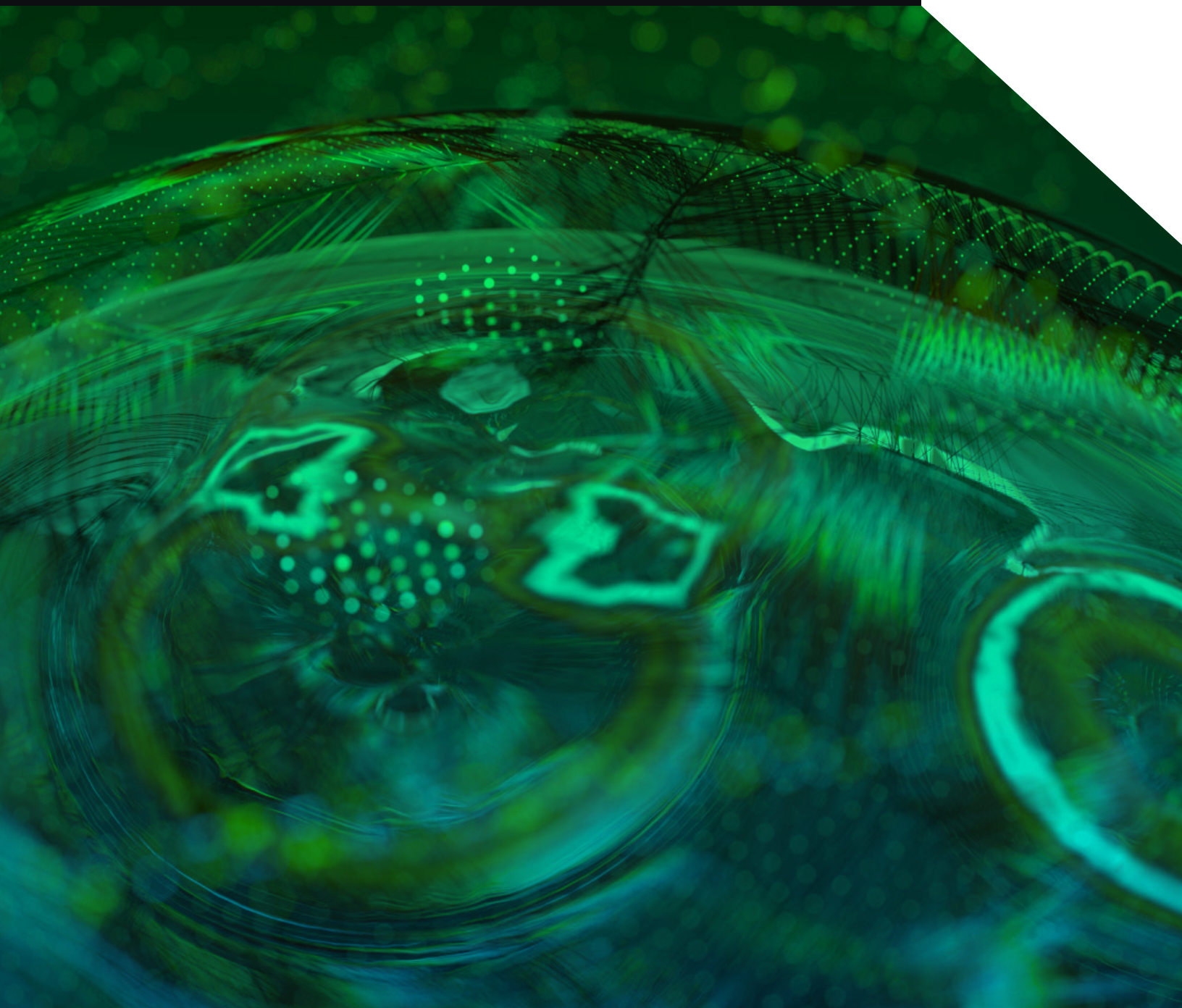


# The Evolution of EDR

Acceleration of Intelligence and Actions

SOLUTION BRIEF



A man in a blue shirt and tie is sitting at a desk in a server room, looking at a computer monitor. In the background, there are several other computer monitors and server racks with glowing lights.

Better intelligence allows  
your security apparatus  
to take decisive actions  
and disrupt attacks.

