AI-Driven EDR

The Current and Future Path for More Intelligent Detection and Response

::: BlackBerry® | **CYLANCE®**

BlackBerry® | CYLANCE®
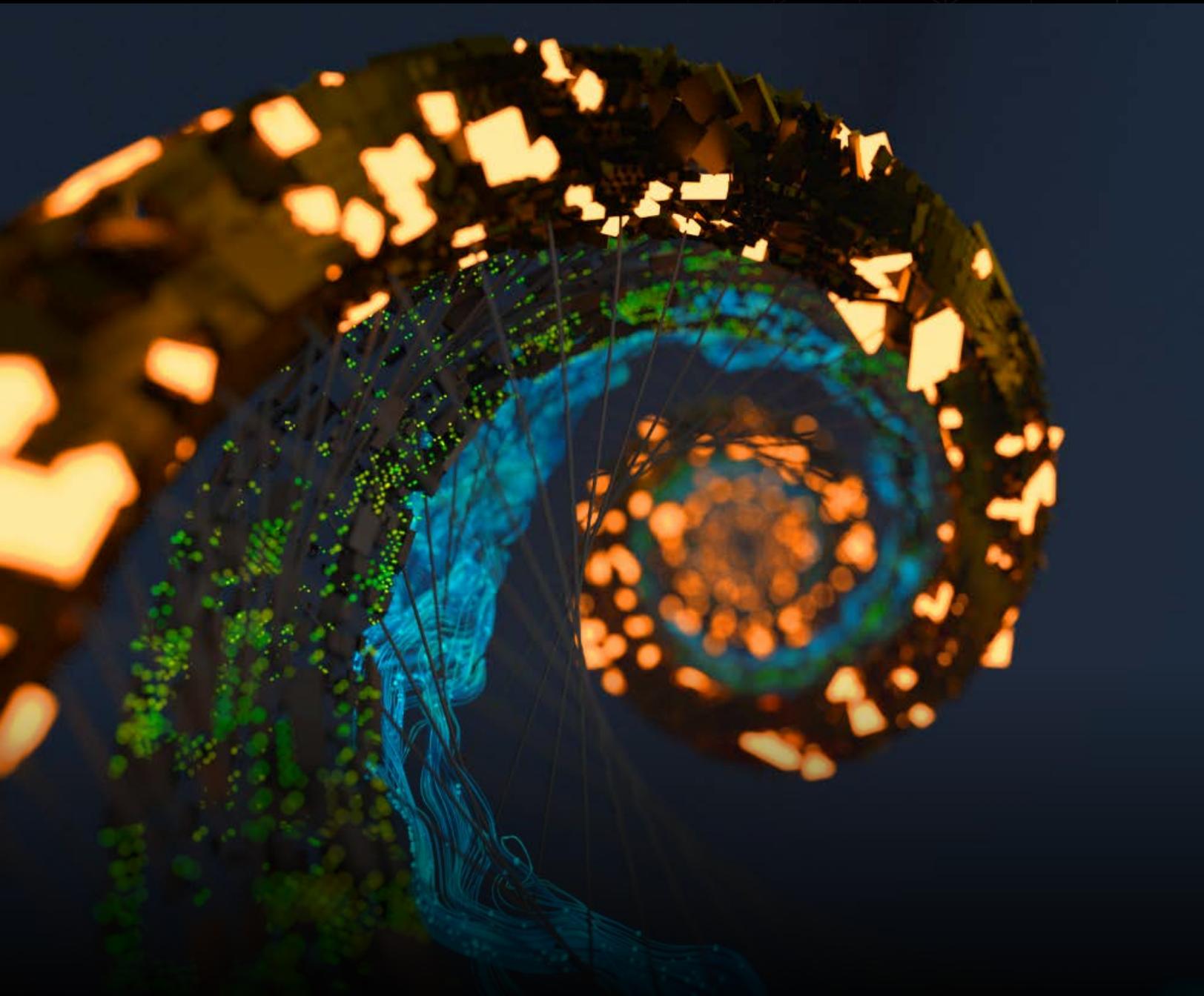
Contents

The State of Endpoint Insecurity

The security professional's job has become an endless game of cat-and-mouse, continually pursuing invisible attackers that can out-think, out-run, and outsmart most security systems. No matter how efficient and nimble the professional, the attackers are fast, too. And getting faster every day. As a result, endpoints remain vulnerable.

