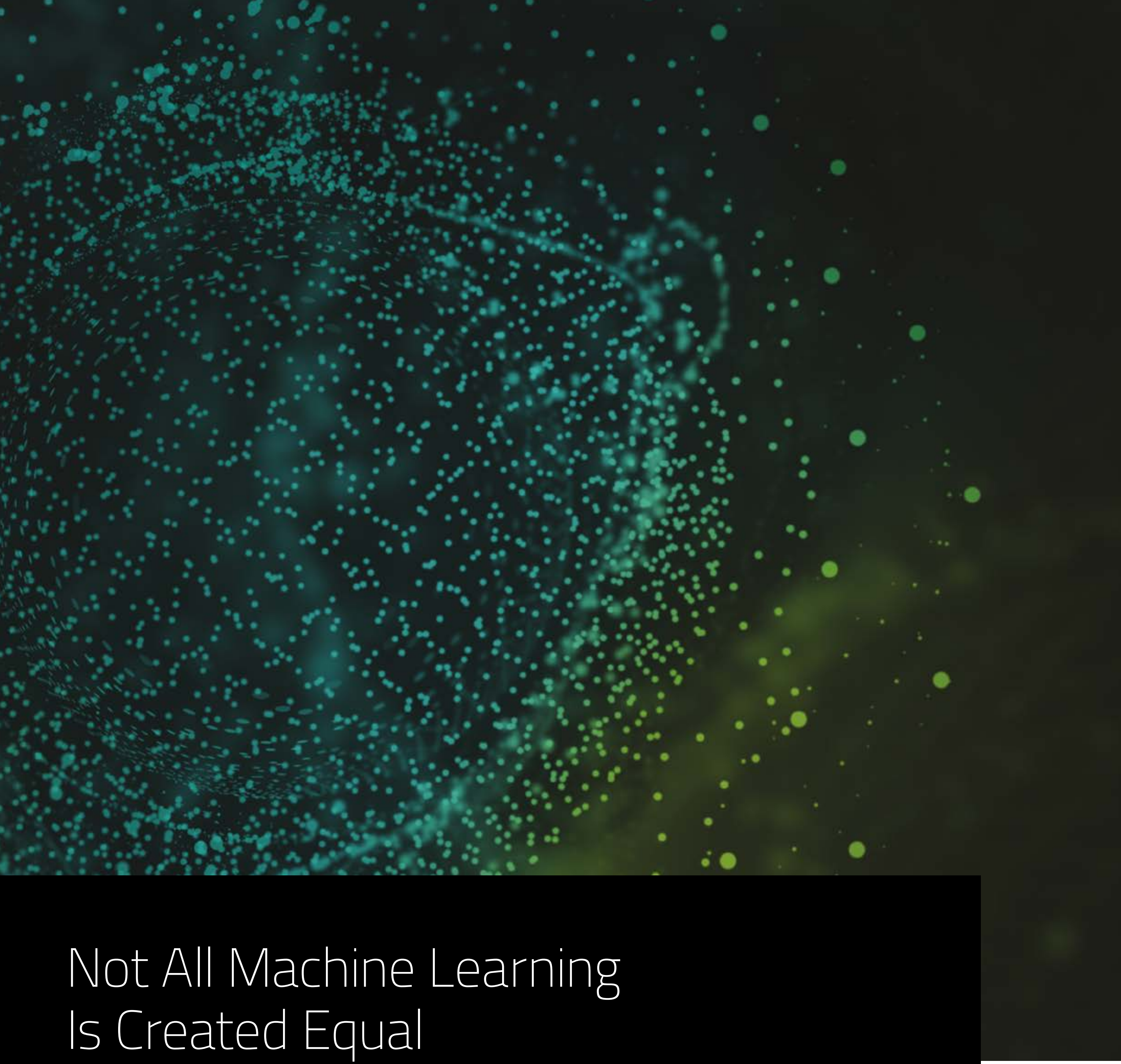


Not All Machine Learning Is Created Equal

Why Cylance Beats the Competition When It Comes To Endpoint Protection

The 21st century marks the rise of artificial intelligence (AI) and machine learning capabilities for mass consumption. A staggering surge of machine learning has been applied to a myriad of uses — from driving cars to curing cancer.

