Artificial Intelligence:

The Smarter Approach To Information Security

Traditional AV solutions are no match for today's sophisticated attacks.

BlackBerry | CYLANCE

BlackBerry | CYLANCE

Contents

The Current Threat Landscape

The news headlines are replete with stories of devastating data breaches, compromising the personal and professional data of millions. Cyber attackers spare no industry, infiltrating the assets of even the most sophisticated technology adopters, in turn impacting their executives, employees, and perhaps worst of all — customers and users.

All of which beg the question:

WHAT'S GOING WRONG?

The answer lies not in changing the motives of bad actors, but rather, in the advanced techniques that help them evade traditional methods of system protection. Traditional AV solutions, which adopt a reactive approach to cyber attacks, are ineffective at preventing breaches, relying solely on continually updated signatures or patches to address known threats. But, threats are quickly evolving and multiplying, overwhelming these traditional systems. And, the damage has been staggering.

SINCE 2014, SIGNIFICANT CYBER ATTACKS HAVE INCREASED BY

230%

The Center for Strategic and International Studies has been tracking significant cyber incidents since 2006. They define a significant attack as one that targets "government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars."[1] Their research concludes that significant cyber attacks have increased 230% since 2014. In recent years, armed with knowledge stolen from the CIA and tools lifted from the NSA, threat actors have demonstrated an elevated level of proficiency.

To fully understand how these and other threats evade traditional defenses, it's critical to understand their characteristics and methodologies.

1 Significant Cyber Incidents, (CSIS, 2018)

Single-Use, Highly Targeted Malware

Part of the exponential growth of malware, and the bulk of the attacks on various industries, can be attributed to the continued rise in polymorphic and single-use malware.

There is a general misconception that publicly available repositories of malware signatures are a complete catalog of in-the-wild malware. This misguided perception is further elevated by thin endpoint controls that rely on looking up hashes or validating binaries against these public sources to determine if a file is a threat. But, public repositories of signatures are by no means comprehensive, complete, up-to-date, or a reliable record of all the malware that could impact an organization.

Malicious actors do not want their creations to end up on public malware lists (or otherwise in-the-wild) and frequently take steps to ensure that does not occur. They often use single-use or host/campaign-specific binaries to remain hidden.

It is also well known that attackers take steps to complicate and inhibit analysis of their creations if they are discovered. As a result, the most worrisome malware, from the high-level commodity code to the ultra-sophisticated targeted attacks, will never show up in repositories, making them undetectable to traditional AV solutions.

Successful malicious campaigns often remain hidden or dwell for months or even years before components become known. Even at that point, it is often only by a stroke of luck that a file gets uploaded to a public repository, starting the chain of events where it is picked up by other analysts, pivoted upon, and exposed for what it is.

MALICIOUS ACTORS DO NOT WANT THEIR CREATIONS TO END UP ON PUBLIC MALWARE LISTS.

Fileless vs. Script-Heavy Attacks

Advancements in fileless attacks are providing new ways for threats to hide from once reliable detection methods. The definition of a fileless attack has been somewhat stretched over the last few years.

Malware that stays fully memory-resident and does not rely on additional script execution is completely fileless. However, the use of additional scripts (JavaScript, PowerShell, etc.) to enhance evasion and persistence enter and present a gray area of what should be called script-heavy attacks. An example would be Cerber's use of JavaScript/VB to download final payloads, or delay payload execution by calling an additional PowerShell script to then download and detonate.

The initial stages of attack, in the Cerber scenario, are not the full malware payload, but there are still files involved during these stages. The same holds true for attacks initiated via malicious documents with Macros/VB or other forms of embedded code.

Fileless attacks are attractive to malicious actors because of their enhanced evasion, stealth, and persistence, but we need to be precise in how we use the term fileless so as to accurately describe what is really occurring during these attacks.

Ransomware

Meanwhile, new opportunities developed in ransomware-as-a-service (RaaS), opening the gates of malware-for-profit to everyone. Ransomware encrypts data then often extorts users by selling them a decryption key.

RANSOMWARE ENCRYPTS DATA THEN OFTEN EXTORTS USERS BY SELLING THEM A DECRYPTION KEY.

This is not a new or novel phenomenon. In 2016 and 2017, the sheer velocity of ransomware attacks was overwhelming for the majority of industries and security teams, growing threefold and affecting users across 160 countries and 16 different industries. However, ransomware attacks then decreased sharply as cryptocurrency mining, or cryptojacking, took over in popularity. In 2018, ransomware was nowhere near the most common or popular vector of infection, however, it still remains a popular strategy of attack as is evidenced by the ransomware attack on the City of Atlanta in March 2018.

