Artificial Intelligence: The Platform of Choice

BlackBerry® | CYLANCE®

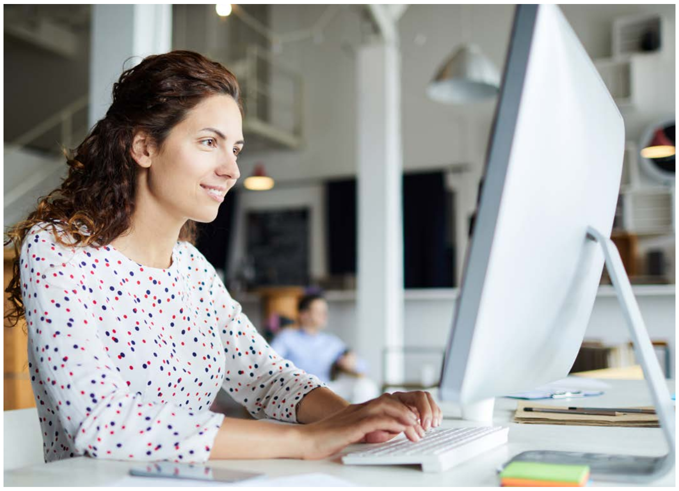
Separating Science from Fiction

Artificial intelligence (AI) leads the charge in the current wave of digital transformation underway at many global companies. Organizations large and small are actively expanding their AI footprints as executives try to comprehend more fully what AI is and how they can use it to capitalize on business opportunities by gaining insight to the data they collect that enables them to engage with customers and hone a competitive edge. But, while AI may indeed be the frontier of enterprise technology, there remain many misconceptions about it.

Part of the confusion stems from the fact that AI is an umbrella term that covers a range of technologies — including machine learning, computer vision, natural language processing, deep learning, and more — that are in various stages of development and deployment. The use of AI for dynamic pricing and targeted marketing has been in use for a while, but actual AI computing where machines think like humans is still many years from becoming mainstream. The various possibilities between these poles prompt a range of reactions from people who understand different aspects of AI's disruptive potential.

As a field, AI encompasses three distinct practice areas:

- Artificial superintelligence is the type popularized in speculative fiction and in movies such as *The Matrix*. The goal of this type of research is to produce computers that are superior to humans in virtually every way, possessing what author and analyst William Bryk referred to as "perfect memory and unlimited analytical power."
- Artificial general intelligence refers to a machine that is as intelligent as a human and equally capable of solving a broad range of problems that require learning and reasoning.
- Artificial narrow intelligence exploits a computer's superior ability to process vast quantities of data and detect patterns and relationships that would otherwise be difficult (or impossible) for a human to detect manually, as is used in the fields of cybersecurity and other big data applications.



AI in the Enterprise

Companies have begun investing in AI in order to make better use of the data they gather and the increased computing power to which they have access. According to a recent McKinsey Global Institute Report[1], AI investments were between $26 billion and $39 billion in 2017, a three-fold increase over the previous three years. Research firm IDC predicts enterprise spending on AI[2] and cognitive computing to grow to $46 billion by 2020.

AI is used to forecast electricity demand at utility companies, to train vehicles to become chauffeurs and truck drivers, and to power robots that pack and ship Amazon orders. Netflix, for example, says the AI algorithm behind its search-and-recommendation engine has saved it $1 billion[3] in potential annual losses from canceled subscriptions. Early adopters of the technology tend to be technology, telecommunications, and financial services firms that deploy AI across technology groups and as a core part of their business. One thing they all have in common? All successful deployments have the full support of executive leadership.

Security, Risk, and AI

The use of AI can change the nature of the work people do, moving labor away from menial tasks to more strategic functions. It can be used to parse through data about customers, operations, business activities, and other processes that staff cannot compute or manage manually. But, AI can't operate on its own or in a vacuum. It needs humans to create the knowledge trees upon which it learns, to train algorithms to become more sophisticated, and to perform system maintenance.

For example, AI helps security practitioners identify threats across an expanding attack surface (think: mobile, cloud services, and the Internet of things) by automating data aggregation across different data files, mapping them back to compliance requirements, and ruling out false positives. AI also helps security teams assess risk and potential harm from threats that target specific internal and external data regarding security protocols, exploits, malware, and threat actors. In addition, AI can automate remediation processes that are used for incident reporting that can be augmented by human analysis to boost effectiveness and reliability. Remember, AI does not just detect threats, it also stops attacks from executing in the first place, thereby preventing future incidents.

The increased need for AI to assist with staff augmentation has enterprises actively seeking employees who have familiarity with the technology to help expand business capabilities — and job seekers are responding to that need. 64% of respondents in a recent security investment survey[4] feel that more candidates at every level are using AI as a differentiator on their resumes and in interviews. Respondents also reported that these skills are a critical deciding factor in the hiring process.

