CylanceOPTICS™

Frequently Asked Questions

Question	Answer
What is CylanceOPTICS?	CylanceOPTICS is an endpoint detection and response component providing consistent endpoint visibility, root cause analysis, scalable threat hunting, and integrated incident response. Augmenting CylancePROTECT® prevention, CylanceOPTICS enables security analysts to focus on detecting hard-to-find threats across the enterprise and taking corrective action fast.
When will v2 be released?	CylanceOPTICS v2 will be released on May 24, 2017.
What are the major features of CylanceOPTICS?	▪ **Root Cause Analysis —** Web-based, on-demand, root cause analysis of attacks blocked by CylancePROTECT as well as other interesting artifacts identified on endpoints ▪ **Smart Threat Hunting with InstaQuery —** Search endpoint data instantly for potential threats hiding on endpoints ▪ **Fast Incident Response —** Take incident response actions fast, quarantining, acquiring suspicious files, and/or isolating compromised endpoints from the network ▪ **Built for Scale —** High performance architecture built for scalability
What makes CylanceOPTICS unique?	The combined solution of CylancePROTECT and CylanceOPTICS built on the Cylance artificial intelligence (AI) platform, helps you consolidate and distill the security tools your team uses down to a manageable set, in turn reducing redundancies, eliminating high infrastructure expenses, and improving your team's ability to more proactively secure your endpoints.
How is CylanceOPTICS making use of artificial intelligence?	In v2, users will be able to complete AI based root cause analysis to determine how attackers are attempting to compromise their endpoints. In future releases, the use of AI will be extended into machine learning models, running locally on the endpoint, and designed to identify threats.
Is there a combined installer for CylancePROTECT and CylanceOPTICS v2?	Initially there will not be a combined installer for CylancePROTECT and CylanceOPTICS, however later in 2017, we will be releasing a combined installer for both CylancePROTECT and CylanceOPTICS.

Question	Answer
Does CylanceOPTICS only work with CylancePROTECT?	CylanceOPTICS does require CylancePROTECT. If you are working an opportunity where the organization does not want CylancePROTECT, but is interested in CylanceOPTICS, please contact your manager for guidance.
How will CylanceOPTICS help with the threats CylancePROTECT does not prevent?	With CylanceOPTICS, you will gain consistent visibility across all your endpoints, enabling targeted threat hunting. This targeted threat hunting will help you find hidden threats, those that could not be prevented pre-execution, and give you the tools you need to act fast.
How is CylanceOPTICS managed and deployed?	CylanceOPTICS is deployed using the same cloud-based console that manages CylancePROTECT. Currently CylanceOPTICS is a separate install from CylancePROTECT. Agent version 1400 or higher of CylancePROTECT must be installed on the device before installing CylanceOPTICS. From the management console, CylanceOPTICS can be deployed out to each endpoint for installation. CylanceOPTICS installation supports command-line options.
How do I move from CylanceOPTICS v1.1 to v2.0?	▪ Once 2.0 is enabled in your tenant, any focus view data generated using CylanceOPTICS 1.1 will no longer be available in the console. If you want to preserve your v1.1 focus view data, you can export the data out as a csv file before 2.0 has been enabled in your tenant. Please refer to attached transition document. ▪ Vault is a database that stores up to 1GB of endpoint activity history on each endpoint (equating to 10 days on average). The Vault database structure in v2 has much higher performance. With the v2 Vault upgrade, all data stored in the v1 Vault will be removed, however, we do not anticipate making similar database change in subsequent product releases. ▪ As with CylancePROTECT deployment, we strongly recommend that customers initially deploy CylanceOPTICS 2.0 in a test or pilot zone on a small number of endpoints only. Additionally, navigate to the Settings/Update tab in the console and ensure Production is set to Do Not Update to avoid automatic update in your production environment.

Question	Answer	
What types of endpoint data is collected by CylanceOPTICS?	**CylancePROTECT**	A breadcrumb trail of events that occurred leading up to the malware detection.
	Scheduled Tasks	Start times, associated users and processes, and executables.
	File	Create, modify, delete, and rename events along with metadata and file attributes.
	Firewall	Enumerates all profiles and rules for Windows Firewall.
	User	Previously logged on users. Associates users with actions, including create/modify/delete events. Identify anonymous logins, network logins, off-hour logins, and failed logins.
	Registry	Create/modify/delete events for registry keys and values. Identifies over 120 persistence points: locations that are used by malware to persist after system reboot.
	Network	ARP, DNS requests, URLs for a downloaded file, IP connects, Wi-Fi radios and access points, Bluetooth radios and devices, and modifications to HOSTS file.
	Removable Media	Removable media insertion events along with files being copied to/from and executed. Identify whether the malware detected originated from removable media. Identify source code files and documents being copied to removable media.
	Device	Complete view of the system, including the operating system, installed applications, BIOS, hardware, computer manufacturer, and languages. Enumerates loaded drivers and registered services.
	Process	Create, delete, suspend, load, and modify events for processes, threads, and modules.

Question	Answer
Where is the data that CylanceOPTICS collects stored?	CylanceOPTICS data is stored locally on the device and is available upon request from the console. By storing data locally rather than in the cloud, CylanceOPTICS can: ▪ Capture a higher volume and wider variety of system data ▪ Reduce the amount of cloud storage needed and eliminate the need for network storage ▪ Decrease network traffic to the cloud by only sending forensically relevant data
Can I buy CylanceOPTICS without CylancePROTECT?	CylanceOPTICS is designed specifically to work with CylancePROTECT. Existing CylancePROTECT customers can add on CylanceOPTICS and begin enjoying the deeper insights provided by this combined solution. If you are not currently a CylancePROTECT customer, we offer node range pricing that is easy to understand. As your business grows, CylanceOPTICS can easily grow with you.
Can CylanceOPTICS work alongside an EDR solution?	Technically there is no reason CylanceOPTICS cannot work alongside any security product. We believe as you begin working with CylanceOPTICS, you will quickly see that the value you get from CylanceOPTICS far exceeds the results you get from your other security solutions.
Can CylanceOPTICS work alongside McAfee, Symantec, etc.?	Technically there is no reason CylancePROTECT and CylanceOPTICS cannot work alongside any security product, including the products of legacy AV providers. We believe as you begin working with CylanceOPTICS, you will quickly see that the value you get from CylanceOPTICS far exceeds the results you get from your legacy AV solutions.
What are the system requirements for CylanceOPTICS?	▪ **Memory —** 4 GB ▪ **Available Disk Space —** At least 500 MB (1 GB is recommended). The CylanceOPTICS installation is small. CylanceOPTICS data stored locally can be over 100 MB per day for busier systems. ▪ **Additional Requirements** • NET Framework 4.5 SP1 or higher • Internet connection to register the product • Local Administrator rights to install the product

Question	Answer				
What operating systems are supported?	Windows Version	SP 0 x86	SP 0 x64	SP 1 x86	SP 1 x64
	7	✓	✓	✓	✓
	8	✓	✓		
	8.1	✓	✓		
	10 (1507) Initial Release	✓	✓		
	10 (1511) November Update	✓	✓		
	10 Redstone (1607) Anniversary Update	✓	✓		
	10 Redstone 2 (1703) Creators Update	✓	✓		

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

©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20170515-1092