Traditional solutions are vulnerable to ransomware due to two inherent shortcomings: They either must wait for a signature to ensure detection, or they react too slowly when the infection takes hold and continues on its path. This can be the result of cloud-based lookups for conviction or the lack of pre-execution controls. Cyber attackers are well aware of these weaknesses and continue to exploit them with ransomware attacks that make headlines each day. Today, ransomware represents a multi-million dollar criminal enterprise costing companies and governments billions in collective losses worldwide[2], with Wannacry one of the most damaging and persistent to ever impact businesses and governments around the world.

Victims of WannaCry are impacted when they click on a phishing email that delivers a .zip file disguised as a fake invoice, job offer, security warning, undelivered email, etc. Once the infection takes place, it encrypts its victim's files using the AES cipher and demands a ransom that increases in value as time passes.

WannaCry

First detected on Friday, May 12, 2017, *and still ongoing*, ransomware threat WannaCry (aka WannaCrypt, WCry, WanaCryptOr 2.0, or Wanna Decryptor) is an example of a ransomware variant. Leveraging a vulnerability within Windows operating systems, WannaCry uses an exploit called EternalBlue to automatically target and propagate itself to vulnerable Microsoft Windows operating systems across the Internet. The EternalBlue exploit is reportedly just one of the tools believed to have originally belonged to the National Security Agency (NSA), which was stolen and dumped by the group self-identified as The Shadow Brokers.

---

2 Morgan, Steve "Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017", Cybersecurity Ventures, 28 May 2017, https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

To date, WannaCry has infected thousands of endpoints, including some very high-profile targets. The U.K.'s National Health Service was torpedoed by Wannacry and forced to put life-saving surgeries on hold. Spanish telecom provider Telefonica sent employees home after the infection tore through its offices in May 2017. Russia's Ministry of Internal Affairs reported more than 1,000 infections. Germany's rail system was hit with WannaCry's ransom message appearing on train station pay terminals.

To Err Is Human

While these attacks are sophisticated in avoiding detection, their destructive powers are moot without a pathway for infection. The top two infection vectors include email and drive-by-downloads. Both are the result of human error, a shortcoming that can be minimized with training and education. No matter how vigilant, though, human error will persist, exposing the limitations of legacy solutions that merely detect attacks, not prevent them from executing on endpoints in the first place.

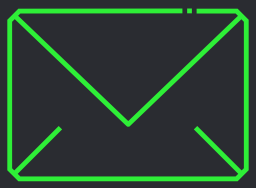
An Economic Model for Failure

The reactive nature of legacy AV protection has led to a proliferation of inefficient and ineffective solutions. This expansion can be understood by looking at the repeated failures through an economic lens.

The primary cause of economic inefficiency is the misallocation of resources. To understand how the information security sector has traditionally mishandled resources, we must examine how the industry develops solutions. Antivirus software and other security solutions evolve by crafting responses to new threats. Each new solution adds a layer of protection to the last.

While this method of responding to threats is completely understandable, it is not particularly efficient. Every layer of protection may require additional resources. Following a pattern of erecting new defenses to address emerging threats ultimately leaves security solutions top heavy and demanding on resources.

THE TOP TWO INFECTION VECTORS INCLUDE EMAIL AND DRIVE-BY DOWNLOADS.



The end result is inefficiency. Every minute dedicated to learning new systems or processing additional security data diverts time and resources away from the core business.

Cybersecurity stocks of antivirus companies and ETFs typically rise (often dramatically) in the wake of ransomware attacks, a counter-intuitive profit increase that inhibits, not encourages, change. An industry built upon providing secure computing should not profit from failures. Consider the economic ramifications that occurred when mad cow disease appeared in the United States. American ranchers did not reap higher prices for cattle. On the contrary, the U.S. beef industry lost almost $11 billion over three years. A public failure routinely causes a market reaction whether a company sells automobiles, fast food, or smartphones. Yet, the information security sector has proven an exception to the rule, largely because of misplaced public trust.

Multiple layers of new protections built upon legacy solutions introduce control frictions into the environment. This directly impacts productivity, which results in inefficiency. Yet, there is little financial impetus on traditional solution providers to change.

AN INDUSTRY BUILT UPON PROVIDING SECURE COMPUTING SHOULD NOT PROFIT FROM FAILURES.

Why Traditional Approaches Fail

Traditional AV solutions lack the inherent capabilities to combat today's sophisticated cyber attacks because they generally rely upon the following strategies:

1. Pattern or Byte Matching

Pattern matching is used to check a sequence of tokens for the presence of the constituents (parts) of a pattern. In contrast to the flexibility offered by pattern recognition, the match must be absolutely exact.

A signature is the digital fingerprint of a piece of malware. It contains a unique string of bits, with a binary pattern representing the malware. Each time a traditional AV product encounters a new file, the AV product looks through its signature list to determine whether the byte in the signature matches the byte in the file. If it does, it moves on and checks the next byte. It continues through the whole file in this way. If every byte of the file matches every byte in one of its signatures, exactly, it flags the file as malware.

