CylanceOPTICS™ Distributed Search and Collection Architecture

Feature Focus

Distributed Search and Collection

One of the biggest challenges organizations have when it comes to implementing endpoint detection and response (EDR) technologies is dealing with the enormous amount of data these products typically collect.

This data is generally aggregated in either a cloud storage environment or on physical, on-premises servers. In either case, the organization is faced with additional, ongoing costs associated with using EDR technology.

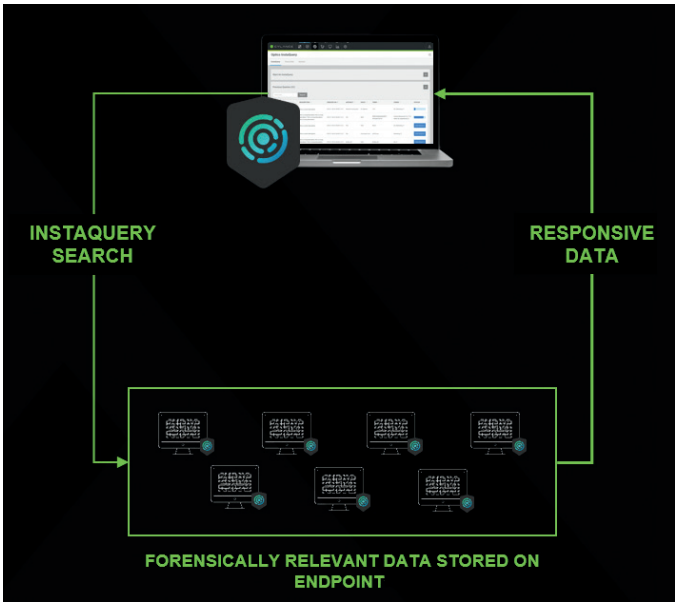
To alleviate these costs, CylanceOPTICS takes a different approach to data collection in order to optimize the type of data collected and the way in which that data is collected, searched, and analyzed.

Collection Approach

Unlike other EDR technologies that operate with a 'take all' approach to data collection that results in huge amounts of storage requirements, CylanceOPTICS employs a focused approach to collecting data, honing in and collecting only the most forensically relevant data. For instance, some solutions may capture all registry values from an endpoint, which makes sense from a comprehensive collection perspective, but provides little value from a security perspective. There are generally less than 500 registry values on a typical endpoint that provide useful security information. It is this smaller, focused set of registry keys that CylanceOPTICS monitors. If any of these keys are modified, the product will capture the data. This is just one example of how the CylanceOPTICS approach differs from other EDR products, providing a much more focused and valuable set of data that can be manually searched by security analysts and used to detect threats automatically.

Distributed Collection Approach

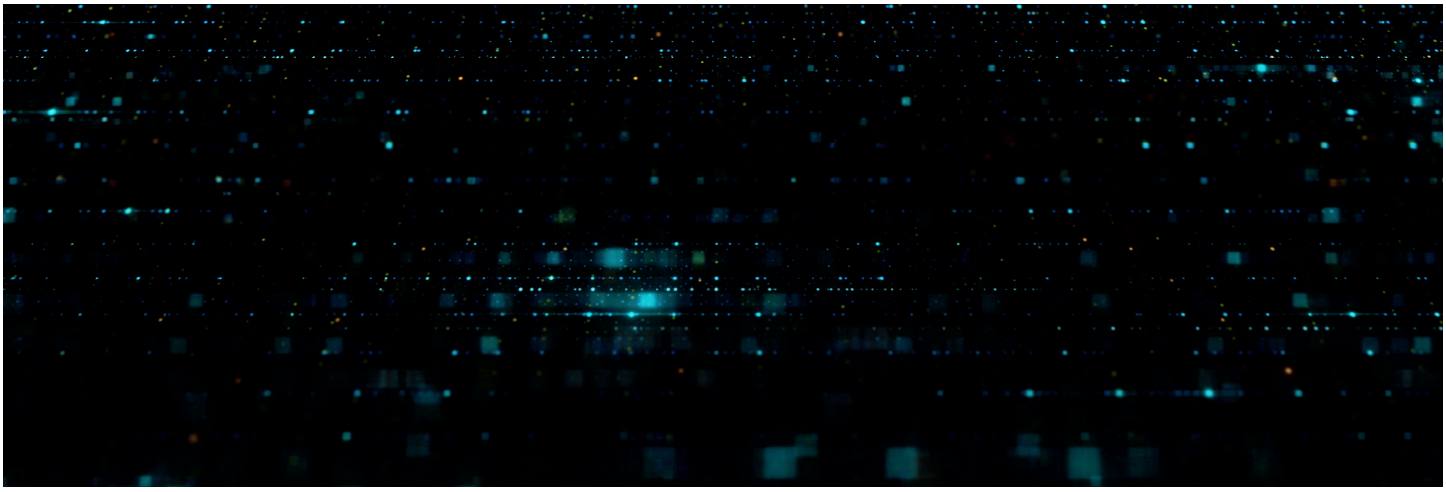
CylanceOPTICS has been designed to optimize both the search and collection of forensically relevant endpoint data. Unlike other EDR products that force the collection of everything that occurs on the endpoint and aggregate the data into a cloud or on-premises server, CylanceOPTICS stores data locally on each endpoint. The stored data capacity is 1 GB per endpoint,



which equates to roughly 10 days of activity on a very active endpoint, and around 20 days on a less active endpoint. This approach means that organizations can avoid the added data storage costs that are frequently associated with purchase and use of other EDR products.

Search Approach

With data stored locally on the endpoint, the CylanceOPTICS search approach also differs from other EDR products. Search with CylanceOPTICS occurs on the endpoint with only responsive data being collected and stored in the cloud. For example, if a security analyst is interested in determining if any of the corporate endpoints have a certain file that has been identified as an indicator of an advanced attack, he or she can create a search from the InstaQuery (IQ) interface in the cloud-based management console. That query is then communicated to the CylanceOPTICS service running on each endpoint. The service will then perform a search of the stored data on the endpoint and gather all responsive items. It is these items, and these items alone, that are then moved to the cloud environment where the security analyst can continue the investigation. Once again, this limits the bandwidth and data storage required to complete searches.



Technical Details Summary

The following data is collected by CylanceOPTICS:

CylancePROTECT®	Vault back traces from a CylancePROTECT event and gives users a bread crumb trail of events that occurred leading up to the malware showing up on the device
File	Captures file create, modify, delete, and rename events along with metadata and file attributes Correlates file to process relationships Identifies alternate data streams (Resource forks on MacOS) Identifies files from removable devices
Process	Captures process create and exit events Captures module loads Captures thread injections Correlates processes with their owning user and image file Correlates processes to all of their activity, including files, registry keys, network connections, etc. Determines if process is being debugged Determines if process is using removable media
Network	IP address Layer 4 Protocol Wi-Fi radios Visible access points Bluetooth radios and devices HOST file entries and changes DNS cache ARP Cache Static and dynamic routes Network interfaces
Registry	Captures create, modify, and delete events for registry keys and values Identifies over 120 persistence points: locations that are used by malware to persist after system reboot Correlates registry keys/values with the process that created them Identifies delayed delete files Correlates persistent registry key/value with the file that is trying to persist through a specialized parser
User	Captures all users that have logged onto the device previously Associates users with the actions they perform, including create, modify, and delete events Correlates users with malicious activity
Removable Media	Captures removable media insertion events along with files being copied to/from and executed Captures device details Identifies processes that make changes to or copy files from removable media Identifies whether the malware detected by CylancePROTECT originated from removable media

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

20170505-1041