CylancePROTECT® with OPTICS

Deep visibility into your CylancePROTECT detected and blocked events

CylancePROTECT with OPTICS uncovers the origin of an attack giving your security organization the information it needs to take corrective and widespread action immediately.

Respond to incidents faster

With clear line-of-sight to the activity on endpoints across your entire environment, you can take action fast when an incident occurs.

Improve your security posture without additional resources

Artificial Intelligence and machine learning replace the need for armies of incident responders, so only actual attack data and high-confidence suspicious file activity is investigated.

Gain Clear Insight Into Your Threat Activity

The landscape of modern cybersecurity has changed forever. Today's security campaigns are waged at the endpoint and traditional security tools fail at preventing sophisticated attacks. Security teams need complete attack protection that can stop threats before they execute, propagate, and cause damage.

CylancePROTECT stops malware dead in its tracks better than any traditional endpoint protection solution. And now, CylancePROTECT with OPTICS gives organizations a complete endpoint prevention and detection solution that provides continuous, unparalleled visibility into endpoint threat activity. Incident responders can act more quickly and with greater insight with CylancePROTECT with OPTICS.

CylancePROTECT with OPTICS leverages our world-class artificial intelligence and machine learning capabilities to protect and inform with full optical clarity into detected and blocked events. It records device activity, allowing organizations to filter and correlate suspicious and malicious activity. Organizations can not only see what threats are in their environment, but also see where they came from, when they first showed up, and how they got there.

Benefits of CylancePROTECT with OPTICS

- Pre-execution protection that suppresses incident response needs
- Visibility into the origins of the malware found by CylancePROTECT, allowing in-depth root cause analysis
- Integration with CylancePROTECT for ease of deployment and management – no additional agent or management console is required
- Full attack view using any system or OS object to build attack chain relationships

Security analysts can readily view and interact with system-level activities across the entire system without being bogged down viewing unrelated activities or process chains. Using CylancePROTECT with OPTICS, analysts use advanced threat detail to enable quick detection of advanced endpoint threats and gain the ability to take immediate corrective actions.

About Cylance

Cylance® is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist.

By coupling sophisticated machine learning and artificial intelligence with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats.

A focused view highlights the infection vector and relevant security events automatically so analysts can obtain full attack insight and enable a complete incident response investigation.

THREAT AND EVENT DETAILS CAPTURED BY CYLANCEPROTECT WITH OPTICS:

Event Type	Description of Events
CylancePROTECT	▪ Back tracing from a CylancePROTECT detect or quarantine event gives users a bread crumb trail leading up to the malware showing up on the device
File	▪ Capture file create, modify, delete, and rename events along with metadata and file attributes ▪ Correlate file to process relationships ▪ Identify alternate data streams ▪ Identify files from removable devices
Process	▪ Process create and exit ▪ Module loads ▪ Thread injections ▪ Correlation of processes with their owning user and image file ▪ Correlation of processes to all of their activity, including files, registry keys, network connections, etc.
Network	▪ IP address ▪ Layer 4 protocol
Registry	▪ Capture, create, modify, and delete events for registry keys and values ▪ Identify 120+ 'persistence points' that are used by malware to persist after system reboot ▪ Correlate registry keys/values with the process that created them ▪ Correlate persistent registry keys/values with the file trying to persist through a specialized parser
User	▪ Capture all users that have logged onto the device previously ▪ Associate users with the actions they perform, including create, modify, and delete events ▪ Correlate users with malicious activity
Removable Media	▪ Capture removable media insertion events along with files being copied to and from media, including files that execute ▪ Capture device details ▪ Identify processes that make changes to or copy files from removable media ▪ Identify 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

CYLANCE™