Cyberbit

Cyberbit uses behavioral analysis to detect and respond to threats.

Overview
Created to protect the most high-risk organizations in the world, Cyberbit secures enterprises and critical infrastructure against advanced cyber threats.

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

> **"Effective endpoint security including detection of unknown zero day threats requires collecting massive volumes of events and rapid processing using multiple cybersecurity behavioral algorithms."**

OFIR BARZILAY
VP R&D
Cyberbit

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.

Solution
Cyberbit, a global provider of cybersecurity products, developed the Cyberbit Endpoint Detection and Response (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.

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 OpenText™

At a Glance

- **Industry**
  Software & Technology

- **Location**
  Ra'anana, Israel

- **Challenge**
  Analyze large volumes of endpoint data to detect indications of cyber-attacks.

- **Products and Services**
  Vertica Analytics Platform

- **Results**
  + Provides near real-time data insertion at the scale of hundreds of thousands of endpoints, resulting in enterprise-grade threat detection quality.
  + Delivers higher detection rates and dramatically reduces false positives.
  + Supports large-scale deployments across hundreds of thousands of endpoints.

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.

Results

With gigabytes of data recorded every minute, a highly efficient ETL process—extracting, transforming, and loading data—is critical for effective threat detection. The OpenText™ 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.

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 OpenText 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 OpenText'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. OpenText's efficient search capabilities enable rapid querying which is essential for security analysts to outpace attackers.

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 OpenText 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
www.microfocus.com/opentext

opentext™