It's not a matter of simply adding additional security personnel. Industry-wide, the IT professional is a scarce commodity with demand far outpacing supply. By 2022, there will be a shortage of 1.8 million IT workers in the United States[1], leaving companies even more short-handed to perform day-to-day tasks, much less those that are critical for security. In fact, in a recent survey conducted by ESG, the top two weaknesses of endpoint security staff were the "ability to investigate a cybersecurity incident involving an endpoint to determine root cause and the attack chain," and "monitoring endpoint status to attain a real-time or near real-time inventory of endpoints on the network."

Even for organizations with ample IT staff, endpoint security stack complexity is making their job inefficient and unproductive. The average organization maintains seven different software agents installed on endpoints[1]. As a result, much of their IT team is forced to wade through a burgeoning thicket of binary bloat and false alerts, diverting their attention from more critical enterprise pursuits. In fact, roughly one-third of analysts' time[1] is being spent on processing alerts that have unknowingly already been processed, a huge drain on overall efficiency.

ESG summarized the issue as "endpoint security staff often struggle to monitor endpoint security, investigate events, and take remediation actions in collaboration with IT operations. Given the global cybersecurity skills shortage, endpoint security solutions must improve threat prevention efficacy, simplify the investigations process, and offer automated remediation functions for cybersecurity and IT staff."

---

1   CylanceOPTICS Infographic: Case for a New Approach to EDR

Key Weaknesses of Endpoint Security Staff

Endpoint security staff often struggle to monitor endpoint security, investigate events, and take remediation actions in collaboration with IT operations. Given the global cybersecurity skills shortage, endpoint security solutions must improve threat prevention efficacy, simplify the investigations process, and offer automated remediation functions for cybersecurity and IT staff.

Original survey question:

Which of the following do you consider your organization's biggest weaknesses as it pertains to the individual(s) responsible for endpoint security?

Ability to investigate a cybersecurity incident involving an endpoint to determine root cause and the attack chain — **16%**

Monitoring endpoint status to attain a real-time or near real-time inventory of endpoints on the network — **16%**

Ability to remediate without re-imaging an endpoint system — **14%**

Resource availability to deploy and configure new endpoint security tools — **14%**

Proliferating Endpoints

The focus, of course, wasn't always on the endpoints. But, as personal computers became commonplace in the late 1980s and early 1990s, would-be-attackers (and soon after, an emerging security industry) realized this sprawling network of touchpoints created an equally sprawling network of vulnerabilities, which in turned spawned a marketplace filled with antivirus and anti-malware solutions.

The variety of attack types necessitates a comprehensive defense strategy, one with a prevention-first capability that minimizes security risks. That's easier said than done as cyber attacks grow increasingly sophisticated and elusive:

Malware — Whether in the form of ransomware, trojans, or adware, malware continues to wreak havoc on systems worldwide.

Fileless Threats — Fileless attacks are on the rise as attackers realize the ease with which legitimate admin tools and memory can be used to compromise a system without writing any files to the disk. Many security products have no ability to prevent these types of attacks.

Malicious Scripts — Scripts are a favorite tool of choice for many attackers for several reasons. First, for novice attackers, malicious scripts are readily available in the cyber crime underworld, which makes it easy to find one that meets the attacker's needs. Additionally, scripts are often difficult for security products to detect, as there are many legitimate uses for scripts.

Malicious Email Attachments — Phishing attacks are one of the most effective ways attackers gain access to an endpoint. Employees unwittingly open malicious attachments, thinking they are legitimate, and enable attackers to undertake any number of malicious actions.

And with bring-your-own-device policies proliferating across enterprises, which in turn utilize a range of software-as-a-service solutions, endpoints have become the weak link when it comes to cyber attacks, making their protection a paramount corporate concern.

The endpoint detection and response (EDR) landscape was driven largely by an industry recognition of the fact that there is a limit to how effective a signature-based approach (and the manual, time intensive development and distribution cycle) is as compared to the ease of acquiring and launching a zero day threat from malware variants acquired on the dark net.

The Rise of Endpoint Detection and Response (EDR)

To combat these and other threats, enterprises are increasingly turning to endpoint detection and response (EDR) solutions that provide advanced endpoint protection.

What is EDR?

Endpoint detection and response, or EDR, refer to the capabilities that, when deployed on endpoints, allow for fine-grained detection of evidence of security incidents, investigation of said incidents and, should it be necessary, some form of response.

Main Reasons for Deploying An EDR Solution

Organizations are deploying endpoint detection and response (EDR) solutions to accelerate threat detection, reinforce incident response, and complement endpoint threat prevention. To maximize their value, EDR solutions must be easy to deploy and use, and must deliver measurable benefits as quickly as possible.

