

Key Benefits

Simple, instant malware detection — CylanceV identifies threats in portable executables using machine learning technology which can classify samples that it has never seen before without relying on signatures, sandboxing, or other less effective techniques.

Reduce malware analysis time — CylanceV can scan entire folders or disks to identify threats and provides an easy to understand *Threat Indicator* report outlining each file's capabilities that are highly prevalent in malware.

Complements your security investments — CylanceV can be used to classify and analyze a sample before whitelisting it, to feed endpoint threat info into network appliances or SIEMs, or sanitize your applications before shipping it to customers.

Reducing security operations team workload — CylanceV can help manage the amount of unclassifiable information to focus Incident Response, Forensics and IT departments to the most dangerous threats, saving time, improving effectiveness and increasing the ROI of security investments.

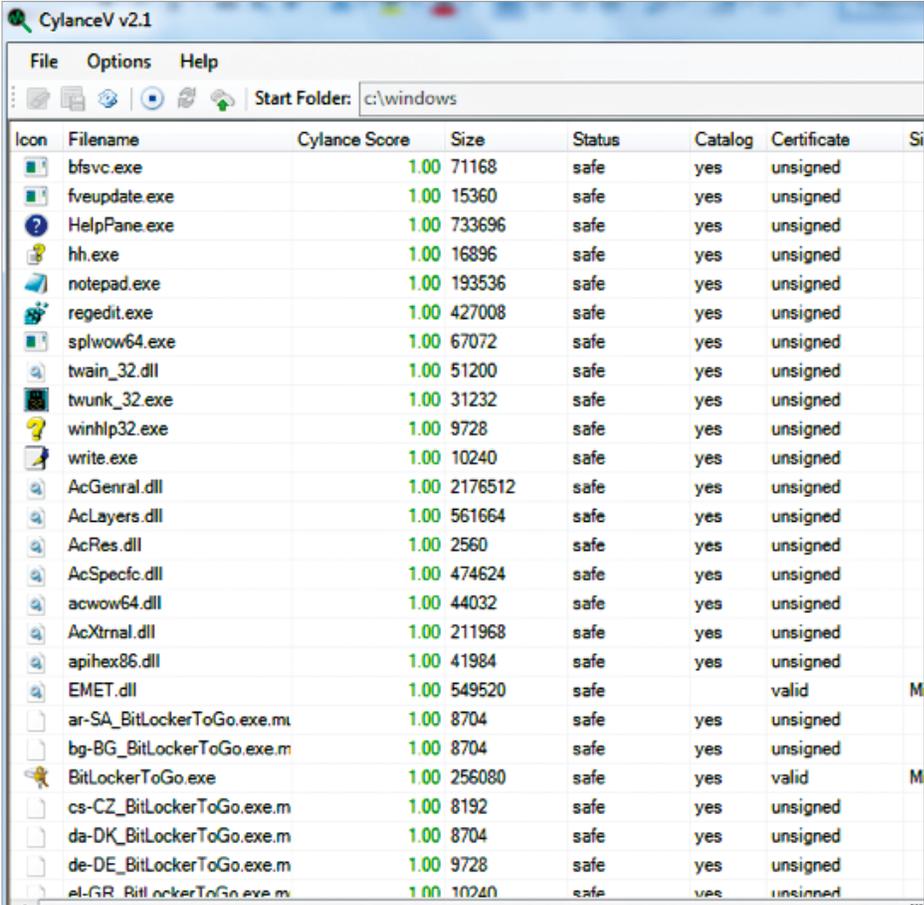
Full support for air-gapped networks — The CylanceV classifier and analysis engine experiences no feature degradation when operating without a network connection.

What Is CylanceV?

CylanceV is an application that uses Cylance's mathematical model to classify files as good, unsafe, or abnormal. The Cylance® models used by CylanceV classify samples by correlating them with the features found in millions of good and bad samples. It leverages the CylanceINFINITY™ Cloud and the power of artificial intelligence and machine learning techniques to identify and classify threats across your organization or on a single compromised system at the click of a button.

How Does CylanceV Work?

CylanceV uses a mathematical approach to determine the risks associated with data entering, traversing, and at rest within an enterprise. At the product's core is a modeling environment based on machine learning and algorithmic science that serves as a continually-improving decision-making engine for identifying what's good and what's bad. CylanceV computes a 'confidence score' for every sample as part of the classification process. When a file is given a Cylance score of 0.80, it means the model is 80% confident about the file being good. Abnormal samples have low confidence scores.



Icon	Filename	Cylance Score	Size	Status	Catalog	Certificate	Si
	bfsvc.exe	1.00	71168	safe	yes	unsigned	
	fveupdate.exe	1.00	15360	safe	yes	unsigned	
	HelpPane.exe	1.00	733696	safe	yes	unsigned	
	hh.exe	1.00	16896	safe	yes	unsigned	
	notepad.exe	1.00	193536	safe	yes	unsigned	
	regedit.exe	1.00	427008	safe	yes	unsigned	
	splwow64.exe	1.00	67072	safe	yes	unsigned	
	twain_32.dll	1.00	51200	safe	yes	unsigned	
	twunk_32.exe	1.00	31232	safe	yes	unsigned	
	winhlp32.exe	1.00	9728	safe	yes	unsigned	
	write.exe	1.00	10240	safe	yes	unsigned	
	AcGenral.dll	1.00	2176512	safe	yes	unsigned	
	AcLayers.dll	1.00	561664	safe	yes	unsigned	
	AcRes.dll	1.00	2560	safe	yes	unsigned	
	AcSpecfc.dll	1.00	474624	safe	yes	unsigned	
	acwow64.dll	1.00	44032	safe	yes	unsigned	
	AcXtrnal.dll	1.00	211968	safe	yes	unsigned	
	apihex86.dll	1.00	41984	safe	yes	unsigned	
	EMET.dll	1.00	549520	safe		valid	M
	ar-SA_BitLockerToGo.exe.m	1.00	8704	safe	yes	unsigned	
	bg-BG_BitLockerToGo.exe.m	1.00	8704	safe	yes	unsigned	
	BitLockerToGo.exe	1.00	256080	safe	yes	valid	M
	cs-CZ_BitLockerToGo.exe.m	1.00	8192	safe	yes	unsigned	
	da-DK_BitLockerToGo.exe.m	1.00	8704	safe	yes	unsigned	
	de-DE_BitLockerToGo.exe.m	1.00	9728	safe	yes	unsigned	
	el-GR_BitLockerToGo.exe.m	1.00	10240	safe	yes	unsigned	

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.

CylanceV also checks for various capabilities that are prevalent in malware and provides a *Threat Indicators* report to explain the classification. For example, the report would call out an executable's capabilities like logging of keystrokes, ability to inject code or terminate other processes, ability to tamper with windows firewall policy, etc.

Who Uses CylanceV?

- **Compromise Assessment teams** — to isolate malware samples in a compromised network.
- **Forensic Analysts** — to understand malware's capabilities.
- **Helpdesk teams** — to classify and analyze a binary before adding it to the organizational whitelist.
- **Security Operations teams** — to augment their network security and situational awareness capabilities by feeding information about binaries into their SIEMs.

What Are the Differences Between CylanceV and CylancePROTECT®?

Feature	CylanceV	CylancePROTECT
Advanced Malware Detection	Yes	Yes
Advanced Malware Protection	No	Yes
Blocks Memory Exploits	No	Yes
Console Type	Local Console and Command Line Interface	Cloud-based Console
Full Detection in Air-gapped Networks	Yes	Yes
Threat Indicators Report	Yes	Yes

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