## Executive Summary

Endpoint detection and response (EDR) is an essential part of the security stack, providing controls that perform critical security tasks across all phases of an attack. However, it faces significant challenges in adapting to a rapidly changing threat landscape. In order to deliver on its intended goals, EDR must evolve in the following ways:

- Transition from slower, cloud-based detection to machine-speed detection and enforcement on the host
- Shift from slow responses occurring later in the kill-chain to early attack disruption
- Improve low-confidence detection of anomalies to high-confidence threat detection with a low rate of false positives
- Allow analysts to move from *investigation by default* to *investigation by choice*
- Deliver understandable and actionable intelligence to analysts instead of raw data of undetermined value

To achieve these goals, EDR must make functional advancements in terms of the speed and quality of the **intelligence** it delivers. Better intelligence allows your security apparatus to take decisive **actions** and disrupt attacks.

- **Intelligence:** BlackBerry Cylance has developed an AI-driven approach to EDR that delivers high-confidence security intelligence which can drive automated workflows. To use an analogy, our EDR doesn't provide analysts with a math problem to solve, but with answers that include the supporting work.

- Actions:** Modern threats operate at machine speed on the host, which means effective EDR needs to do the same. While traditional EDR relies on slow cloud-dependent processes, BlackBerry Cylance deploys lightweight, ultra-fast AI on the device. Our local EDR agents can follow fully automated security playbooks, resulting in faster, coordinated responses that stop malicious processes before they progress.

Device-resident AI will play a critical role in the evolution of EDR. In fact, predictive AI is improving the efficacy of EDR, security operations, and the overall safety of the enterprise today.

## Prevention and Detection: Unique Use Cases with Common Goals and Requirements

Enterprise security has experienced major philosophical and architectural shifts over the past several years. Historically, the lion’s share of security resources was dedicated to prevention tools that identified known malware. However, as threats became more sophisticated in evading signature-based controls, achieving persistence, and carrying out sustained attacks, it became clear that new prevention tools were needed. Organizations had to adapt to changing threats, detect them throughout the life cycle of an attack, and drive appropriate responses. The industry quickly pivoted at both the endpoint and network levels, and detection became the name of the game.

This shift in focus led to a false dichotomy where detection and response were viewed as separate from prevention. This is primarily because early EDR supported a different use case than traditional prevention. Prevention was automated and quickly accomplished its work without human intervention. EDR was tied to incident response, threat hunting, and other human-led investigations. However, as EDR matures, the perceived boundary between it and threat prevention is rapidly dissolving.



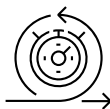
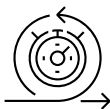

### IR and Hunt by Choice, Not by Default

Preventative and investigative use cases are both critical to enterprise security. However, traditional EDR relies heavily on human-assisted investigations. This puts additional pressure on security staff who are often already taxed with other work responsibilities. This makes traditional EDR a gamble; it can accelerate investigations, but also may create significant data of unknown value requiring additional attention from analysts.

Organization’s threat response should not be crippled by unnecessary technological limitations. Moreover, there is no logical reason why one phase of an attack should be addressed with fully automated prevention while all other phases require human assistance. The best possible technology should be applied to each phase of attack, allowing SOC teams to choose where to focus their investigations.

However, it is not enough to simply document the phases of an attack. With each progressive step, the attack may become more difficult to remediate and cause additional material damage. Persistence techniques may require

## Evolution of EDR

Past Forensics and Live Response	Present Enterprise Detect and Respond		Future Prevention First	
 <b>Batch Scripts</b>	 <b>Batch Scripts + Deployment + Scaled Analysis</b>	 <b>Flight Recorders</b>	 <b>Flight Record Platforms</b>	 <b>AI Platform</b>
<ul style="list-style-type: none"><li>▪ Not scalable: Go to each machine</li><li>▪ Limited to artifacts present on the system</li><li>▪ Time consuming: Two to eight hours collection plus two hour analysis per system was fast</li></ul>	<ul style="list-style-type: none"><li>▪ Scalable</li><li>▪ Generated tons of useful data for analysts to sift through</li><li>▪ Hunting</li></ul>	<ul style="list-style-type: none"><li>▪ SE mitigations</li><li>▪ Intelligence-driven detectors</li><li>▪ Two to eight hours per incident</li></ul>	<ul style="list-style-type: none"><li>▪ Prevention first</li><li>▪ Enterprise ready</li><li>▪ Customers struggle because no story is provided</li></ul>	



