BlackBerry
Intelligent Security. Everywhere.

White Paper

BlackBerry vs. Traditional AV Solutions

Preventing Threats with Artificial Intelligence and Machine Learning

Executive Summary

A few years ago, a proactive prevention-based security posture was more an aspiration than a reality. Legacy AV tools relied on signature hash matching and heuristics to detect malware. Often, they required a suspect file to execute on, and subsequently infect, an endpoint before it could be judged malicious. Others required massive volumes of data to be sent to the cloud to be analyzed, introducing unacceptable delays in detection and response. All these approaches are inherently reactive.

In an era when 350,000 new malware variants are released into the wild each and every day, traditional approaches to endpoint defense are no longer viable. Yet, perhaps out of inertia, some organizations still cling to a traditional, reactive approach to cybersecurity that has long since passed its expiry date. Fortunately, a prevention-first security approach based on artificial intelligence (AI), machine learning (ML), and automation is both proven and practical.

Why Traditional AV Solutions Fail

Traditional AV solutions are ineffective at thwarting modern threats because they rely on detection methods that can all too easily be circumvented.

Signature Matching

A signature is a unique string of bits that functions as a malware file's digital fingerprint. Each time a traditional AV product encounters a new file, it compares a byte in the file to bytes in its signature database. If a match is found, the AV product continues this sequential byte-by-byte matching process until the entire file has been inspected. To be flagged as malware, every byte in the examined file must match every byte in the signature exactly. However, signature-based tools can easily be evaded if an attacker modifies or obfuscates their code or if the AV vendor has yet to complete the tedious manual process of creating and distributing a signature update for one of the 350,000 new malware variants released in the wild each day[1]. This byte-by-byte matching process is often so resource-intensive that endpoints can become unresponsive or unstable during scans, inconveniencing end-users and reducing their productivity. Signature-based AV is also management-intensive because it requires staff to download, install, distribute, and audit an ongoing stream of signature file updates.

Heuristic Approaches

Heuristics approaches utilize code matching, rather than signature matching, to identify malware. In static heuristic analysis, a suspect program is decompiled so that its source code can be compared to the source code of malware in a heuristics database. If the match meets the specified percentage of similarity, the suspect program is classified as malware. In dynamic heuristics, the binary is safely isolated in a virtual machine, or sandbox, where it's allowed to run so that the heuristics can intercept each function in the execution sequence and determine what the code is designed to do. If the code over-writes files, attempts to self-replicate, or performs

[1] AV-TEST Institute

other suspicious actions associated with malware, then the suspect program will be flagged as malware and quarantined.

Heuristics approaches have similar limitations to those of signature-matching methods because they require lookups to a remote database, which delays the detection process. In addition, since the same functions can be used in both malicious and legitimate ways, heuristic approaches are prone to classifying benign files as malware, blocking necessary functions, and generating high rates of false positive detections.

Hash-Matching Approaches

Hash functions are algorithms that utilize compression and encryption techniques to transform a sequence of binary data of any length into a string of characters with a fixed length. If two files have the same hash values, then they can be judged to be identical. Legacy AV products that use hash matching compare the computed hash value of a suspect file with the hash of known malware. If they match exactly, the suspect file is classified as malware. However, changing even a single bit in the suspect binary will produce a completely different hash value. Consequently, hash matching techniques are easily evaded by polymorphic and single-use malware.

To partially offset the limitations of these approaches, many vendors are jumping on the bandwagon and claiming that their solutions also incorporate AI and ML technologies. However, if you examine their products closely, you will discover they are using them to generate signatures, heuristics, or hashes, which must then be vetted manually. Otherwise, they will fail to stop malware or instead block benign files, resulting in high rates of false negative and false positive detections.

How BlackBerry Leverages the Power of AI and Machine Learning

Instead of signatures, hashes, and heuristics, BlackBerry® Cyber Suite utilizes AI and ML algorithms to build predictive models that automatically detect threats and prevent malicious code from executing.

Supervised vs. Unsupervised Learning

In supervised learning, a data scientist builds a model with samples that have already been identified, or labeled, with respect to the property under investigation. BlackBerry® Protect models, for example, are trained on a vast data set of known safe and unsafe executable files to detect and prevent the execution of malware and malicious scripts. Classification is an example of a supervised learning method.

In unsupervised learning, the properties that distinguish one group of samples from another are unknown and must be discovered by the algorithm. Unsupervised learning methods are effective, for example, at detecting anomalous behavior patterns, like those that enable BlackBerry® Persona to perform continuous authentication. Clustering is an example of an unsupervised learning method. When solving complex problems, it's common practice for data scientists to use both unsupervised and supervised learning methods in combination.

BlackBerry data scientists build models using an immense crowdsourced data set of known safe and unsafe executable files in Microsoft® Windows®, macOS®, Linux®, iOS®, and Android™ frameworks. A statistically valid sample of these files is selected and then disassembled by algorithms into their constituent building blocks, known as features. These include such attributes as file size, signing attributes, string data, icon, imports, permissions in a data section, packers, compiler type and language, headers, directories, and more than a million more. Any static element that can be pulled from memory or from disk into memory can be analyzed. These features are then formatted for efficient processing and analyzed using both supervised and unsupervised machine learning methods.