Original survey question:

What is the primary reason your organization deployed or is planning on/ interested in deploying an EDR solution?

We believe that an endpoint detection and response solution can help us improve the time and effectiveness related to incident response measures — **16%**

We require visibility into the entire threat lifecycle to understand specific attack chain behaviors to respond to incidents and to harden our defenses — **15%**

We believe that an endpoint detection and response solution can help us improve the time it takes for incident detection by engaging in threat hunting — **15%**

We believe that an endpoint detection and response solution complements our existing endpoint protection platform (EPP) suite — **14%**

> **"ORGANIZATIONS ARE DEPLOYING ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTIONS TO ACCELERATE THREAT DETECTION, REINFORCE INCIDENT RESPONSE, AND COMPLEMENT ENDPOINT THREAT PREVENTION."**
> —ESG

In addition to protecting endpoints against threats, the capable solution at a minimum must be able to perform the following:

Investigate Attack and Alert Data

Stopping a threat from impacting endpoints is critical to ensuring sensitive data remains secure. But, the effort needs to provide future value to the enterprise to help stop future attacks from executing. When a threat is thwarted, security professionals must be able to capture critical data and perform a root cause analysis to understand the origin of the attack and how an attacker attempted to compromise the endpoint.

Perform Targeted Threat Hunting

Some malicious activities are easy to identify, while others are more ambiguous. When a computer begins to behave irregularly or it is determined that an endpoint may be at risk of compromise, it is critical that an organization's security toolkit gives it the visibility required to make definitive judgments.

Perform Dynamic Threat Detection

There are several ways to identify potential threats and compromises. First, security analysts can perform searches across endpoints to identify suspicious artifacts, and through manual investigation, determine that a threat exists. While there is tremendous value in this process, it simply does not scale across an enterprise. To root out threats hidden on endpoints, an automated approach to threat detection must be used.
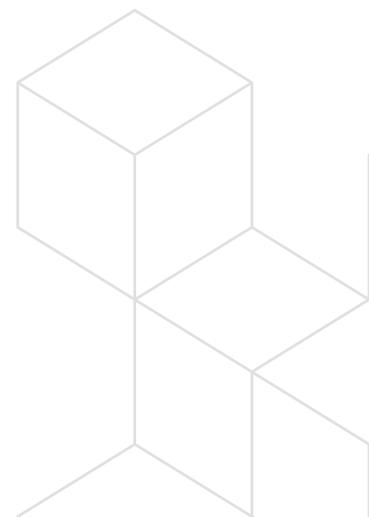
Offer Response Capabilities

When an attack is detected, quarantining the suspicious attack while locking down the endpoint is paramount to minimize damage. Depending on the attack, rolling back the system to a previous state may also be necessary.

Not all EDR solutions are alike (see below), but the more mature offerings bear a number of similar characteristics or baseline attributes:

- Can be installed on any endpoint in minutes.

- Requires no hardware or expensive data streaming.

- Does not require constant updates.

- Enables zero-latency detection and response by storing and analyzing data locally on the endpoint.

- Delivers self-contained, automated, machine learning threat detection modules that uncover otherwise hard to find threats.