As security matures, fully automated AI should be applied to the EDR phases of detection, investigation, containment, and remediation. The illustration below shows how AI can apply to each of these phases:

Detection	Investigation	Containment	Remediation
<ul style="list-style-type: none"> <li>Block malicious activity</li> <li>Use various data analytics techniques to detect suspicious system behavior</li> </ul>	<ul style="list-style-type: none"> <li>Provide contextual information</li> <li>Record and store endpoint-system-level behaviors</li> </ul>	<ul style="list-style-type: none"> <li>Use various data analytics techniques to detect suspicious system behavior</li> </ul>	<ul style="list-style-type: none"> <li>Provide remediation suggestions to restore affected systems</li> </ul>
<ul style="list-style-type: none"> <li>Enterprise Threat Hunting with CylanceOPTICS <i>InstaQuery</i></li> <li>ML-powered incident detection with CylanceOPTICS <i>CAE (Context Analysis Engine)</i></li> </ul>	<ul style="list-style-type: none"> <li>Incident/Threat Root Cause Analysis with CylanceOPTICS <i>FocusView</i></li> </ul>	<ul style="list-style-type: none"> <li>Aggressive Endpoint Containment with CylanceOPTICS <i>Device Lockdown</i></li> </ul>	<ul style="list-style-type: none"> <li>ML-driven automated response with CAE remote scripting advanced forensic artifact retrieval via CylanceOPTICS <i>Automated Package Playbooks</i></li> </ul>

## Shared Goals and Requirements

Recent trends in cybersecurity show that multi-step attacks have become the norm and successful breaches are on the rise. To adapt, organizations need to address the full life cycle of an attack. As shown below, both prevention and EDR benefit from using AI to quickly achieve security goals.

Requirement	Value To Prevention	Value To EDR
Detects threats that are new or don't match a signature	Identifies new or polymorphic malware	Identifies new secondary payloads or malicious use of approved tools (PowerShell, etc.)
Detects with high accuracy and low false positives	Delivers a standard prerequisite for prevention	Enables fully automated responses without analyst intervention
Provides fast enforcement	Stops malware before a file can execute	Stops a process before it progresses to the next phase
Maintains context across the kill-chain	Provides multiple opportunities to mitigate a threat	Provides additional context to drive detection and fast enforcement
Delivers conclusive insights and visibility into a threat		Provides analysts with answers instead of more work, delivering forensics for investigations by choice

Clean Signal and Early Action

By combining AI-based approaches to prevention and EDR, we can deliver security at a speed matching or outpacing the threat. This allows us to fundamentally shift the dynamic of EDR from reactive responses to real-time countermeasures. Fast, reliable AI running on the host allows actions to be taken early, drastically reducing the number of events that require analysts. An AI-enabled EDR ensures that analysts can focus on the truly exceptional events without having to first sort through countless meaningless ones.

When further investigation is warranted, AI can provide analysts with defensible conclusions. By bringing together AI-driven prevention and AI-driven EDR, organizations achieve true prevention, fully automated security orchestration, and improve the productivity of human analysts.