More than two-thirds of survey respondents have been able to prevent more breaches since they began using AI-powered tools. Four-fifths said AI detected threats before their security teams could, and found threats humans couldn't see. In other words, AI tools — and BlackBerry® Cylance® believes native AI technologies have the advantage here — are one of the most valuable weapons in the threat-prevention arsenal.

AI doesn't just make systems smarter. It makes employees smarter, too, by enabling security practitioners to expand their competency. There are chatbot applications designed to help mentor junior security team members to use specific technologies and AI that adjusts the information it presents based on user knowledge. As IT departments try to attract employees across a broader range of skill levels, AI security products will evolve to become more flexible in terms of the assumptions about users' backgrounds and be more proactive about helping them learn.

Augmenting talent with robust AI solutions can also help close the technology skills gap. The talent shortfall, especially in cybersecurity, is well documented and often remarked upon. Some analysts predict that by 2022, the global shortage of cybersecurity professionals could reach 1.8 million.[5]

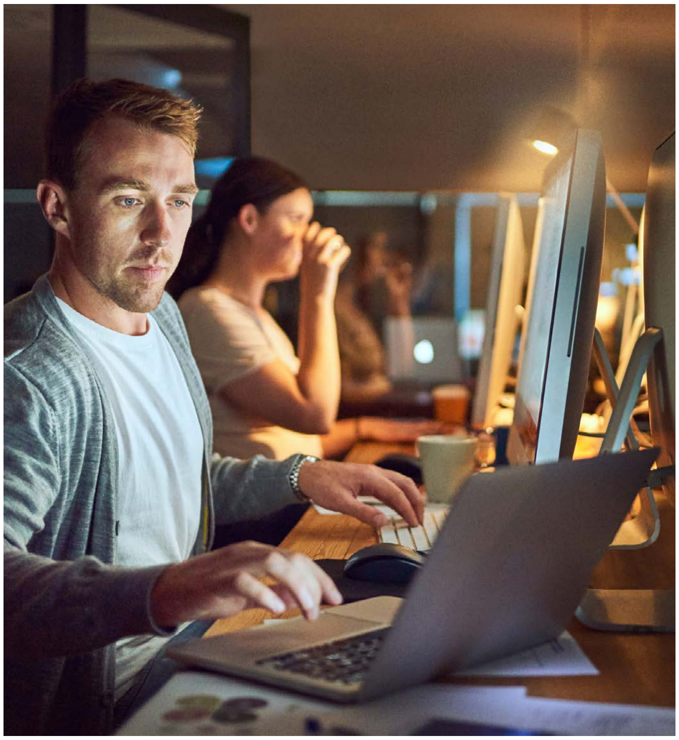
While there are many security solutions in the market that are adding AI and machine learning capabilities, there also AI technologies that are emerging to solve market needs from an entirely different perspective.

The BlackBerry Cylance AI Platform™

Most security providers claim to use AI or machine learning in their product and services offerings. While this may be true in that providers can optimize and automate some aspects of their heuristics or signature-generation processes, such activity falls well short of the full promise of AI to prevent against future threats.

BlackBerry Cylance has built the largest native AI platform in the security industry, enabling it to offer a portfolio of solutions ranging from enterprise endpoint protection, detection, and response, to smart antivirus for consumers, to OEM solutions. The platform is resilient and requires only minimal updates to its multigenerational AI models. It also provides powerful data science capabilities using deep learning algorithms designed to detect anomalous patterns.

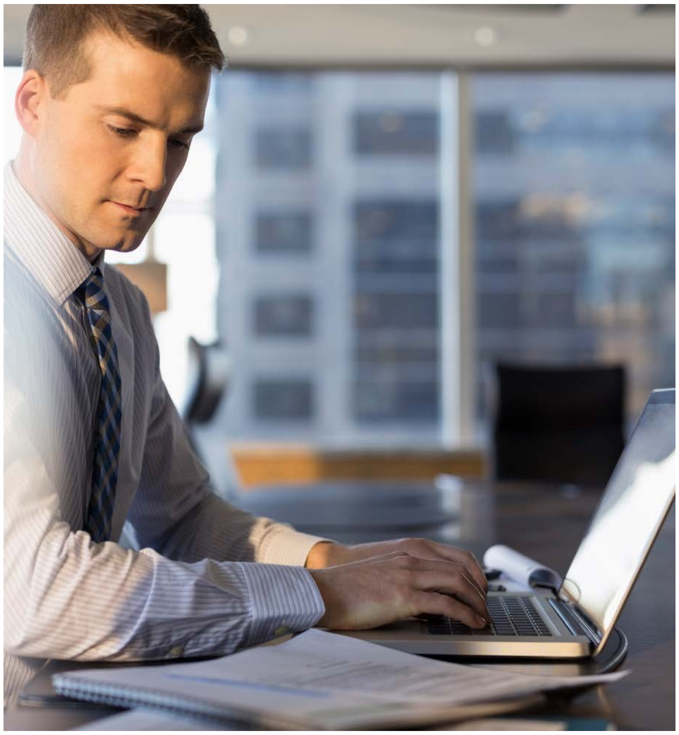
The BlackBerry Cylance AI Platform is a unified technology architecture built on continuous integration and continuous delivery principles (also known as CICD principles) to drive a high velocity of capabilities through native AI endpoint security solutions and delivers continuous threat prevention, detection, and response regardless of whether the endpoint resides on or off the network.



