CYBERBIT
PROTECTING A NEW DIMENSION

Cyberbit EDR

Endpoint Detection and Response

Detect unknown and zero day attacks using machine learning and behavioral analytics

The Challenge

Verizon's DBIR report shows an increase in malware-related breaches of nearly 30% year over year. Despite the growing investment in cyber security, sophisticated attackers still manage to bypass even the most advanced security systems, including next-generation, non-signature based security. The reason is that advanced threats are coded to look like legitimate behavior. Therefore, they are extremely difficult to identify using conventional systems and can proceed unimpeded within the target networks. Conventional security systems generate countless alerts requiring security experts to correlate, analyze and prioritize them manually. Detecting and responding to advanced and targeted attacks requires a new approach.

IOC-Based Detection Is Not Enough

Today's cybersecurity threats are so dynamic that a mere 10% of hashes last for more than 90 seconds (Verizon DBIR 2016). When attackers can create new permutations of old threats by the minute, security systems cannot rely solely on Indications of Compromise (IOCs) for detection. These subtle changes in a known threat's code modify its attributes and allow the malware to easily bypass IOC-based detection mechanisms and inflict damage.

To detect and respond to advanced, targeted threats, forward-thinking organizations need to apply advanced detection techniques, beyond IOCs.

Cyberbit EDR

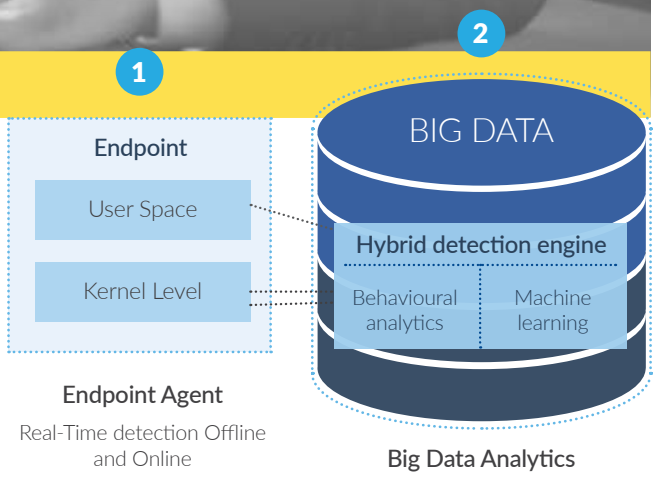
Cyberbit EDR provides a new approach for detecting and responding to advanced threats at the endpoint level. It is based on a hybrid detection engine, which combines behavioral analysis with machine learning algorithms that use statistical modeling to identify abnormal activity.

This hybrid approach, unique to Cyberbit EDR, is proven to detect a broader range of malicious activities, including threats that have never before been encountered, and is more effective at differentiating between normal and abnormal activity. As a result, it minimizes false positives without compromising on high quality detection.

Cyberbit EDR Benefits

- **Detect unknown threats –** a unique hybrid detection engine combines machine learning and behavioral analytics to detect unknown threats within seconds and minimize false positives.
- **Improve analyst productivity and lower the entry bar for new analysts –** replace manual analyst work with automated processes. Accelerate investigation, analysis and response by using visualization tools that correlate disparate data sources into a unified display of the incident lifecycle.
- **Quickly identify high priority threats –** traditional approaches require security experts to analyze numerous data feeds and prioritize threats manually. Cyberbit EDR automates this process, saves valuable time and ensures that high priority events are addressed.
- **Improve threat visibility –** Cyberbit EDR collects granular endpoint data continuously and makes it easily accessible and searchable, so analysts can drill down into threats as needed.
- **Combine detection and forensics –** Cyberbit EDR is a powerful detection platform as well as a robust forensics platform to the fullest extent, combined in one single product.
- **Remediate and respond with a click of a button –** execute response, remediation and prevention measures on all hosts across the network
- **Scale up without disrupting QoS –** Cyberbit EDR is deployed in large scale large public and private sector organizations, supporting hundreds of thousands of endpoints

How Does It Work



Cyberbit EDR provides multi-phase analysis – starting at the endpoint and continuing in a big-data repository. This approach accelerates threat detection – both on the host and throughout the network, and streamlines response and prevention.

Unlike conventional security solutions that focus either on detection or on forensics, Cyberbit EDR is unique in facilitating the entire threat response lifecycle, from detection to real-time forensics, proactive hunting and response. Its visual user interface simplifies and accelerates complex investigations and response execution.

Cyberbit EDR Main Capabilities

Detect Unknowns

Continuous Monitoring

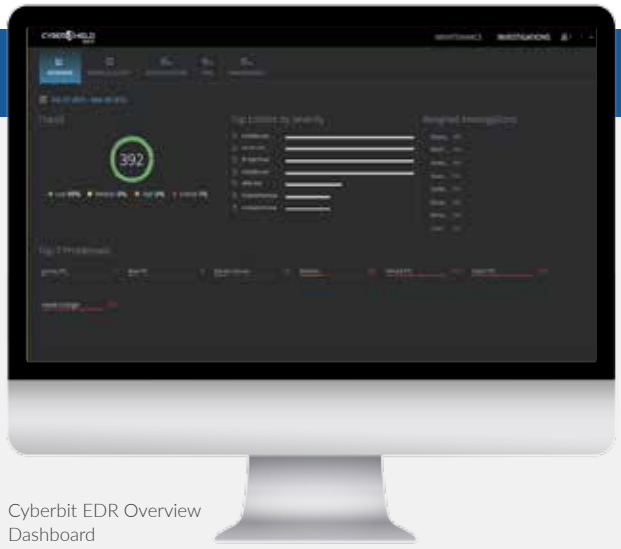
The Cyberbit EDR agent is deployed on all endpoints and servers and monitors all entities and actions in the organizational network, both at kernel level and at user space. It monitors memory, file system, registry, process and network. The data is analyzed both at the agent and in the big-data servers. This accelerates detection and assures Quality of Service. The low footprint agent is easy to deploy without disrupting operations.