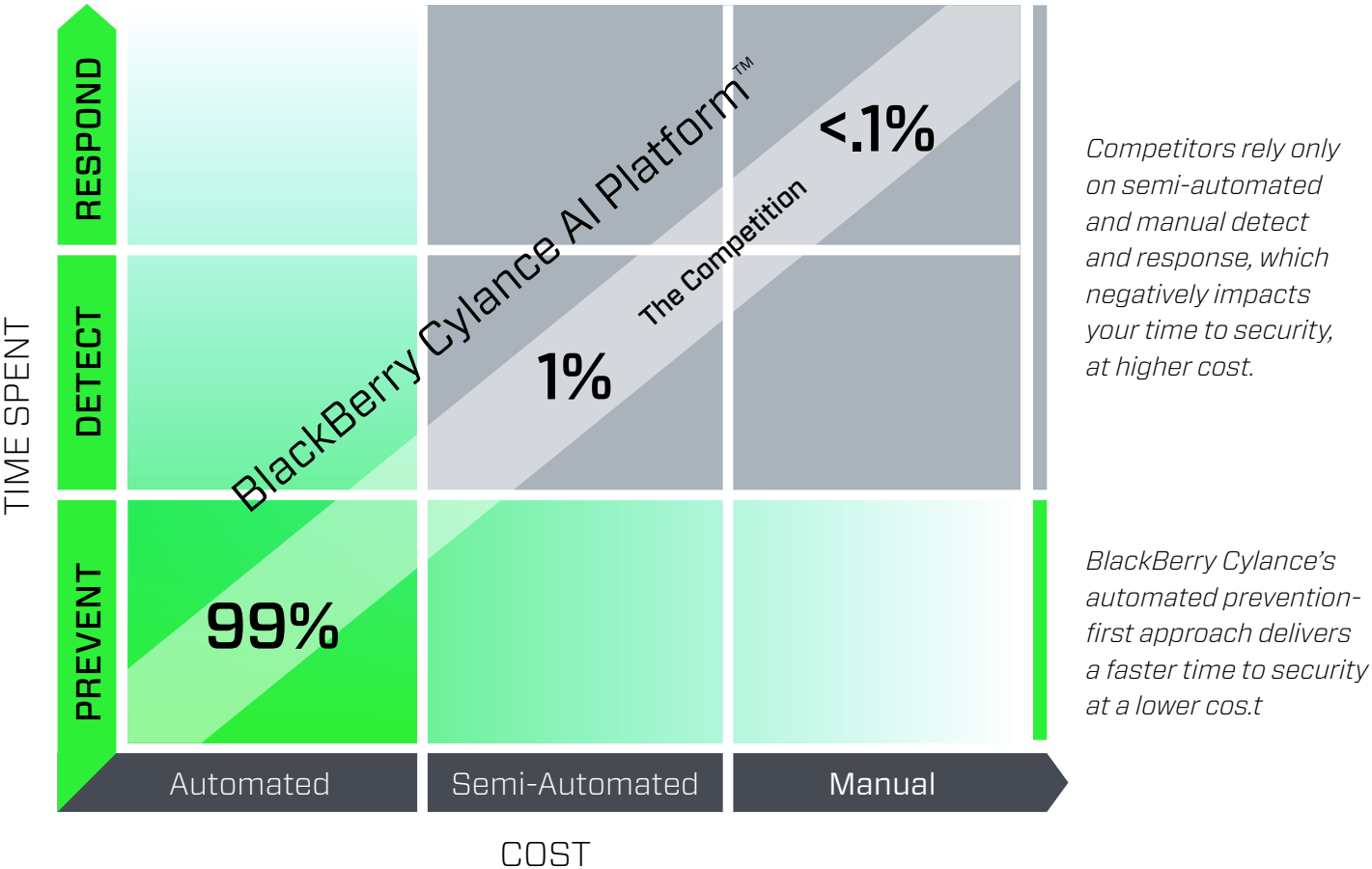
EDR and the Need for Machine-Speed AI

The speed of a cybersecurity solution can be the key to disrupting an attack. Many EDRs are facing challenges in relation to how quickly they can detect a threat and drive an automated response. In this section, we will take a look at the strategic challenges facing traditional EDR and how host-resident AI can deliver fast and effective countermeasures.

ATT&CK, Kill-Chains, and Shifting Left

Teams are increasingly relying on cybersecurity kill-chains and tools like the MITRE ATT&CK framework to understand the progression of an attack and related TTPs. EDR solutions have become invaluable tools for identifying and tracking many of these TTPs. Following a standardized framework helps security professionals detect threats and creates valuable context by correlating information across all phases of an attack.

Automated Prevention-First Security





The endpoint monitors the host for signs of obvious threats, but the more advanced machine learning operations are strictly cloud-based.

However, it is not enough to simply document the phases of an attack. With each progressive step, the attack may become more difficult to remediate and cause additional material damage. Persistence techniques may require manual recovery of a device or even re-imaging of the host. Privilege escalation can allow attackers to access sensitive data or systems and perform lateral movement that expands the scope of the attack.

As a result, it is incumbent on EDR solutions to shift high-confidence detection and mitigation as early in the kill-chain as possible. This is where speed becomes crucial to the success of cybersecurity. Threats run on a compromised host at near machine-speed and can lead to a compromise of data within minutes. In order to disrupt the threat, EDR detection and mitigation must be able to take action before an attack stage completes.

### **EDR and Why the Fight Must Happen on the Host**

Given that EDR is a host-based technology, it may seem odd to highlight the importance of performing security work on the endpoint. After all, endpoint is the E in EDR. However, many EDR responses lag well behind threats. Understanding why requires a brief overview of how threat information is processed.