Smarter EDR
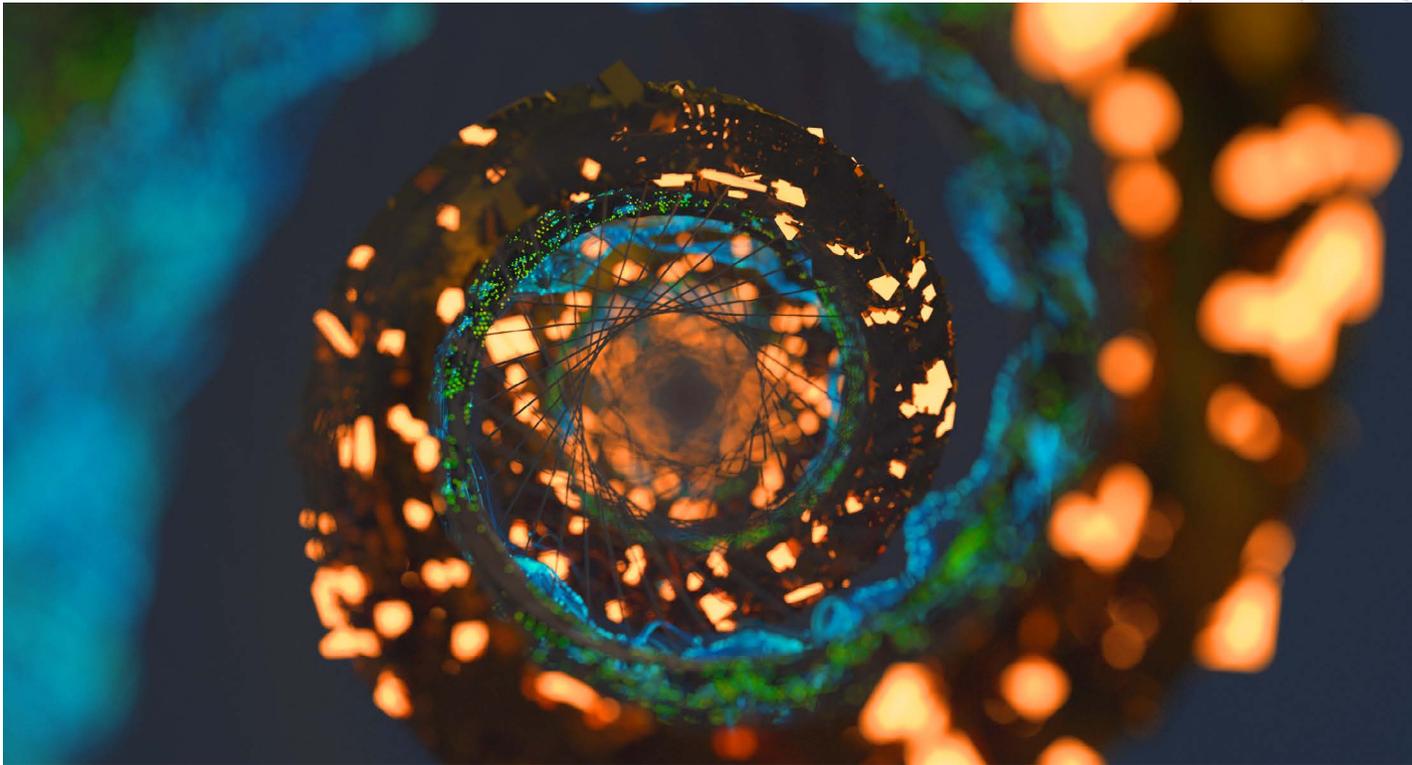
Not all products offer the same capabilities, especially in the detection phase. Most incorporate a rules-based engine customized to configuration settings. Their strength — offering limitless protective options — is also their weakness, as they require continual manual inputs to address evolving attacks and attack patterns. But, with shrinking IT staff, this requirement has become aspirational at best. And, even when staff is available, the most diligent IT professional cannot match the speed of a cleverly disguised cyber attack.

To effectively deal with the growing threats in a timely and efficient manner, automation is key. And, when it comes to automation, there's a smarter way to prevent attacks from compromising endpoints: artificial intelligence.

Artificial intelligence (AI) offers organizations dramatic increases in cyber-attack-fighting capabilities without the need to increase IT resources. The approach is not new — your email's spam folder incorporates machine learning in filtering messages.

When it comes to leveraging AI to protect endpoints, the process involves using data analysis to learn what an event represents, and applying that analysis to create a model that can be used to predict and interpret future behaviors. This can be achieved either locally, on the endpoint itself, or remotely by using cloud-based tools.

Local efforts offer faster response capabilities, but they come with a cost, operating on fewer resources than cloud-based applications. The latter incorporate more expansive datasets, though response times struggle to keep pace with nimble attacks.

Both options replace traditional antivirus solutions and eliminate the need for signatures, a time and resource savings that addresses today's IT staff shortage. Yet, the process is not foolproof. Machine learning can yield false positive alerts, depending on configuration, further straining IT efforts. Organizations must strive for a balance that minimizes false alerts while ensuring the detection of malicious activity.

AI-Driven EDR – Deeper Dive

EDR can leverage machine learning for both functional and non-functional purposes. **Functional purposes** include the ability to analyze behavior across large, complex systems, identifying and preventing attacks from executing on endpoints. It does this by identifying suspicious patterns that occur within network and directory activities, for instance. **Non-functional** applications include human interactions, such as those that occur with analysts' input. In such cases, machine learning can minimize investigative errors while accelerating the adoption of inputs.

