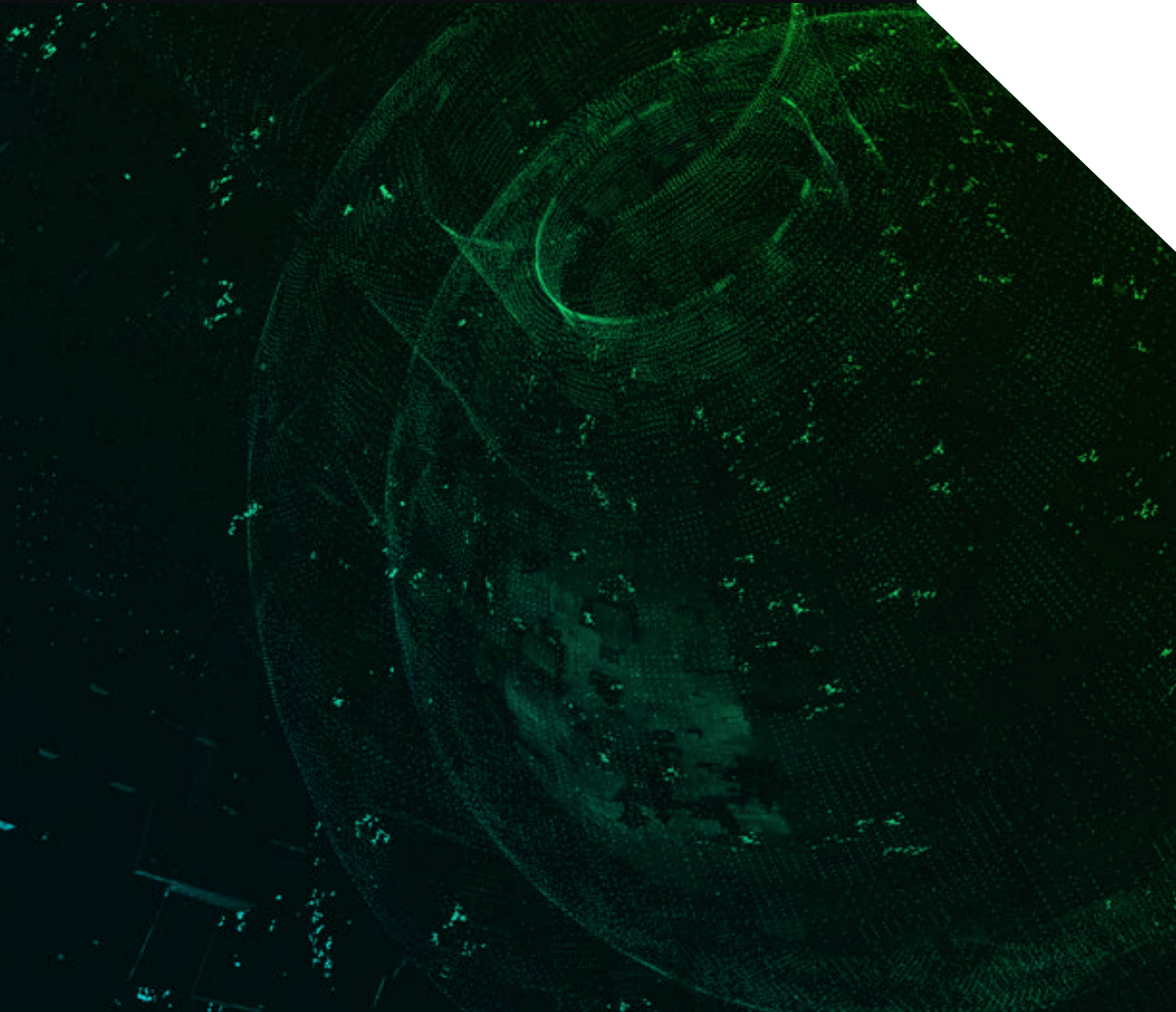



# Not All Artificial Intelligence Is Created Equal

Why BlackBerry Cylance Beats the Competition  
When It Comes To Endpoint Protection

WHITE PAPER





...more tech startups today tout AI to secure funding; and more established vendors now claim to embed AI in their product lines.