Attackers easily bypass signatures by mutating, obfuscating, or otherwise changing the code in their malware. If a single byte is changed in any of the signature's important values, then the signature no longer matches the malware. It becomes toothless, to the extent that a single recompilation with different strings easily evades most signature detection algorithms.

2. Heuristic Approaches

A second AV approach incorporates heuristics (see sidebar). The AV looks at loose properties of the file, such as its size or permissions. The AV then matches things that aren't in the code directly. One example of how this might work is by asking the following questions of the file:

- Does the executable import VirtualAlloc?
- Is the executable greater than 30KB and less than 75KB?
- Does the executable have a section whose permissions are read, write, and execute?
- If these things are true, then it is a virus.

Traditional AV relies heavily on this set of rules to convict a sample, which is easily evaded by cyber attackers. The problem with this approach is that the attacker need only change a single feature, and changing that one feature breaks down the detection ability.

3. Behavioral Analysis

A third AV approach incorporates behavioral analysis, which targets the behavior exhibited by malware by assessing:

- What is the file doing on a file system level?
- What is the file doing on a registry level?
- What is the file doing on a process level?
- What is the file doing on a network level?

This approach is inherently vulnerable, as the malware must run before the AV product can detect it.

What are heuristics?

Heuristics are a set of rules (as opposed to a specific set of program instructions) that are used to detect malicious behavior without having to actually identify the program responsible for it.