While EDRs obviously have an endpoint component, the brains of the solution almost universally resides in the cloud. The endpoint monitors the host for signs of

obvious threats, but the more advanced machine learning operations are strictly cloud-based. This arrangement requires the endpoint to collect and send metadata to the cloud for analysis. While data is being analyzed, the active threat continues to execute attack phases and spread to other endpoints.

A similar problem faces EDR solutions that use signature-based enforcement. An EDR can analyze a file, often identify it as a threat, and create a hash-based signature to use for future enforcement. While this is an improvement, it does nothing to protect an already infected host. In many cases, the next malware infection will self-modify (polymorphism) to avoid the hash-based signature causing the cycle to repeat indefinitely.

### **The BlackBerry Cylance Approach: Machine Speed Detection and Mitigation**

BlackBerry Cylance EDR deploys a lightweight security AI on the host to identify new threats and act before a file executes or a service completes a phase. This is an extension of the same technology that allowed BlackBerry Cylance to deliver predictive endpoint protection. In the BlackBerry® Cylance® model, prevention and EDR work together. New files are analyzed in milliseconds and protective measures are applied before the file executes. Instead of creating hashes for future targets, BlackBerry Cylance protects the current host under attack. This same concept applies to other phases of the attack; AI on the host that analyzes actions and services in real time, disrupting malicious operations before they complete.

## Where the Data Resides Matters

Performing analysis on the host also affects how EDR data is handled at rest. For example, the traditional cloud-based approach to EDR requires large amounts of data to be sent to the cloud for analysis. Since these products lack intelligence on the host, they are forced to act somewhat like flight data recorders, pumping all data to the cloud for analysis and storage.

This approach comes with significant business implications. First, once data leaves the machine, a variety of data privacy and regulatory issues come into play (such as GDPR requirements). Secondly, each host is generating large amounts of data that must be stored and subsequently analyzed. While data storage is relatively inexpensive, it certainly isn't free. Storing high volumes of low-value data for every protected host quickly becomes costly. Lastly, stored information needs to be analyzed by security staff, which has an impact on daily security operations. It's somewhat ironic that EDR products claiming to find a signal in the noise are often the source of noise in the first place.

Performing threat analysis on the host resolves these issues. Storing and analyzing data on-device also allows our EDR to control what information is shared off-host. Private data can remain on the device while security-relevant artifacts are sent for archival and further analysis.

## Intelligence That Empowers Analysts, Hunters, and Automation

Intelligence is a term that is often misused in security today. So-called intelligence feeds deliver an endless supply of IOCs, signatures, reputation lists, and raw information intended to help security teams. Increasingly, data is fed into data lakes that are used by analysts to correlate and enrich information from their daily alerts and events. Threat hunters use these data repositories to seek out threats that may have slipped by their security controls.

However, this level of information is security data, not security intelligence. The actual intelligence is human in nature. The analyst is required to synthesize the data, put it in the proper context, and make decisions. While this is valuable work, it is time-consuming, tedious, and often delivers answers too late to prevent damage.

### Defining EDR Intelligence

Effective EDR needs to deliver intelligence in a way that shifts the heavy lifting away from human analysts. Let's take a moment to define what we mean by intelligence in the context of EDR. In practical terms, intelligence is

the information needed to make an informed decision about an event. Intelligence is not simply collated data; intelligence needs to have consumed the data, analyzed it, and synthesized it into a defensible conclusion. This conclusion should be prescriptive enough to stop the progression of a threat, not simply analyze what has already happened.

In order to deliver this actionable definition of intelligence, analysts need to have confidence in the threat data. In the BlackBerry Cylance approach to EDR, this confidence is built from three Cs — content, conduct, and context:

- Content refers to potentially malicious items such as payloads, malware, etc.
- Conduct refers to actions, and there are thousands of them, such as injecting into a whitelisted process, downloading payloads, or using PowerShell for malicious goals
- Context lets us frame all threat content and conduct as a unified malicious event that requires action

Using these underlying components, we can quickly provide high-confidence answers that can drive effective actions on the host.

### Intelligence Should Automate Work, Not Generate Work

Traditional EDR requires the skills of an organization's highly trained and expensive analysts. While an EDR can help a Tier 1 analyst confirm a threat as a true positive, the job of understanding the threat and determining responses still goes to Tier 3 analysts. This means that many EDRs have just enough intelligence to automate the creation of new work for the most valuable and overworked staff in an enterprise.