BlackBerry Cylance AI-Based Solutions

Combining AI-driven predictive prevention with dynamic threat detection and response, BlackBerry Cylance's EDR solution, CylanceOPTICS, lets IT professionals see and stay ahead of attackers. By harnessing the power of AI to identify and prevent security incidents, CylanceOPTICS allows security personnel to:

- Dissect attacks or artifacts of interest, determine their root cause, and improve security framework.

- Quickly assess endpoint risk, then take action to minimize dwell time and reduce attack surface using instant results from the CylanceOPTICS on-demand, enterprise-wide smart threat hunting capability.

- Customize threat detect and response capabilities by creating their own set of rules, or use the set of rules provided by BlackBerry Cylance.

- Adjust the parameters of existing rules or create new ones that minimize false positives and provide security analysts with high-fidelity alerts to investigate.

- Eliminate the noise by preventing attacks, reducing security alert volume, and improving team efficiency.

- Protect the business by using AI-driven prevention tools to avoid the cost, risk, and long-term impacts of a serious security incident.
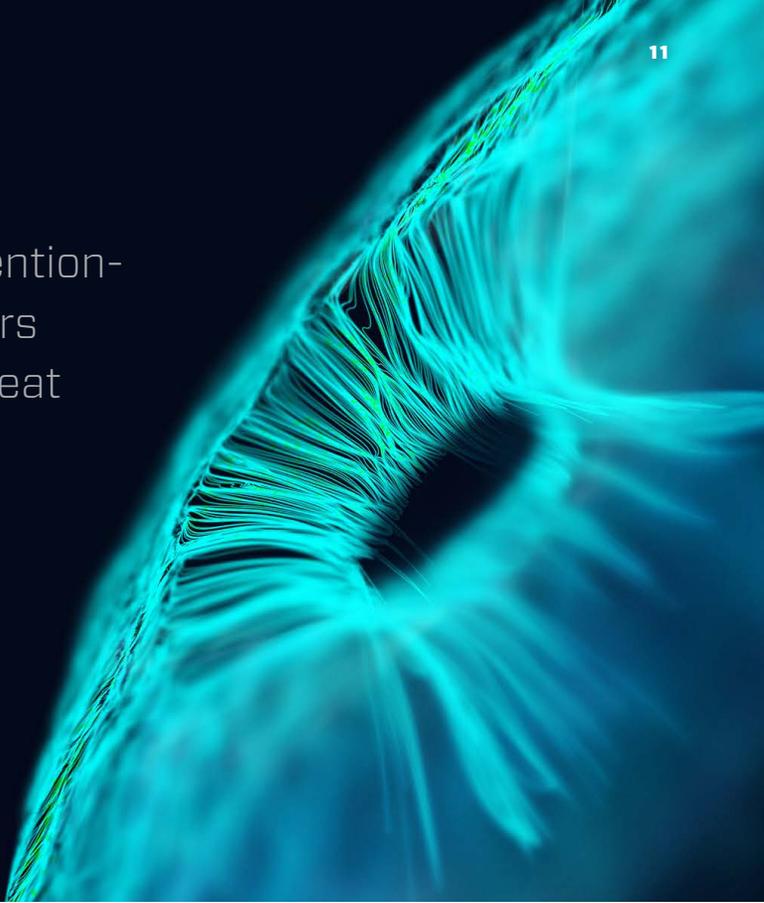
CylanceOPTICS provides a prevention-first approach to EDR that delivers automated machine learning threat detection modules designed to uncover threats that would be nearly impossible to find with static behavior rules.

CylanceOPTICS AI-Driven EDR vs. Traditional Rules-Based EDR

Organizations benefit from endpoint detection and response (EDR) technologies by enabling faster response and remediation for security incidents.

However, attackers have worked hard to develop tactics, techniques, and procedures (TTPs) to defeat legacy rules-based EDR technologies, rendering them less effective over time.

The evolution of TTPs and their impact on security solutions parallels the demise of legacy AV products that have been largely marginalized by attackers. Moving forward, EDR products that rely on rules will be unable to keep pace with new threats.