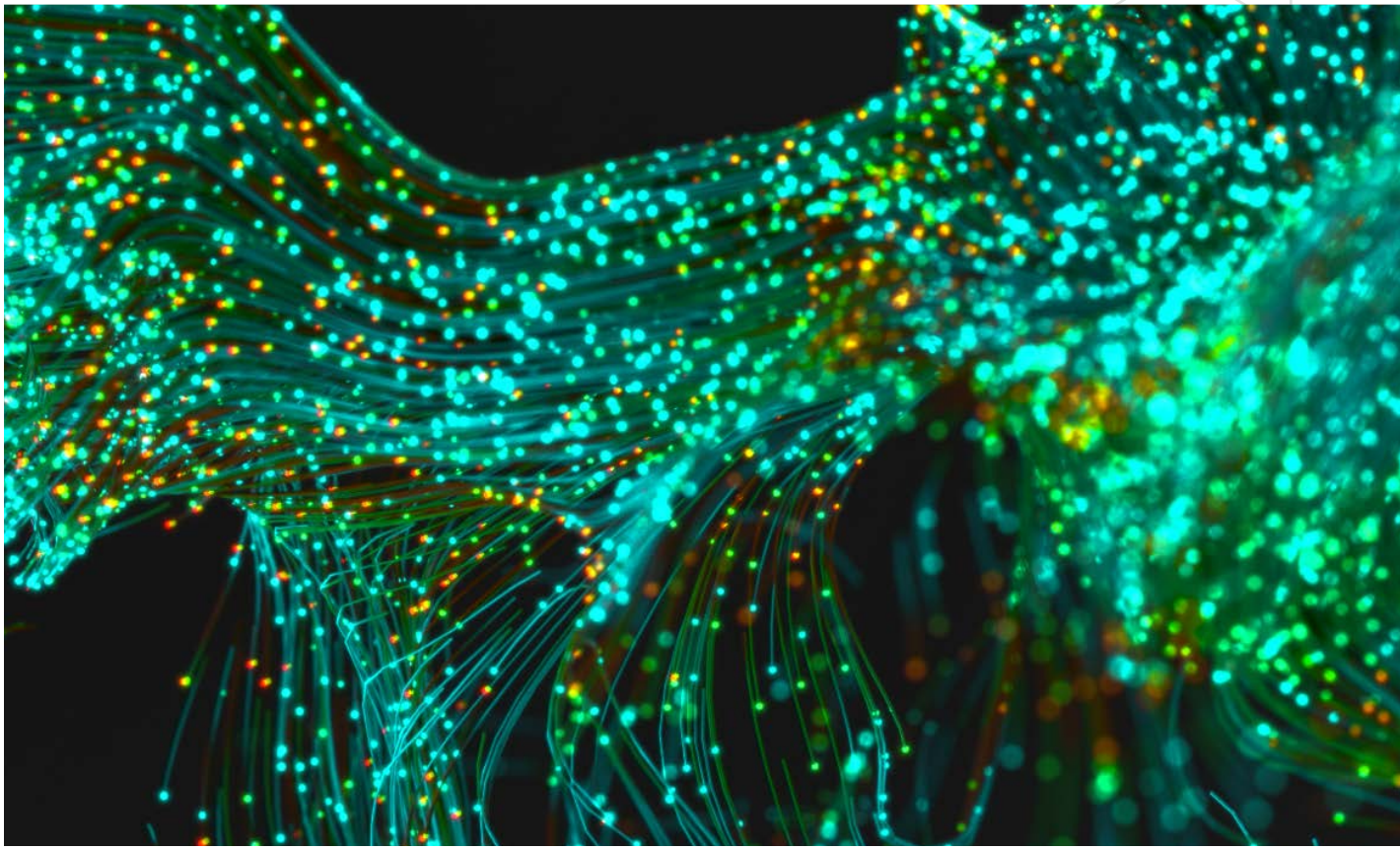
4. Hash-Based Approaches

Finally, AV also uses hash matching, calculating hashes over different parts of the file and then taking a hash over a certain area of the executables (MD5, SHA256, CRC32). The AV analyzes that hash to see if it matches the hash of a known virus. If it does, then the AV designates the file as a virus.

Sometimes, engines will review multiple hashes across the binary to determine matches. For instance, it may divide the file into 1024-byte chunks, removing the hashes from all of them to see whether any match a virus.

However, if a single bit gets changed in any of the areas used to generate the hashes, the hashes produced are wildly different. An attacker need only change one bit of the file to compromise the system.

What Artificial-Intelligence-Driven Solutions Do Better



Fortunately, information security has evolved, with smarter, more powerful solutions available to protect systems and their endpoints. Some of the new approaches now offer proactive protection, operating pre-execution, and therefore preventing breaches, instead of merely reacting to them. The evolution presents a more intelligent and efficient approach to security, no matter the sophistication of the attacker or threat.

Better. Faster. Stronger.

The introduction of artificial intelligence as a foundation for enterprise security fulfills the promise to automate many endpoint security tasks, eliminating many of the issues that hamper traditional AV solutions. At BlackBerry Cylance, we leverage a foundation of AI to deliver a signatureless approach that detects the authenticity of files in just milliseconds, preventing malicious applications from executing.

Our approach has studied billions of files and currently measures 1.4 million features, which are extrapolated for analysis and used to train our machine learning models. Simple examples of these features could be the file length, the use of digital certificates (which are often legitimate but can be stolen), whether the file is using a packer, and the complexity or entropy of the file. Instead of looking at five or 10 features to determine file legitimacy, our machine learning algorithm looks at 1.4 million. This exhaustive approach, with its enormous reference base, dramatically minimizes the risk of a malicious file executing.

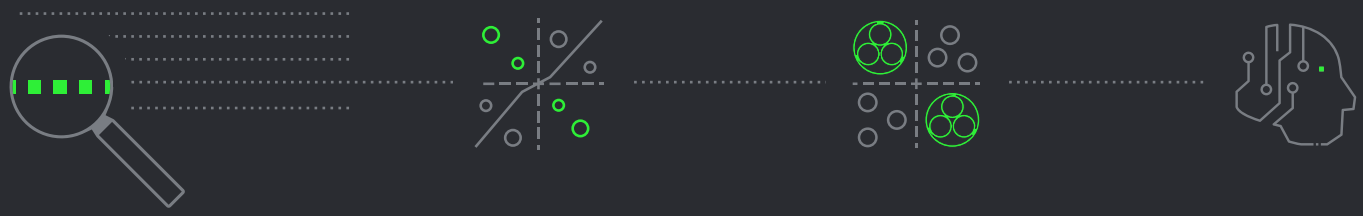
A More Comprehensive Analysis

Our approach has studied billions of files...

and currently measures 1.4 million features...

which are extrapolated for analysis...

and used to train our machine learning models.



AI in the Enterprise – A Look at the Numbers

The value of artificial intelligence applications is not unique to endpoint security. Indeed, AI is making inroads in enterprises as IT decision makers and other corporate leaders realize the benefits it brings to productivity, digital transformation, employee work satisfaction, and information security. Companies that wait too long to integrate AI-driven solutions into their enterprise operations are now likely to run the risk of losing out to faster-moving competitors.

By the Numbers For Security:

70% say their security team is using AI in their threat prevention strategies.

77% say they have prevented more breaches following their use of AI-powered tools.

81% say AI was detecting threats before their security teams could.

78% say the technology has found threats humans couldn't see.

Organizations are already investing in AI, or have immediate plans to invest:

60% say they already have AI-powered solutions in place.

40% say they are planning to invest in them in the next two years.

AI is seen as a competitive advantage:

87% see AI-powered technology as a competitive advantage for their IT departments.

83% are investing in AI to beat competitors.