Hybrid Detection Engine

The hybrid detection engine is a unique approach to identify sophisticated threats, while reducing false positives. The combination of two analysis methods – machine learning algorithms and behavioral analytics, provides reliable detection and actionable, prioritized alerts.

Behavioral Analytics

Cyberbit's behavioral analytics identify expert-defined patterns and behavioral sequences that indicate potentially anomalous activity, called a "trace". Using graph-based



Cyberbit EDR Overview Dashboard

malware analysis, all behaviors, entities and events related to the trace are automatically displayed as a visual graph. This allows analysts to view the full context and sequence of behaviors suspected as a threat.

Correlating data from disparate data sources and understanding its context within a single threat normally requires hours or days of analyst work. Cyberbit EDR's behavioral analytics eliminates this work by automatically adding context to suspicious behavior.

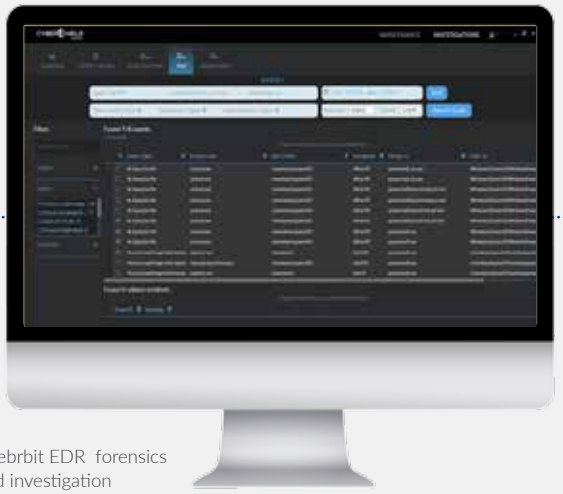
Cyberbit EDR Main Capabilities

Machine Learning Algorithms
Cyberbit EDR uses statistical models to identify anomalies. Its algorithms are provided with hundreds of threat scenarios and learn to identify typical threat behavior in various measured dimension, such as time and causality. After learning the organizational baseline, the machine learning algorithms generate an alert once suspicious activity with high statistical significance in one dimension or more is identified.

Due to its vast sample base, which is constantly fed with new threats, and due to the specific dimensions analyzed and modelled, Cyberbit machine learning manages to detect unknown threat patterns and lower false positives.

Active Hunting

With a friendly UI and investigation module, Cyberbit EDR facilitates active hunting with IOC search and identification throughout the network to provide analysts with proactive detection capabilities.



Cyebrbit EDR forensics and investigation

Easy to Use Real-time investigations

Real-Time Forensics

By using a big data based platform, Cyberbit EDR provides real-time forensics and accessibility to all data within seconds. Having all data at their fingertips – analysts can perform complicated investigations and root cause analyses, and document them for future needs.

Full Visibility

A central big-data repository stores all endpoint data. This provides unmatched visibility of all endpoints and servers and allows the analysts to finally keep on top of their network operations.

Insightful Visualization

Cyberbit's advanced graph-based malware analysis, uniquely draws the full attack trace –including all related entities and events, alongside significant insights provided automatically by the system, allowing analysts to quickly identify and understand the threat and its mode of operation.

Cyberbit EDR Graph Based Malware Analysis

Response and Prevention

With its single endpoint agent Cyberbit EDR supports multiple response and prevention actions, facilitating the entire threat response lifecycle and minimizing time-to-response. Response measures include killing running processes, quarantine of files or workstations, remote file and registry operations, capture memory dump, and preventing malicious process execution.

Optimized Architecture

High Reliability and Security

Cyberbit EDR was designed with strict security requirements in mind, and includes anti-tampering mechanisms, encryption of code and data, and self-monitoring, to provide unmatched security, reliability and availability.

Open and Extendible Architecture

SDKs for adding custom analyses both in agent and big data analytics, Rest API to visualize data in any web interface, and to import and export data to any 3rd party tool.

ABOUT CYBERBIT™

CYBERBIT provides advanced cyber security solutions for high-risk, high-value enterprises, critical infrastructure, military and government organizations. The company's portfolio provides a complete product suite for detecting and mitigating attacks in the new, advanced threat landscape, and helps organizations address the related operational challenges. Cyberbit's portfolio includes advanced endpoint detection and response (EDR), SCADA network security and continuity, security incident response platform, and security team training and simulation. Cyberbit's products were chosen by highly targeted industrial organizations around the world to protect their networks.

CYBERBIT is a wholly-owned subsidiary of Elbit Systems Ltd. (NASDAQ and TASE: ESLT)

sales@cyberbit.net | www.cyberbit.net

US Office:
CYBERBIT Inc.
3800 N. Lamar Blvd. Suite 200
Austin, TX 78756
Tel: +1-7377170385

Israel Office:
CYBERBIT Commercial Solutions Ltd.
22 Zarhin St. Ra'anana
Israel 4310602
Tel: +972-9-7799800

CYBERBIT
PROTECTING A NEW DIMENSION