

As the world's malware problem continues to grow unabated, we have seen many traditional vendors give up on the hopes of providing proactive protection as something that is seemingly too difficult to provide. We've even seen incumbents such as Symantec™ publicly proclaim, "antivirus is dead." With the entire industry having given up on protecting their customers, Cylance® has started to see a new set of emerging players preying on that weakness. This is the new crop of startups that have glommed onto the concept of endpoint detect and response (EDR) as being the next security panacea...just as whitelisting was before it!

Unfortunately for the rest of the endpoint security industry, Cylance hasn't given up on the concept of protection. CylancePROTECT stops malware dead in its tracks better than any traditional signature-based antivirus, and now, we are enhancing our capabilities even further by announcing the arrival of CylancePROTECT with OPTICS.

There are many limitations and inherent weaknesses with the EDR solutions available today:

- No focus on protection or incident suppression
- Focus on detection and investigation of threats AFTER they have impacted an organization
- Overwhelming number of alerts and events - security operations teams literally drown in an ocean of meaningless, trivial and uncorrelated data
- Focus on threat intelligence and simple IOCs and IOAs that are not relevant across different organizations
- Automation is unreliable due to the poor integrity of threat intelligence
- Highly skilled incident response personnel are needed to make tools useful
- Sensitive corporate data is extruded to the cloud for solutions to work or extremely costly internal infrastructure must be acquired and maintained

Recognizing the inherent weaknesses detailed above, CylancePROTECT with OPTICS leverages our world-class artificial intelligence and machine learning capabilities to protect and inform with full optical clarity into any attack that has been attempted.

CylancePROTECT with OPTICS records device activity to filter and correlate suspicious and malicious activity to tell you not only what malware is in your environment, but to also tell you where it came from, who put it there, when it first showed up, and how it got there.



Superior Benefits of CylancePROTECT with OPTICS:

- World-class pre-execution protection that suppresses incident response needs
- No additional AV agent needed since CylancePROTECT is the world's only non-signature AV replacement
- Fully PCI and HIPAA compliant
- Artificial intelligence and machine learning replace the need for armies of incident responders so only meaningful alerts signal call for action
- Endpoints are self-contained and not required to send massive amounts of confidential information to the cloud
- Any system or OS object can be used to build relationships

Researchers can readily view and interact with the entire causality chain across the entire system and NOT simply be resigned to just looking at an unrelated list of activities or process chains, which is a limitation of most solutions. Using CylancePROTECT with OPTICS, analysts are presented with the relevant objects and are guided through relationships, rather than simply being shown process relationships without clear correlation and relationships between other aspects of the operating system that are critical missing pieces of context. A focused view highlights the infection vector and relevant security holes automatically for the analyst.

CylancePROTECT with OPTICS is the world's first incident response solution to apply artificial intelligence and predictive mathematical modeling on system events to identify and prevent malicious activity.



ORIGINS OF MALWARE



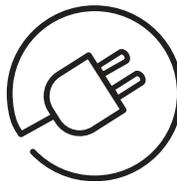
DEEP INSIGHT INTO DEVICES



ENTERPRISE-WIDE VISIBILITY



QUERY FOR OBJECTS



PLUGIN FRAMEWORK



ARTIFICIAL INTELLIGENCE

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 a hacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats. For more information, visit cylance.com

+1 (877) 97DEFEND
proservices@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700 Irvine, CA 92612

