Hewlett Packard Enterprise

CYBERBIT
PROTECTING A NEW DIMENSION

Cyberbit Endpoint Detection and Response (EDR)

Using big data, behavioral analysis, and machine learning to detect cyber threats that bypass conventional security systems

Objective
Analyze large volumes of endpoint data to detect indications of cyber attacks

Approach
Rapid query and investigation of endpoint data, while ensuring an engaging user experience for cybersecurity analysts

IT matters
- Provides near real-time data insertion at the scale of hundreds of thousands of endpoints, resulting in enterprise-grade threat detection quality
- Ensures rapid querying—essential for security analysts to outpace attackers
- Delivers higher detection rates and dramatically reduces false positives
- Enables analysts to perform complex queries over large volumes of data; presents results in easy-to-understand interface

Business matters
- Provides credible, robust, and scalable big data technology that will be trusted by its customers
- Processes massive volumes of endpoint data and efficiently identifies cyber behaviors
- Supports large-scale deployments across hundreds of thousands of endpoints

The industry problem

The organization's endpoints (workstations and servers) are the primary gateways for cyber attackers into the company network, where they access restricted, sensitive data. Conventional antivirus systems are no longer effective for endpoint protection, because they detect threats by comparing them to known virus databases or signature lists. However, today's "zero-day" attacks are far more advanced. They do not appear on signature lists or in virus databases and often bypass conventional security systems. Sensitive organizations such as financial institutions, large enterprises, and governments are continuously targeted by sophisticated cyber attackers and require an alternative approach.

The solution

Cyberbit, a global provider of cybersecurity products, developed the Cyberbit EDR, an advanced endpoint security solution, which uses behavioral analysis to detect and respond to threats that go undetected by conventional systems. Rather than using signatures to inspect files and processes, Cyberbit's EDR uses behavioral analysis algorithms to examine events collected from endpoints across the entire network, identify malicious behavior, and alert the security teams, allowing them to respond to the attack or investigate it further.

Massive data collection, ongoing analysis

To provide effective detection, Cyberbit's EDR continuously records events from the organization's endpoints. Such events include: reading and writing to the registry, file access and enumeration, loading of processes and DLLs, and more. This data is collected across the entire network and sent to a central HPE Vertica Analytics Platform, where behavioral analysis algorithms identify clusters of related events that indicate an attack. Machine learning

algorithms are used to differentiate between malicious and benign behaviors. These algorithms adapt themselves to the customer's environment, resulting in highly effective detection.

Optimizing ETL with Vertica

With gigabytes of data recorded every minute, a highly efficient ETL process—extracting, transforming, and loading data—is critical for effective threat detection. The Vertica Analytics solution provides Cyberbit with near real-time data insertion at the scale of hundreds of thousands of endpoints, resulting in enterprise-grade threat detection quality.

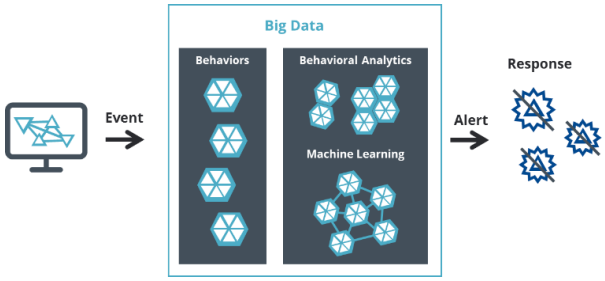
Efficient behavioral detection, forensics, and hunting

Vertica Analytics provides several capabilities that make it an optimal cybersecurity big data platform:

- **Behavioral modeling and detection algorithms, powered by distributed data clusters**
  Cyberbit uses a cybersecurity behavioral data model which transforms granular and generic endpoint events into cyber behaviors. Such behaviors include self-copying of a process, dropper behavior, code injection, privilege escalation, or lateral movement. The Vertica Analytics solution provides distributed data clusters that enable Cyberbit detection algorithms to process massive volumes of endpoint data and efficiently identify cyber behaviors.

- **Effective machine learning with Vertica distributed analytics**
  A key cybersecurity challenge is reducing the number of false positive alerts. Cyberbit applies machine learning algorithms, which continuously learn the customer's network activity to differentiate between normal and malicious behavior. This approach results in higher detection rates and dramatically reduces false positives. Machine learning algorithms are optimized for parallel execution and leverage Vertica's distributed analytics capabilities.

- **Effective data search for forensics and hunting**
  Today's security analysts spend much of their time searching and investigating data. They actively hunt and search for threats within their network, and in the event of an attack, they investigate the data to rapidly understand root cause and mitigate the attack. The EDR platform stores detailed information about each endpoint, including process names, DLLs, command lines, and more. It enables analysts to perform complex queries over large volumes of data, and presents the results in an easy-to-understand interface. Vertica's efficient search capabilities enable rapid querying which is essential for security analysts to outpace attackers.



Cyberbit EDR Detection Approach

Customer at a glance

Industry
Cybersecurity

Primary application
Cybersecurity | Endpoint Detection and Response

Solution
- HPE Vertica Analytics Platform

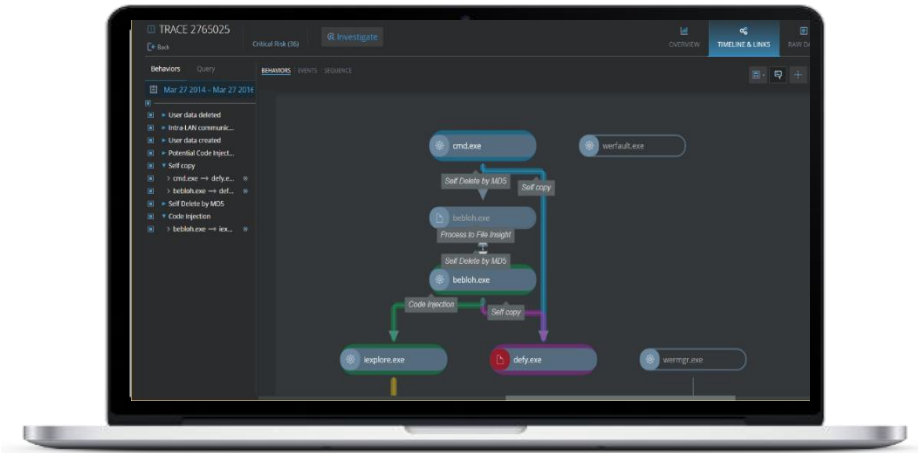
Company overview
- https://www.cyberbit.net
- Headquarters: Ra'anana, Israel and Austin, Texas
- Founded: 2015

Trusted big data technology for the enterprise needs

Cyberbit's EDR is used by large, highly targeted organizations. Cyberbit therefore required credible, robust, and scalable big data technology that will be trusted by its customers, which include governments, financial institutions, utility providers, and telecom operators. The HPE/Vertica brand was an asset in this respect, while the robust system supported Cyberbit's large-scale deployments across hundreds of thousands of endpoints.

Learn more at
hpe.com/vertica

"Effective endpoint security including detection of unknown ("zero day") threats requires collecting massive volumes of events and rapid processing using multiple cybersecurity behavioral algorithms. Vertica's performance and speed provided the ideal big data platform for our EDR platform's needs." – Ofir Barzilay, VP R&D, Cyberbit



Cyberbit EDR: Cyber Behaviors Graph

a00016055enw, May 2017

Hewlett Packard Enterprise