AI increases productivity:

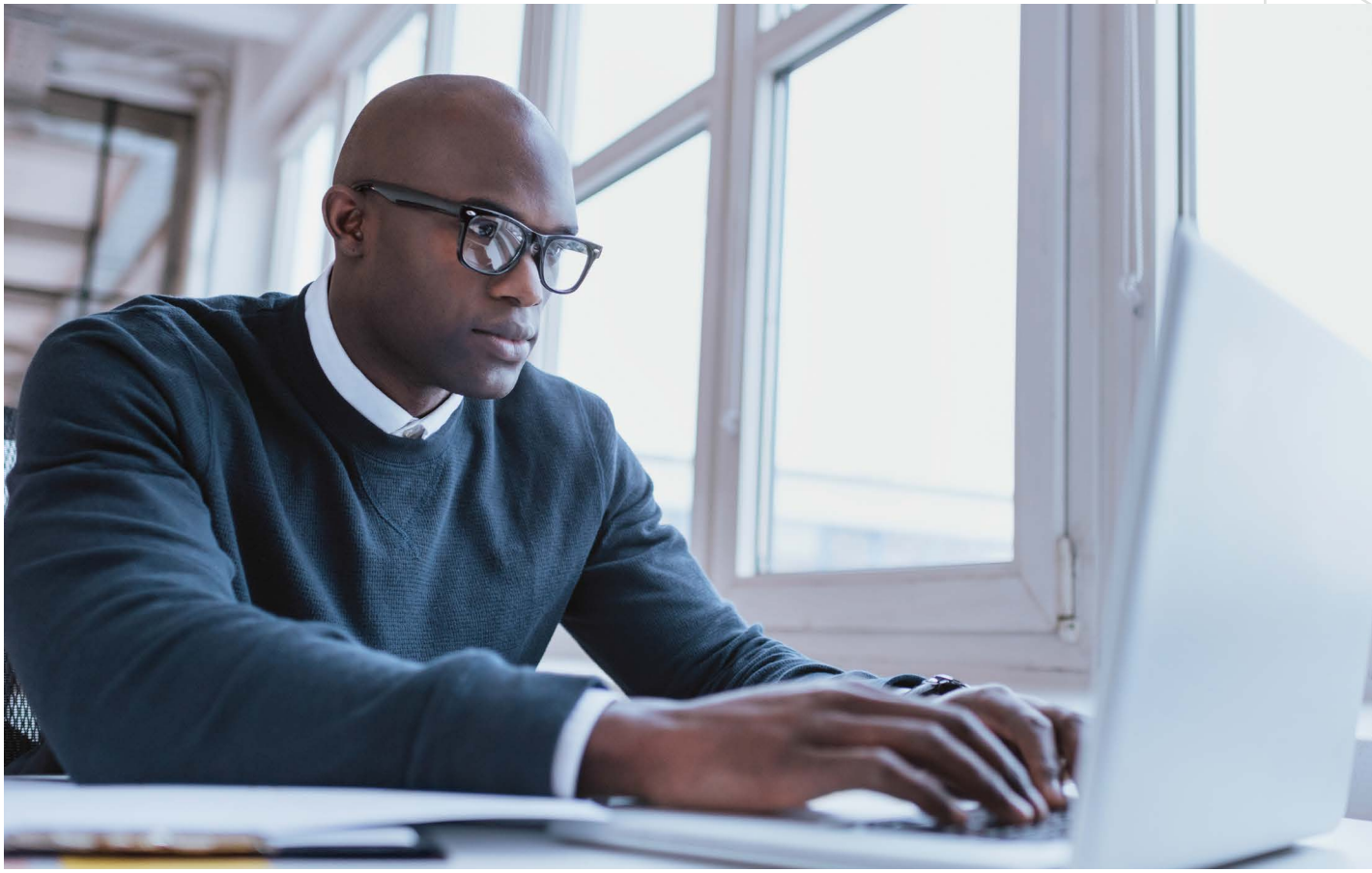
80% believe that teams using AI have become more productive.

81% say AI is critical to the company's digital transformation.

81% say AI will lead to more meaningful work for employees.

MarketCube Survey Conducted on Behalf of Cylance: https://pages.cylance.com/2017-10-03CNTAISurveyReport_LP-Download.html

Evaluating AI-Driven Security Solutions



Choosing an AI-based security solution is not a one-size-fits-all proposition. In becoming one of the most recent security industry buzzwords, the meaning and significance of artificial intelligence has become diminished. When every product boasts AI capabilities, security decision makers may quickly become cynical, even in the face of the most exciting innovation shaping cybersecurity today.

Why Does Your Security Product Include AI Capabilities?

Vendors generally add capabilities to their solutions when they have discovered a new, better way to protect a computer or when they get pressure to expand their capabilities to meet market demand. The inclusion of AI is no different, so it's important to understand the vendor's motivation behind incorporating AI into their technology.

- Why does the product have AI?
- Is the AI performing a new capability or automating an existing capability?
- If a new capability, what is the goal of the AI in the product?
- How does including AI improve a product over similar, non-AI offerings?
- Does your AI replace older security capabilities in your product or is this additive?

Machine Learning vs. AI — What's the Difference?