CylanceOPTICS provides a prevention-first approach to EDR that delivers automated machine learning threat detection modules designed to uncover threats that would be nearly impossible to find with static behavior rules. The value proposition of an AI-driven EDR solution built on a strategy of prevention far outweighs that of traditional EDR solutions, as can be seen in the comparison chart on the next page.
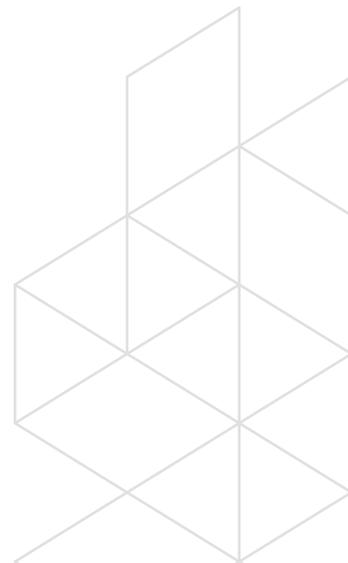
Classifying AI-Driven EDR Capabilities

	Traditional EDR	CylanceOPTICS	Benefits
Security Approach	Provides reactive detection and response	Provides continuous threat and incident prevention	*A prevention-based approach reduces the overall number of incidents that require action/analysis*
Required Skills	Requires advanced security analyst skillset	Is built for security analysts of all skills and experience levels	*A solution accessible to all widens the pool of possible talent who can manage the solution*
Data Collected	Streams all endpoint activity to the cloud continuously or sends it to dedicated hardware	Collects and stores only security-relevant data locally	*Collecting only security-relevant activity data locally significantly reduces liability and improves compliance*
Data Storage	Continuously streams data to the cloud or aggregates on local hardware	Stores data locally on each endpoint	*Storing data locally significantly reduces liability, improves compliance, and optimizes performance and scalability*
Threat Detection Techniques	Requires individual behavior rules be written and continually augmented to maintain coverage levels running from the cloud	Combines behavior rules with trained ML threat detection modules to provide a greater — and always increasing — breadth of coverage, running locally on the endpoint	*Eliminates the need for up to thousands of rules that must be created and maintained by a security expert*
Threat Hunting	Requires significant expertise to configure and perform a multitude of search capabilities	Provides easy-to-configure search criteria and optimized collection of responsive data from endpoints	*Increases the ability to uncover hard-to-find threats without adding staff*
Root Cause Analysis	Combs through collected data to determine where an active threat entered the environment and how to stop ongoing damage	Uses data collected when the threat is prevented by CylancePROTECT to understand the attack vector chosen by the bad actor	*Automated approach shortens time to analysis completion*
IR Capabilities	Requires extensive security expertise to use the advanced tools that identify and mitigate security issues	Takes automated IR actions or enables manual action, deploying pre-configured and custom response actions to return the system to a trusted state quickly	*Automation and machine learning allow organizations big and small to maintain the security posture once thought only available to the largest of organizations*

AI-Driven EDR Drives Better Business Outcomes

Multi-National Manufacturing Organization

BlackBerry Cylance commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine what return on investment enterprises may realize by deploying CylancePROTECT and CylanceOPTICS. The aim of the report was to provide readers with a framework to evaluate the potential financial impact of CylancePROTECT and CylanceOPTICS on their organizations. Here is the summary of what Forrester Consulting found as a result of their economic study of our customer's organization.

About the Customer:

- Multi-national enterprise headquartered in Europe
- Operates 500 locations in 150 countries with 45,000 employees
- $14B annual revenue

Top Customer Challenges:

- Insufficient protection against ransomware, malware, and other threats
- Operational problems with the legacy endpoint security solutions
- Lack of visibility into software downloads

Chosen Solution:

- CylancePROTECT and CylanceOPTICS on 45,000 endpoints

Benefits:

- $8.4M in savings from decommissioning legacy on-premises endpoint security solution
- $3.3M cost savings due to faster remediation
- $1.9M estimated reduced cost of security breach
- $14M total quantified benefits
- 99% ROI over a three-year period
- 97% reduction in machine re-imaging
- 95% reduction in employee time lost due to compromise

Key Results:

- Improved threat prevention
- Simplicity, a single vision for cyber defense
- Faster threat response and mediation
- Improved visibility and control over employee downloads
- Can withstand threats without a cloud connection
- Decommissioned additional endpoint security tools
- Limited burden on system resources

Data Source "The Total Economic Impact™ Of CylancePROTECT®
and CylanceOPTICS™

Cost Savings and Business Benefits Enabled by CylancePROTECT and CylanceOPTICS — May 2019"

Read the full report.

Tufts Medical Center: Protecting 10,000 Endpoints

As New England's oldest permanent medical facility, Tufts Medical Center (TMC) provides critical healthcare services to the Boston Community as well as serves as the principal teaching hospital for Tufts University School of Medicine.

Providing a safe system environment for its patients without interruption is a paramount concern, which means that all of the devices that play a direct role in care delivery and safety are protected at all times.