AI and machine learning have only recently entered the world of cybersecurity, but it's occurring just in time. According to Gartner Research, the total market for all security will surpass $100B in 2019. Companies are looking to spend on innovation to secure against cyberthreats.

As a result, more tech startups today tout AI to secure funding; and more established vendors now claim to embed machine learning in their product lines.

Yet the hype around AI and machine learning — what it is and how it works — has created confusion in the marketplace.

Whether you're a CxO, an IT administrator, or SecOps operator, how do you make sense of the claims? Can you test for yourself to know the truth?

Cylance is a pioneer in applying AI to cybersecurity. The company spearheaded an innovation revolution by replacing legacy antivirus software with predictive, preventative solutions and services that protect the endpoint — and the organization. It stops zero-day threats and the most sophisticated attacks, both known and unknown.

The Cylance Difference

So what makes Cylance machine learning stand out from the rest?

Cylance works because it:

- Achieves efficacy rates at or higher than 99%[1] (compared to 50-60% with legacy AV)
- Requires minimal system resources, has low CPU usage and a small memory footprint
- Prevents attacks with exceptional speed — in milliseconds
- Requires no cloud connection to prevent threats

Unlike human analysis or competitive offerings, Cylance machine learning operates with unparalleled precision, preventing 99% of existing and never-before-seen malware.

How? Cylance AI analyzes statistically similar blocks of file code to identify malicious files. It does this through observation, pattern recognition, and predictive analytics. This approach supplies a quantum leap in endpoint protection over traditional malware signatures, heuristic, or behavioral methods by taking advantage of sophisticated math models to identify malware. Instead of reactive signatures, threats are blocked automatically in real time.

Other vendors claim to use machine learning, but their solutions require a patient zero or a user sacrificial lamb that must get breached by malware or a malicious payload. The first Cylance machine learning model was published more than two years ago. It was so effective that when recently tested, it was shown to prevent zero-day threats released in 2016.[2] What does this mean for consumers? The latest, most advanced iteration of the Cylance math model, two years in the refinement process, predicts, prevents, and protects against zero-day threats yet to be developed. It works against both known and unknown files, essentially stopping threats before they are even created.

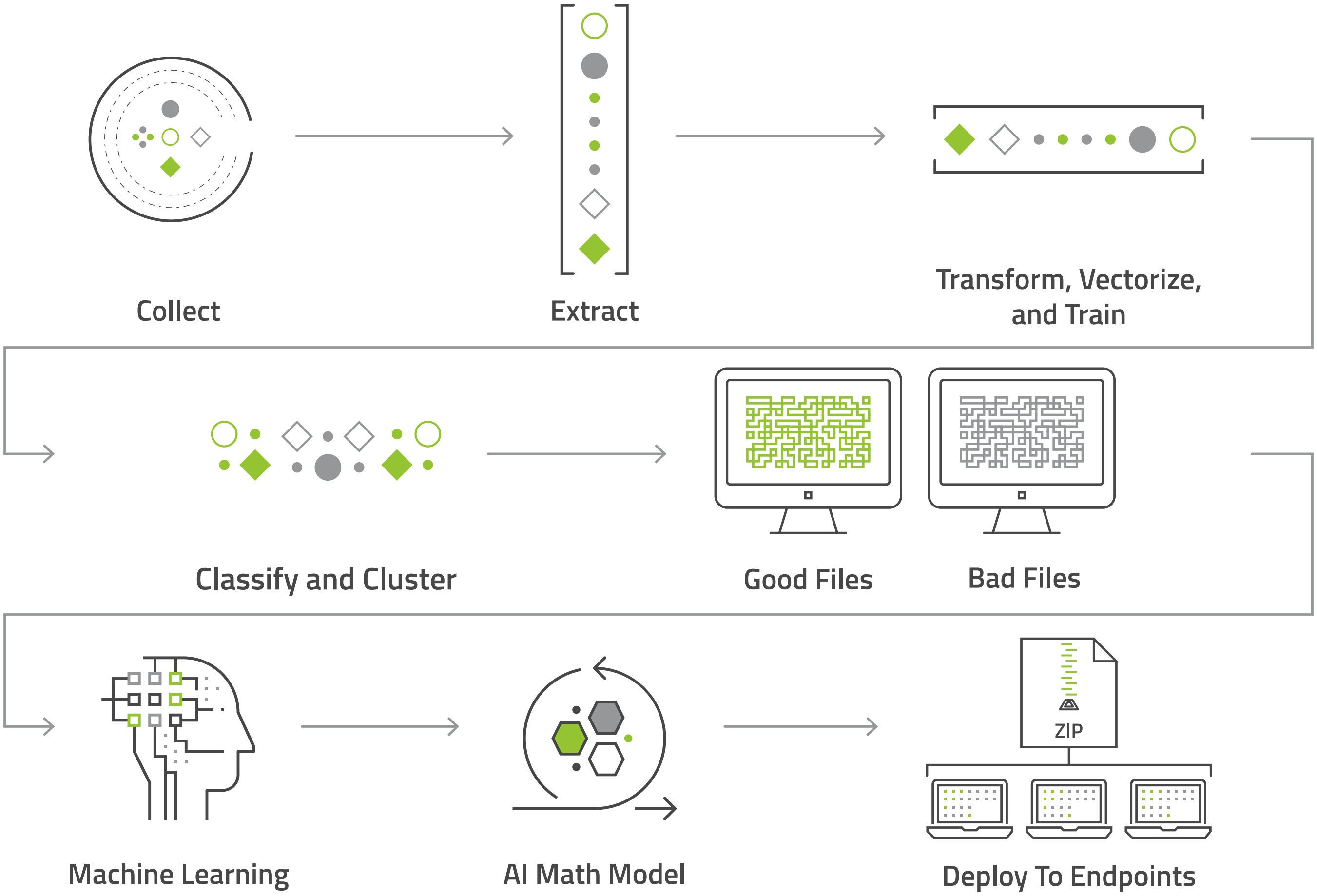
Unlike its competitors that require cloud connections, Cylance is cloud independent. Whether a user is online or offline, it protects at the endpoint. Cylance machine learning models don't need to be connected to the cloud. They operate with minimal impact to performance.