With the platform approach of native AI security addressing prevention, detection, and response across the kill chain, security teams benefit from AI-driven automation, combined with prevention, that delivers sharply reduced dwell times and containment times, as well as increased ROI. For security teams with limited security expertise, the BlackBerry Cylance AI Platform can run as a self-driving security operations center where response to active threats can be initiated without any human intervention. For senior teams that want a more hands-on approach to response, the BlackBerry Cylance AI Platform can deliver the critical data required to make response decisions in a powerful, yet simple to use, interface. This flexibility means that the BlackBerry Cylance AI Platform can help companies of any size, from a lean startup to large multinational organizations, improve their security posture.

To further extend the advantages of an AI platform, BlackBerry Cylance offers an open API architecture that enables organizations to integrate the BlackBerry Cylance AI Platform with their existing security environments and achieve the associated prevention and automation benefits. Easy integration and streamlined data sharing across a variety of technology tools support the best-of-breed deployment that security leaders prefer and a strong ROI on existing investments.

With a platform for rich threat research and intelligence (R&I), the BlackBerry Cylance R&I team brings forward critical discoveries in the threat landscape, uncovering advanced cyber crime and nation-state operations such as The White Company — a state-sponsored actor that launched several international attacks, including Operation Shaheen, which exposed a complex set of attacks targeted at a specific country.



Native AI: The Secret Sauce

Importantly, the BlackBerry Cylance AI Platform delivers a predictive advantage against never-before-seen malware an average of 25 months before it appears online. BlackBerry Cylance deployed malware conviction models in customer environments that were able to detect and block the top 10 malware attacks of 2017 — including WannaCry and NotPetya — an average of two years before those attacks were first detected in the wild.[6] This proven over-the-horizon prevention capability against known and unknown malware is the predictive advantage that only a native AI solution can provide, and BlackBerry Cylance is the only vendor to offer such a sophisticated capability. The obvious benefits to predictive advantage include protection from zero-day polymorphic attacks and packed or obscured malware, which in turn boosts an organization's security posture and allows staff to support more strategic initiatives.

Futureproof Security

BlackBerry Cylance believes the native use of AI against known and unknown threats is disruptive because it delivers significantly more effective results at prevention, detection, and response, and that a data-science-led approach to strengthen AI models against future threat variants offers a clear advantage over solutions that use AI as a plugin or add-on feature.

Having successfully applied AI to prevent threats from executing at the endpoint, BlackBerry Cylance has now advanced to another innovative use of native AI: to detect and respond to threats. By applying machine learning to threat-detection modules, the BlackBerry Cylance AI Platform continuously analyzes changes occurring on each endpoint to uncover threats that would be difficult, if not impossible, for a human analyst to find quickly enough to mitigate. When a potential threat is identified, the BlackBerry Cylance AI Platform can take decisive, automated action in real time to thwart it. Organizations can also launch BlackBerry Cylance-supported custom controls to uncover hidden threats specific to user environments.

The BlackBerry Cylance AI Platform is designed to move beyond a device-centric construct to a multidimensional one, including a user-centric dimension, with AI models and machine-learning algorithms for user context to formulate a trust assessment (or behavior score) that can be used to manage risk of insider threats or compromised credentials.

As enterprises continue to drive digital transformation, there is a necessary disruption of security architectures required to drive the balance of risk, cost, and business velocity. The use and application of AI as a platform is central to this disruption. The BlackBerry Cylance AI Platform is focused on driving this necessary disruption with continual evolution of AI models that will deepen the insight and prevention capabilities across devices, users, and data.

Reference

1. *McKinsey Global Institute, Artificial Intelligence The Next Digital Frontier; June 2017*
2. *IDC, Worldwide Spending On Cognitive and Artificial intelligence Systems Will Grow to $19.1 Billion in 2018; March 2018*
3. *Business Insider, Why Netflix thinks its personalized recommendation engine is worth $1 billion per year; June, 2016*
4. *Cylance, Artificial Intelligence in the Enterprise: The Race Is On*
5. *The Global Information Security Workforce Study, 2017*
6. *SE Labs Intelligence Testing, Predictive Malware Response Test, March 2018*

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