"Endpoints and endpoint security are where all the action is," said Taylor Lehmann, CISO of Wellforce, an association of healthcare institutions that provide care throughout Massachusetts, to which TMC is a member. "It's the things that happen on those devices that need the most amount of focus if you want to disrupt an attack, even a sophisticated attack."

When assessing EDR solutions, Taylor concluded that signature-based AV was unable to combat emerging attacks, and that its need to remain online and networked to receive updates did not provide adequate safeguards for its endpoints. "These facts create issues that prevent these solutions from performing well with attacks and never before seen threats," he said.

Taylor tapped BlackBerry Cylance to deploy CylanceOPTICS on select machines for evaluation before concluding that it identified malicious files previously undetected by existing signature-based systems. Taylor also deployed CylancePROTECT, which delivers artificial-intelligence-powered malware prevention, application and script control, memory protection, and device policy enforcement to prevent successful cyber attacks. Further testing revealed a higher overall detection rate of malicious files and malware as well as a general decline in overall malware infections, once the BlackBerry Cylance solutions completed implementation and configuration.

"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

La Jolla Institute: Better Threat Visibility

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 CylanceOPTICS and CylancePROTECT, which are compatible with the various technologies used by the Institute's numerous laboratories. With BlackBerry Cylance products 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 CylanceOPTICS and CylancePROTECT 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.

What's AI Got To Do With It, Anyway?

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 a machine's ability 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".

At BlackBerry Cylance, our preference for attacking security problems with artificial intelligence is not unique. Artificial intelligence 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 adopt AI, or at least explore the possibilities with AI, run the risk of losing to faster-moving competitors.

For security teams, AI is improving 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, and this will only increase:

60% of the IT decision makers surveyed say they already have AI-powered solutions in place.

40% said 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.

Evaluating AI-Driven Security Solutions
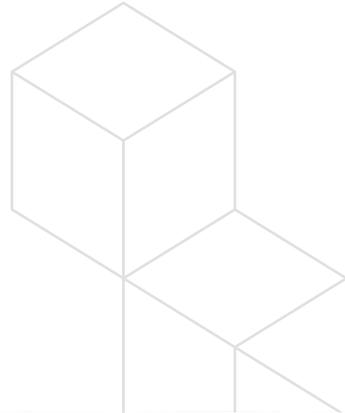
Choosing an AI-based security solution is not a one-size-fits all proposition. Artificial intelligence has become a security industry buzzword so broadly applied as to become almost meaningless. When every product boasts AI capabilities, security decision makers may quickly become cynical, even in the face of the most exciting innovation shaping cybersecurity today.

These definitions may raise more questions than they answer when they are applied 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 that should be poses to any security vendor when evaluating AI-based security solutions.*

1 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?

2 How Can Your AI Benefit My Organization?

It is not uncommon for vendors to add capabilities into their products 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?

3 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, but 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.

- Is your AI simple and can only identify current threats, or is it complex and can identify brand-new, never-before-seen threats?

4 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?

BlackBerry Cylance simplifies the deployment process, delivering a prevention-first endpoint security solution that prevents successful attacks while simultaneously reducing the noise generated by the entire security stack.

When selecting a new EDR provider, it's important to review the transition process closely, along with post-deployment benefits. Here are four things to consider before making your short list of EDR solutions:

- **Effectiveness —** Any new security solution should deliver considerably increased prevention capabilities over existing products. 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 are being considering. A unified platform reduces the overall number of agents and alerts to manage and can make staff much more productive and proactive.

- **Performance —** Verify how much of a computer's processing capabilities any prospective solution will consume.

Key Weaknesses of Endpoint Security Staff

CISOs want an endpoint security strategy that enhances efficacy, improves operational efficiency, and supports the cloud computing initiatives of the business. New types of endpoint security tools must be designed with advanced machine learning that greatly improves threat prevention AND must provide the right dashboards, runbooks, and UI to help streamline operations.

Original survey question:

Which of the following considerations would you characterize as having the most significant influence on your organization's endpoint security strategy moving forward?

Increasing the efficacy of addressing new types of threats	**26%**
Improving the operational efficiency for end-users and the IT and security teams	**26%**
The need to align our endpoint security strategy with our use of cloud computing services	**24%**

- **Vendor Viability —** With so many vendors claiming to provide the same end results, perform due diligence before selecting a vendor. At a minimum, 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 deploy a rip-and-replace strategy or a gradual rollout. If the latter especially, you'll want to work with a vendor that can provide knowledgeable assistance to ensure a seamless transition.