AI-enabled EDR should act as a virtual, automated SOC that runs on the host. With the ability to make fast, high-confidence detections, an AI-driven EDR can incorporate an organization's policies and automate appropriate response actions. This can include running remote scripts automatically, collecting low-level forensics, and locking down the device. These actions can all be driven automatically and in near real time, effectively reducing the workload on highly skilled analysts.

### Explainable Intelligence for Analysts and Hunters

In order to provide real value to incident responders, threat hunters, and orchestration systems, EDR needs to deliver actionable intelligence. Effective EDR provides explainable answers that people and systems can use without having to perform analysis themselves. This is where BlackBerry Cylance's AI-driven EDR sets itself apart from traditional solutions.

Using predictive AI, BlackBerry Cylance is able to provide an analyst with insightful answers about a new or unknown binary. Just as importantly, the information is explainable in human terms. For example, without any IOCs or prior knowledge of the file, BlackBerry Cylance's AI can determine a file acts as a trojan, a backdoor, or has worming capabilities. This allows analysts both to accelerate the triage and IR playbooks associated with detected threats.

Intelligence for Security Automation

The industry has increasingly adopted new detection solutions, such as security orchestration, automation, and response tools, also known as SOAR. These technologies use orchestration playbooks that can automatically bring together context from disparate solutions and even integrate with security enforcement products. However, in many cases, these playbooks run into the same problems as traditional EDR. If detections lack confidence, the playbook must often go through a human analyst for confirmation before the SOAR will act.

BlackBerry Cylance's ability to use AI to drive high-confidence detections allows orchestration tools to deliver on their original promises. While the BlackBerry Cylance EDR can easily enforce security on the host, an integration with a SOAR can allow our threat intelligence to drive other controls, such as firewall rules, to block malicious URLs or IP addresses. This extends the power of an organization's entire security infrastructure without negatively impacting valuable human resources.

An Introduction To the BlackBerry Cylance Solution

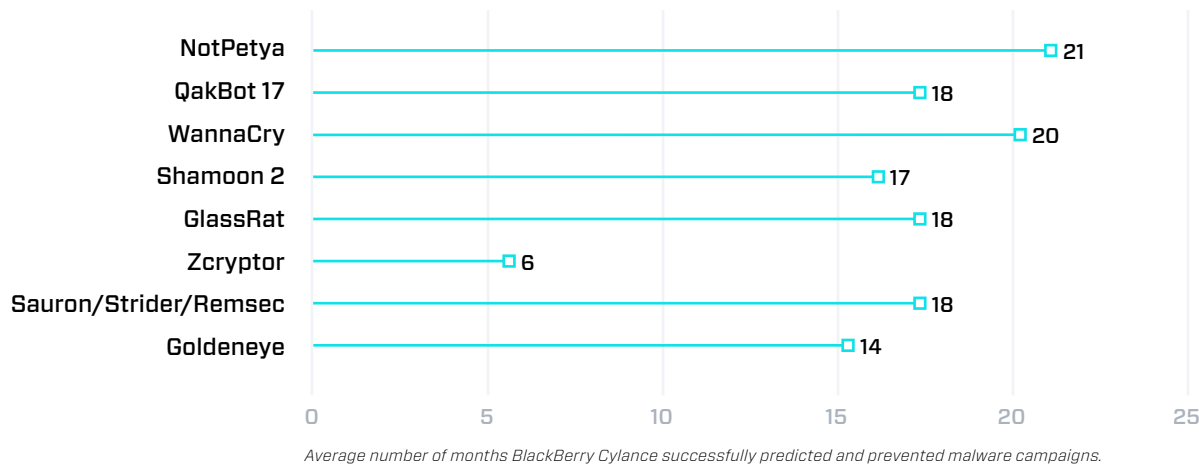
BlackBerry Cylance provides an advanced approach to threat prevention and EDR with its products CylancePROTECT® and CylanceOPTICS™. Our approach brings coordinated protection that extends across all phases of an attack. BlackBerry Cylance solutions are built on revolutionary AI that can identify unknown threats within microseconds without using signatures. During the prevention phase, CylancePROTECT can block a threat before it executes. During later stages, CylanceOPTICS can stop processes before they spawn the next phase of attack. Our solutions provide consistent coverage across the kill-chain and deliver high-confidence threat intelligence to analysts and automation tools.