The resulting models are rigorously tested and optimized to differentiate between safe and unsafe executables with more than 99% accuracy[2]. The training data set is continuously expanding, allowing the models to continue learning and improving in their abilities to accurately detect both existing and future forms of malware.

AI and Machine Learning in Action

Consider the example of a BlackBerry® predictive model built with a deep neural network, a complex branched system of nodes and layers, that feeds back into itself to continually improve its detection accuracy. The model can be visualized as an enormous and complex maze, where each of the millions of features and feature combinations are individually assessed and weighted.

Once optimized and deployed, the model dis-assembles each incoming file and assesses its features layer-by-layer based on their presence, absence, and weighted values. In the final layer, the model completes its analysis by generating a confidence score that predicts whether the file is malicious or benign. The entire process takes milliseconds to complete and executes locally on the endpoint.

To create malware capable of evading detection, the attacker would have to reverse-engineer the model by back-tracking through each layer and determining the computations performed at each node. This is equivalent to attempting to traverse a maze with thousands of pathways both backwards and blindfolded.

Why Choose BlackBerry as Your Endpoint Security Partner?

BlackBerry Cyber Suite enables organizations to safeguard their desktop, server, and mobile devices with unparalleled effectiveness, ease of use, and minimal system impact. Working together, BlackBerry Cyber Suite solutions provide the unified threat prevention and policy management capabilities organizations need to optimize their resilience and enhance their productivity:

- **BlackBerry Protect** is an endpoint protection platform (EPP) solution that utilizes AI and machine learning to prevent the execution of malware on Microsoft Windows, macOS, and Linux systems. The solution also protects

[2] NSS Cylance Security Value Map™(SVM)

endpoints with advanced script and application control, memory protection, and device control features. All protection is applied at the endpoint automatically, without any reliance on cloud lookups or a network connection.

- **BlackBerry® Protect Mobile** is a mobile threat defense (MTD) solution that provides iOS and Android users with advanced AI-driven threat protection at the device and application levels.
- **BlackBerry® Optics** is an endpoint detection and response (EDR) solution that augments BlackBerry Protect by utilizing AI, context analysis, and MITRE ATT&CK® framework rules to detect advanced threats and automate the incident investigation and response processes with playbook-driven workflows.
- **BlackBerry Persona** is a continuous authentication solution that utilizes behavioral analytic models at the endpoint to compute trust scores and control user access to enterprise assets.

BlackBerry Cyber Suite architecture consists of a lightweight unified agent that is managed via the BlackBerry SaaS-based cloud console. The console easily integrates with existing software management systems and security tools. Hybrid and on-premises management options are available for air-gapped environments.

Fully integrated, the solutions work together seamlessly, sharing data for reporting, calculating risk, and enabling policy control across domains. And since AI sustains and connects them, they can continuously leverage and learn from one other, thereby reducing the chaos of the battlespace and the complexity of the security infrastructure.

Endpoint Protection: BlackBerry Cyber Suite

Capability	BlackBerry Protect	Legacy AV
Malware detection	Proactive, powered by AI and ML.	Reactive, relies primarily on signatures, heuristics, and cloud look-ups to a threat database.
Pre-execution prevention	Yes. Malware and malicious scripts are prevented from executing.	No. Malware must almost always detonate to be detected.
Stopping zero-day malware	Yes.	No.
Blocking malicious scripts and fileless attacks	Yes.	Only if heuristics match attack method.
Application control	Yes. Preserves system and configuration integrity of fixed-function devices.	Varies with product.
Device usage control	Yes. Prevents infections from infected mass storage devices.	Varies with product and availability of malware signature.

Endpoint Protection: BlackBerry Cyber Suite		
Capability	**BlackBerry Protect**	**Legacy AV**
Autonomous protection	Yes. All malware prevention and security policy enforcement occur at the endpoint.	No. Cloud connection usually required. Protection can rapidly degrade if the endpoint is offline, even for short periods.
System performance	Transparent to end-users. Consumes minimal system resources and requires no intrusive scans.	Intrusive to end-users. Causes system performance issues, especially during frequent required scans.
Threat management	Signatureless and prevention-first approach minimizes management overhead.	Requires significant overhead to manage signatures and re-image infected systems.
Leveraging AI and ML	Core technology used throughout BlackBerry Cyber Suite.	Peripheral technology. Often used to supplement legacy AV methods or generate signatures and heuristics.

To complement these solutions, BlackBerry® Security Services offers an extensive portfolio of cybersecurity consulting and professional services to assist clients in their transition from a reactive to a prevention-first security posture. Together, BlackBerry software and services solutions enable clients to enhance their resilience while realizing a rapid return on their security investment.

Visit our website for more information, or to arrange a BlackBerry Cyber Suite proof of concept.

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 175M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

BlackBerry. Intelligent Security. Everywhere.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.