To effectively evaluate AI-based security technologies, it is first important to understand the meaning of AI and machine learning in the context of cybersecurity:

Artificial intelligence is the broader concept of machines being able to carry out tasks in a way that humans consider intelligent.

Machine learning is a more specific application of AI that is based upon the principle that machines can perform assigned tasks intelligently if they are given access to data sets and allowed to learn for themselves — this process is often referred to as "training".

These definitions may raise more questions than they answer when you begin to apply them to how technology vendors are incorporating these capabilities into their products. To further discern the AI messaging signal from the noise, here are four categories of questions you should pose to any security vendor when evaluating AI-based security solutions.

How Can Your AI Benefit My Organization?

It is not uncommon for vendors to add capabilities into their product for reasons other than customer benefit, especially for solutions that may have been on the market for a number of years. It is important that you understand how each vendor's implementation of AI will improve your overall security.

- Will the results show up in our bottom line and in employee productivity?
- How does the incorporation of AI impact the performance of the product and its use of endpoint computing resources?

How Smart Is Your AI?

AI can be simple or complex. Simple AI is good at making decisions based on known information, like picking chess moves given the current state of a chessboard. It weighs existing data to determine an optimal result and can repeat this behavior through multiple iterations. It has no memory of the past and no great ability to anticipate the future.

Complex AI requires massive training data sets, a neural-net architecture, and considerable time to train appropriately. It excels at pattern matching and predictive tasks. Complex AI does not return quantitative answers (e.g. make chess move X), but instead returns qualitative answers (e.g. 89% chance this object is the same as other objects).

It's important to understand what type of AI the security vendor is using so that you have the right expectations of results.

How Do You Maintain Your AI?

The maintenance required to keep AI well-trained and relevant all depends on how the AI is being used. For instance, if the vendor is using AI to automate signature creation for new threats, the AI is typically maintained by the vendor and enables more frequent signature updates. This may not actually benefit the organization as it may result in more updates to the endpoints. Alternatively, if the AI is trained in the cloud and then deployed to the endpoints to make real-time decisions on threats without constant updates, the organization can benefit from consistent prevention with minimal maintenance.

- Where does your AI reside? Is the AI running in your cloud or running locally on the endpoint?
- How is the AI specifically used? Is the AI used to automate signature creation? Is the AI used to make real-time decisions on threats?
- When and where is the AI trained? Is it at the endpoint, or prior to deployment to the endpoint?
- How much maintenance, including employee training and active attention, does your AI solution require?
- How often is the AI retrained?

Powerful Business Impact

Of course, preventing cyber attacks from compromising endpoints is not an isolated concern. Security administrators must balance the mandate of providing adequate security with the related business needs of end-users and their ability to work in an unfettered manner.

When evaluating whether an AI-driven endpoint security solution is right for you, it's important to consider the business benefits an AI-driven solution could deliver, including but not limited to, maximizing resources, lack of additional required headcount, easy deployment, increased productivity, and return on investment.

Maximizing Resources

One of the common consequences of traditional AV is the burden it places on productivity. End-users know this too well, with seemingly endless computer startup routines that involve downloading updates with new signatures, monopolizing processing power. This stagnation comes at a steep cost, often in excess of $1,000 per employee per year, or $10 million for a company with 10,000 employees.

BlackBerry Cylance conducted several tests to determine the impact on a computer system and the user's ability to perform several common actions, such as copying or creating files, and their impact while detecting and quarantining malware. The results reveal that our AI-based endpoint security product CylancePROTECT®, which eliminates the need for time- and resource-intensive updates, minimizes this productivity concern by using significantly less system resources at idle than traditional AV solutions, and by delivering a significant performance boost during detection and cleaning.

Quantifying Productivity Losses Related To Legacy AV

If you're using a bloated antivirus program, you're likely losing over $1,000 a year per employee!

The average worker works **5 days** a week, **50 weeks** a year.

5 days
× 50 weeks

250 DAYS

Let's assume the average knowledge worker loses **10 minutes** a day.

10 minutes
× 250 days

2,500 MINS. / 42.67 HOURS

The average American worker earns **$26.00** an hour

$26.00
× 42.67 hours

$1,109 .42

No Additional Headcount Required

The La Jolla Institute for Allergy and Immunology (LJI) is dedicated to researching and understanding the human immune system. The non-profit research organization consists of 23 independent laboratories led by world leaders in immunology. This multi-lab environment encourages out-of- the-box thinking, creative problem solving, and collaboration between researchers, which leads to life-saving innovations. LJI scientists produce some of the most-cited research papers in the field.

LJI deployed CylancePROTECT and CylanceOPTICS™, which were compatible with the various technologies used by the Institute's numerous laboratories. With BlackBerry® Cylance® solutions in place, researchers no longer suffered through long reboots or distracting security popups.

