

# CylancePROTECT®
# Malware Execution Control

Feature Focus

CYLANCE™

## What Is CylancePROTECT Malware Execution Control?

Malware Execution Control is the core protection technology of our flagship product, CylancePROTECT. This technology leverages artificial intelligence and machine learning to detect and prevent malware on Windows, Mac, and Linux based environments before it executes. This revolutionary approach provides effectiveness far beyond traditional signature-based approaches.

## What Is the Secret Behind Cylanceprotect's Efficacy Against Malware?

Security challenges are tough to solve and dynamic in nature. The threat you see today will likely morph into a threat that a traditional antivirus signature won't recognize tomorrow. Recognizing that, Cylance® takes a formulaic data science approach to protection, harnessing the power of the cloud with the scalability and efficiency of artificial intelligence and machine learning. This eliminates the human-produced signature element in judging the rectitude of a file, and enables CylancePROTECT to predict with very high certainty if a file is safe to run.

Here is how the data science process works: The CylancePROTECT math model trains on an immense data set from both safe and unsafe executable files in Windows, Mac, and Linux frameworks. The algorithm breaks down these files into their fundamental building blocks, and then examines millions of characteristics of each file. The data features examined include any static element you can pull from memory or disc into memory: file size, signing attributes, string data, icon, imports, permissions in a data section, packers, compiler type and language, headers, directories, and the presence or absence of features in combination to name a few. The resulting data from the feature extraction is then vectorized and used to train the machine learning model on what is safe to run, and what is unsafe. Finally, we classify to help ascertain the rectitude of the file in question and cluster the results to assess to what the file is most similar. The similarity and clustering gives the context around the endpoint file.

When a new, unknown file is encountered on the endpoint, we can then use this information to determine statistically whether a file is safe to run before it is executed. This process is automated, and done in real time.

| Known Good files | Feature A | Feature B | Feature C |
|---|---|---|---|
| File1.exe | 1 | 0 | 0 |
| File1.exe | 0 | 0 | 1 |
| File1.exe | 1 | 0 | 0 |
| **Good score** | **2** | **0** | **1** |

| Known Bad files | Feature X | Feature Y | Feature Z |
|---|---|---|---|
| File1.exe | 0 | 0 | 0 |
| File1.exe | 0 | 1 | 1 |
| File1.exe | 1 | 1 | 0 |
| **Bad score** | **1** | **2** | **1** |

*Figure 2 – Simplified CylancePROTECT algorithm table*




*Figure 1. The CylancePROTECT dashboard*

## How Does CylancePROTECT Malware Execution Control Work?

CylancePROTECT's architecture consists of a lightweight agent installed on the host and managed by a Cylance cloud console. CylancePROTECT's malware execution control will detect and prevent malware using tested mathematical models on the host, independent of cloud connectivity, signatures, trust-based systems, or behavioral analysis. It is capable of detecting and quarantining malware in both open and isolated networks without the need for continual updates, rendering malware, ransomware, fileless attacks, bots, and future variants useless. As the threat landscape evolves, so does CylancePROTECT. By constantly training on a vast set of real-world threat information, CylancePROTECT keeps users one step ahead of the attackers.

Cylance's mathematical approach stops the execution of harmful code regardless of having prior knowledge or employing an unknown obfuscation technique. In conjunction with CylancePROTECT's application control, device control, script control, and memory protection, no other anti-malware product compares to the effectiveness, simplicity, and protection of CylancePROTECT.

## How To Use CylancePROTECT Malware Execution Control

CylancePROTECT is designed to be easy to use, while preserving unparalleled effectiveness against the most nefarious cyberthreats. Complete details about CylancePROTECT can be found on the Cylance website.

## About Cylance

Cylance is the first company to apply artificial intelligence, machine learning, and algorithmic science to cybersecurity to improve the way companies, governments, and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance's award-winning product, CylancePROTECT, quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated artificial intelligence and machine learning with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be predictive and preventive against advanced threats.



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

CYLANCE™

©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.

20170608-1268