In addition to its products, BlackBerry Cylance offers ThreatZERO™ consulting services that provide technological expertise and personalized, white-glove service. Whatever your solution provider, make sure there is back-end support that ensures your solution runs smoothly and effectively.

Testing One, Two, Three

Once you're in the final consideration phase, ask prospective vendors to perform a compromise assessment of your system. With BlackBerry Cylance, such a review consists of working closely with our world-renowned security experts who provide a customized assessment of systems, personnel, and best practices.

The true test of any security
solution should be how
well it performs for your
organization. Request
a live demonstration of
the solutions that you're
considering.

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?

- 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 and Detection for Superior Protection

True endpoint security does not come from prevention or detection alone. To combat today's attacks, organizations must have a strong AI foundation which feeds their prevention and detection capabilities in order to keep pace with attackers. With BlackBerry Cylance solutions, enterprises get the best of both worlds, maximizing the return on security stack investments, making analysts more efficient, and making the business more secure.

Endpoint security is growing in importance and must be maintained constantly. Organizations that can improve security outcomes across their endpoint detection and response practices in an efficient manner will be able to support the agility that their business and the modern threat environment demand.

Ready to enhance your security posture with CylanceOPTICS?

- Check out www.cylance.com/optics for more information.

- See AI-Driven EDR In Action for Yourself: Request a Demonstration.

- Looking beyond traditional signature-based AV and EDR to solutions that deliver prevention-first predictive security? Talk To One of Our Experienced Security Experts.
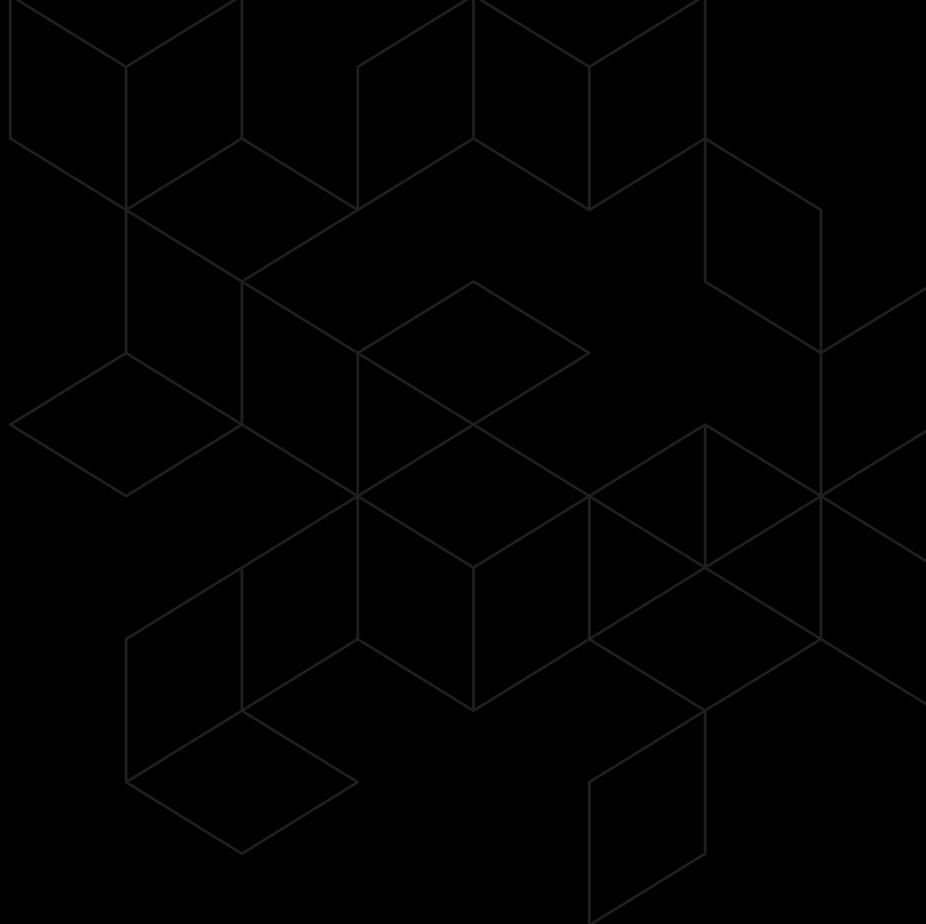
+1-844-CYLANCE
sales@cylance.com
www.cylance.com

BlackBerry® | CYLANCE®

20190424-0265