CylanceOPTICS proved especially valuable to LJI, which considered running a managed SIEM or hiring a security agency to monitor LJI's infrastructure. The cost of SIEM services or independent security monitoring would have taken a considerable toll on the Institute's limited budget.

Using CylancePROTECT and CylanceOPTICS puts a wealth of information at LJI's fingertips, allowing its staff to manage and monitor threats with minimal added expense. "BlackBerry Cylance is enabling us to be in control of security in a way that previously felt like we needed someone else to do for us," said Michael Scarpelli, IT Director at LJI.

"BLACKBERRY CYLANCE IS ENABLING US TO BE IN CONTROL OF SECURITY IN A WAY THAT PREVIOUSLY FELT LIKE WE NEEDED SOMEONE ELSE TO DO FOR US."

—Michael Scarpelli, IT Director at LJI

Easy Deployment

International workwear company Engelbert Strauss & Co. employs 1,200 people, is represented throughout Europe by ten subsidiaries, and serves a large number of international commercial customers.

Engelbert Strauss & Co. relied on a traditional signature-based AV solution to secure the company's 1,000 endpoints and 200 servers, but administration of the solution was becoming increasingly expensive. Despite a relatively large IT team, it took weeks to create and monitor the necessary set of rules with the existing antivirus solution, and training also took up a considerable amount of time.

The company deployed BlackBerry Cylance solutions that feature an intuitive interface that requires very little training, phasing out the company's previous AV solution. "The implementation of CylancePROTECT had no impact on operations, and we were able to complete the rollout in a timely manner," said Rudiger Faust, IT Team Leader for Engelbert. "We did not have to uninstall the existing solution immediately or before commissioning CylancePROTECT as is usual with other products. CylancePROTECT has already blocked new malware in addition to malware that was not revealed by the existing solution. In addition, it has found several versions of outdated software that was just taking up space on our systems. Last but not least, we can rely on the amazing first-class support of the BlackBerry Cylance team."

Increased Productivity

California's Orange Unified School District operates 40 schools, employs 3,000 staff and faculty, and serves 29,000 students. Its system includes sensitive information, such as children's personally identifiable information. The district must also comply with the Family Educational Rights and Privacy Act or FERPA.

The district was experiencing an escalating volume of targeted cyber attacks, including malicious file downloads, ransomware, and spam. The district had stopped investing in signature-based AV because it proved ineffective more than 50% of the time.

The district decided to deploy CylancePROTECT, with its IT team quickly discovering threats never reported by its previous AV, including potentially unwanted programs that had been lurking on client systems for upwards of five years. CylancePROTECT identified wireless key dumps, password sniffers, and files made to pass encrypted data. Ultimately, the team quarantined nearly 500 items, and the district has not experienced any subsequent issues with ransomware, viruses, or infections. "It is a set-and-forget application because you don't have to worry about whether it is updated. You know that it is loaded and protecting your systems," said Tam Nguyen, Director of Information Technology for the school district, who also appreciates CylancePROTECT's collective user score when assessing threats. "When you see a file was blocked by 100% of all CylancePROTECT users, you can easily determine if it is good or bad."

Return on Investment

To provide objective analysis of our AI solutions and their effectiveness on organizations, BlackBerry Cylance engaged Forrester Research to conduct an economic impact study. Based on its research, Forrester concluded that companies that invested in BlackBerry Cylance's threat protection solution realized the following over a three-year period:

- $7.7 million in benefits (vs. costs of $2.2 million), for a net present value (NPV) of $5.5 million
- 251% ROI

"IT IS A SET-AND-FORGET APPLICATION BECAUSE YOU DON'T HAVE TO WORRY ABOUT WHETHER IT IS UPDATED. YOU KNOW THAT IT IS LOADED AND PROTECTING YOUR SYSTEMS."

—Tam Nguyen, Director of Information Technology, California's Orange Unified School District

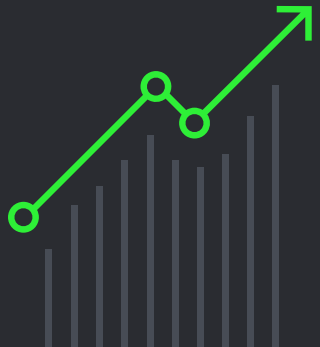
Furthermore, Forrester characterized the following risk-adjusted, quantified benefits for one of BlackBerry Cylance's government customers, a large county in the U.S., as representative of other enterprises that deployed BlackBerry Cylance solutions:

- **Yearly cost savings of $2.3 million** due to reduced incidence of zero-day threats and data breaches. CylancePROTECT reduced the possibility of having a data breach by almost 99% for the county's confidential, high-value information across all of its 20,000 customer records.
- **$260,000 in cost savings related to remediating/re-imaging systems.** The county's significant costs in employee and end-user time spent re-imaging machines that had been compromised due to malicious software was reduced by 98% following the introduction of CylancePROTECT, saving the county over $260,000 across over years.
- **Improved productivity for IT, network, and security FTEs** of three-year present value of $1.8 million. CylancePROTECT reduced the time needed to manage the cybersecurity process, helping the IT and security employees to be 40% more productive, focusing on tasks that brought incremental value for the county.