Effective machine learning requires vast quantities of data, which is one of the hurdles 21st century innovation has overcome. Big data and the Internet of things have helped produce data at unprecedented scale. The Cylance file database used to train models is extensive and ever expanding. With dedicated teams of data scientists, engineers, and researchers, as well as a globally expanding user community, the database continues to enrich and grow daily. Additionally, our latest algorithmic model was trained using our collection of over 2.8 billion code samples to recognize approximately 1.4 million threat features. This type of file disassembly is analogous to mapping the human genome to its genetic code with the ultimate goal of understanding the intent of a piece of software before it runs.

Machine learning requires a massive amount of data to process, and it needs equally massive compute processing. Cylance leverages hundreds of high-performance computing clusters that live in the cloud to build its artificial intelligence model. The result is fast, efficient pre-execution protection that works in milliseconds.

[1] NSS Labs Advanced Endpoint Protection: Cylance Security Value Map, April 2018

[2] SE Labs Intelligence-led Testing: Predictive Malware Response Time, March 2018



Cybersecurity vendors may make machine learning claims, but you can ask a few simple questions to determine for yourself.

1. Does the machine learning capability work without requiring a patient zero or sacrificial lamb?
2. How extensive is the machine learning math model and how many years has it been tested in the real world?
3. Do your cyberprevention capabilities prevent threats from executing?
4. Does the machine learning capability work both in connected and disconnected environments?
5. Can your protection work in milliseconds, with little impact to CPU usage?

Conclusion

Cylance machine learning has reinvented endpoint protection by providing predictive, preventative approaches that proactively stop attacks before they start.

Legacy AV could not fix the core of the problem, so vendors supplied layers of additional protection or in some cases, offered solutions they label as machine learning enabled. Yet these solutions still require a breach or sacrificial lamb and can't prevent threats never-before-seen or unknown.

True machine learning predicts and protects the endpoint pre-execution, takes advantage of sophisticated mathematical models that assess a file's intent, and achieves success rates previously unimaginable. It requires less technology and fewer resources, and analyzes files at the code-level — evaluating millions of variables to determine if it is malicious or benign. It works without cloud connectivity and at lightning speed to achieve greater than 99% efficacy.

Your Cybersecurity Resource

Cylance AI and machine learning protect organizations around the world, and it can protect you. For more information or to request a demo, visit www.cylance.com.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618