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

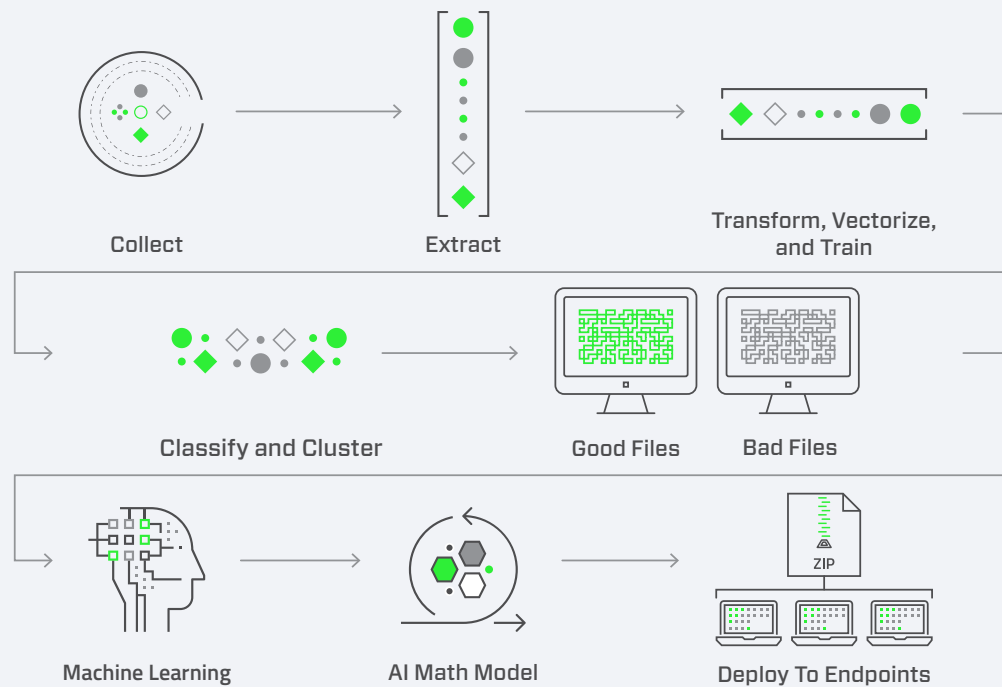
AI has only recently entered the world of cybersecurity, but it's occurring just in time. According to Gartner Research, the total market for all security will surpass \$100B in 2019. Companies are looking to spend on innovation to secure against cyber threats.

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

Yet the hype around AI — 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?

BlackBerry Cylance is a pioneer in applying AI to cybersecurity. The company spearheaded an innovation revolution by replacing legacy antivirus software with 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 BlackBerry Cylance Difference

So what makes BlackBerry Cylance AI stand out from the rest?

BlackBerry Cylance works because it:

- Achieves efficacy rates at or higher than 99.1%<sup>1</sup> (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, BlackBerry Cylance AI operates with unparalleled precision, preventing 99.1%<sup>1</sup> of existing and never-before-seen malware.

How? BlackBerry 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 AI, but their solutions require a patient zero, a user sacrificial lamb that must get breached by malware or a malicious payload in order to create an easily obfuscated signature. But BlackBerry Cylance AI does not require a sacrificial lamb, signatures, or even for the threats it blocks to be known. In fact, according to a report from NSS Labs,<sup>2</sup> BlackBerry® Cylance® technology has the ability to stop threats an average of 25 months before they are even created. Known as Predictive Advantage, this ability allows BlackBerry Cylance products to stop virtually all zero-day threats.

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

Effective AI 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 BlackBerry 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

<sup>1</sup>NSS Labs Advanced Endpoint Protection: Cylance Security Value Map, April 2018

<sup>2</sup>SE Labs Intelligence-led Testing: Predictive Malware Response Time, March 2018

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.

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

Cybersecurity vendors may claim to use AI, but you can ask a few simple questions to determine for yourself:

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

## Conclusion

BlackBerry Cylance AI has reinvented endpoint protection by providing 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 AI-enabled. Yet, these solutions still require a breach or sacrificial lamb and can't prevent never-before-seen or unknown threats.

True AI 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 99.1%<sup>1</sup> efficacy.

## Your Cybersecurity Resource

BlackBerry Cylance AI protects organizations around the world, and it can protect you.

For more information about new artificial-intelligence-based cybersecurity technologies that can secure all of your organization's endpoints, visit [www.cylance.com](http://www.cylance.com).

## About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.



+1-844-CYLANCE  
sales@cylance.com  
www.cylance.com