Companies that invested in CylancePROTECT realized the following over a three-year period:

$7.7 Million
IN BENEFITS

251%
ROI



2017 Forrester Total Economic Impact Report: https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Total_Economic_Impact_Cylance_October_2016_ANONYMOUS.pdf

Deploy at Your Pace

Deploying a security solution doesn't have to be an either-or proposition. BlackBerry Cylance products allow users to migrate gradually, introducing our technology more completely only after it assesses performance and efficiency. For Engelbert Strauss, that was precisely the approach they pursued. While they were impressed by the prospect of what CylancePROTECT could deliver, they were hesitant to overhaul their complex system without verifying its efficacy.

"We were looking for a truly novel approach, and I have to admit that I was impressed by the mathematical concept underlying the solution," said Rudiger Faust, the company's IT Team Leader. "We quickly decided to test the solution and start a proof of concept on about 10% to 15% of all systems. For that, we needed six people in total and less than an hour of training. The solution is quick and easy to use, resource saving, and eliminates the annoying import of updates. Except for occasional system updates, the solution just runs in the background."

Because Engelbert Strauss operates around-the-clock, its requirements for trouble-free migration are paramount. In addition, in the field of logistics, high-performance components are required that work discreetly in the background. "That describes CylancePROTECT in full," Faust said, "but the solution has another advantage. To my knowledge, it is the only one that works in addition to other endpoint security solutions. During the migration phase, we wanted to run BlackBerry Cylance products in parallel with our existing solution in order to safely exclude the false positives that occur. The pleasant side effect is that we were able to carry out the rollout at the same time in a relaxed manner."

Your Path Forward: Augment or Replace?

Considerations When Replacing Your AV

When selecting a new security vendor, it's important to review your options closely. Here are four things to consider before making a selection:

- **Effectiveness:** Any new security solution should deliver considerably increased prevention capabilities over your existing product. There are many third-party testing reports publicly available that offer comparisons of the most common endpoint security products on the market today.
- **Simplicity:** Pay close attention to the effort required to install, run, and maintain any new security solutions that you are considering.

- **Performance:** Verify how much of your computers' processing capabilities any prospective solution will consume. Remember the performance drag caused by your AV solution? That's something you'll want to avoid.
- **Vendor Viability:** There are more than 1,600 security companies actively selling their wares. With so many vendors claiming to provide the same end results, perform your due diligence before selecting a vendor. At a minimum, you should consider:
    - **Reputation:** Does the vendor have good reviews from current users? Does the vendor have partners that frequently recommend their products? What do analysts say about the vendor?
    - **Vision:** What does the vendor have planned for the solution for the next 12 months? What about the next five years?

Additionally, decide whether you're going to move forward with a replacement or augmentation strategy. In either instance, you'll want to work with a vendor that can provide knowledgeable assistance to ensure seamless integrations and transition.

At BlackBerry Cylance, our ThreatZERO™ Consulting Services team provides technological expertise and personalized, white glove service that optimizes our solutions. Whatever your solution provider, make sure there is back-end support that ensures your solution runs smoothly and effectively.

See For Yourself

Finally, request a live demonstration of the solutions that you're considering. The true test of any security solution should be how well it performs for your organization. Any company selling a security product should be happy to demonstrate its performance within your infrastructure. Be wary of companies that only offer internal test results as this puts the onus on the end-user to adjust. This means the training of the model for the endpoint is incomplete. At a minimum, seek to determine the following:

- Does the AI provide levels of aggressiveness?
- What cloud dependencies does the AI rely upon to be effective? Can the AI be as effective offline as it can be online?
- Can the AI prevent never-seen-before malware on the endpoint without connectivity to the cloud?
- Can the AI prevent malware that its training set has never seen before?
- Has the AI been tested by a third party that confirms its ability to detect and/or prevent malware that did not exist when the AI model was trained?

Choose Prevention, Not Detection, for Superior Protection

Those frustrated with the limitations of traditional AV solutions understand that detecting a threat post-impact and then mitigating the damage just doesn't deliver the same value as preventing a threat from executing on endpoints in real time.

It's time to replace your AV investment and realize the security, financial, and performance benefits associated with artificial intelligence. ***The smarter solution for endpoint protection.***

Take the Tour: Discover the power of CylancePROTECT on a self-guided tour.
See for Yourself: Request a demonstration.
Talk To an Expert: Request a services consultation.

BlackBerry | CYLANCE

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

20190418-0164