily targeted organizations, Cyberbit EDR combines machine learning and behavioral analytics with big data. These combined detection mechanisms allow it to detect the most evasive threats, including file-less attacks, while keeping a low rate of false positives. Cyberbit EDR does not rely on IOCs for detection, and does not require external internet connectivity for analysis, response or blocking. All data is analyzed on-premises, and never sent out of your organization.

Pure Behavioral Detection
Independent of IOCs

Zero dependency on Cloud
Avoid geopolitical concerns

Zero dependency on external connectivity
Built for fully air-gapped networks

Highest endpoint sample rate
Continuous recording of all data

Breakthrough Visualization
Play back and click through the attack story

Fully Tested and Hardened Agent
Anti-tampering and other protections

Detecting IoC-less Threats that Others Miss

AV
- Signature Based Threats

NGAV
- Signature-Less Threats with IoCs
- Non-Signature Threats with definite Behavioral Indicators

EDR
- Evasive, IOC-Less Threats
- Threats with vague signals, often spanning across time and multiple endpoints

How It Works

Automatic visualization of attack story

Winning 100% of air-gapped PoCs, Cyberbit EDR provides superior detection and response as follows:

1. **Behavioral baseline -** Using an agent installed on each endpoint and server, Cyberbit EDR creates a behavioral baseline of normal network activity.

2. **Continuous recording -** The agent continuously records all kernel-level endpoint activity and sends it to a big-data repository.

3. **Machine learning based threat analysis -** Leveraging behavioral analysis, expert threat research, and machine learning algorithms auto-tailored to the customer's network, the platform detects threats and anomalies while minimizing false positives.

4. **Breakthrough attack visualization -** The attack story is automatically visualized in an intuitive attack graph, saving hours of analyst investigation. Video playback of the attack story enables seeing its full sequence.

5. **Threat hunting -** Can be performed using the data stored in the big data repository.

6. **Remediation and response -** Can are initiated with a single click, supporting a variety of actions to block the threat and allow quick remediation

The Cyberbit EDR Platform
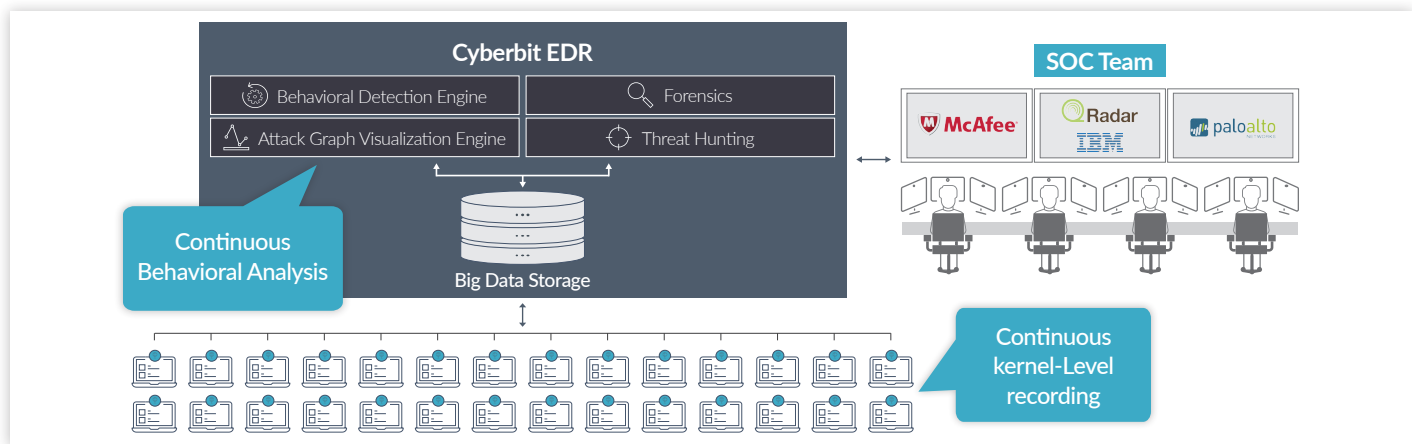
Thwart Both Known and Unknown Threats

Cyberbit EDR can be combined with an NGAV anti-malware add-on for complete end-to-end protection against IOC-based and IOC-less attacks, identifying and blocking both known and unknown threats pre-execution.

EDR SDKs - Tailor the Platform to your Needs

Cyberbit EDR lets you add new behaviors to the detection engine using its Analysis SDK. New sensors can be added to the agent to record additional events using the Agent SDK.

ABOUT CYBERBIT™

Cyberbit provides a consolidated detection and response platform that protects an organization's entire attack surface across IT, OT and IoT networks. Cyberbit products have been forged in the toughest environments on the globe and include: behavioral threat detection, incident response automation and orchestration, ICS/SCADA security, and the world's leading cyber range. Since founded in 2015 Cyberbit's products have been rapidly adopted by enterprises, governments, academic institutions and MSSPs around the world. Cyberbit is a subsidiary of Elbit Systems (NASDAQ: ESLT) and has offices in Israel, the US, Europe, and Asia.

sales@cyberbit.com | www.cyberbit.com

US Office:
Cyberbit Inc.
3571 Far West Blvd #168 | Austin, TX 78731 | Tel: +1-512-676-8731

Israel Office:
Cyberbit Ltd.
22 Zarhin St. Ra'anana | Israel 4310602 | Tel: +972-9-7799800