Prevention First

The BlackBerry Cylance solution includes both the prevention product, CylancePROTECT, and the EDR product, CylanceOPTICS. These solutions work together to identify and stop threats as early in the kill-chain as possible. By focusing on preventing threats, the BlackBerry Cylance solution is able to keep attempted attacks from turning into actual security incidents. This, in turn, leads to fewer event alerts and a lighter workload for the security operations team.

Our prevention capability is built on innovations in predictive AI, which can identify threat features years before active samples are released in the wild. Predicting future threats may seem like an unusual claim, but it is one that can be studied empirically. While we can't test malware from the future, we can test new malware against older versions of BlackBerry Cylance products. In doing such tests, we can measure how far back in time BlackBerry Cylance products would have been able to identify a given threat. The chart below summaries how far in advance our predictive AI was able to detect some of the most notorious malware families today:

Prediction Allows for Pre-Zero-Day Prevention





Our threat verdicts can be rendered in milliseconds, on the host, without the need to lookup information from the cloud. CylancePROTECT can even detect and block a malicious payload before it executes. This offers an advanced and effective frontline of defense for unknown, polymorphic, and zero-day threats.

Fast, Actionable EDR

CylanceOPTICS extends the same capabilities found in CylancePROTECT, including ultra-fast host-based detection, mitigation, threat intelligence, visibility, and context across the entire kill-chain. The solution resides on the host, thereby avoiding the communication bottlenecks that allow threats to outpace traditional EDR solutions. The ability to detect malicious actions within milliseconds allows BlackBerry Cylance products to stop attacks in progress, limiting the overall damage inflicted by incidents and reducing cleanup costs.

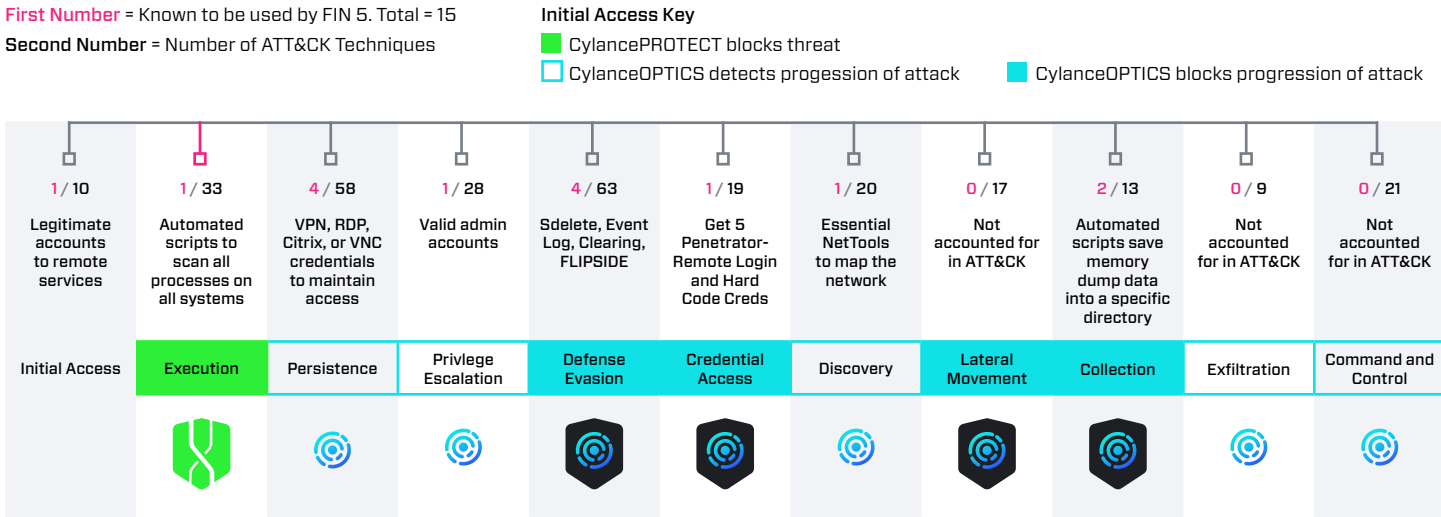
As an example, we can look at an attack by the threat group known as FIN5. This group developed their own malware and used several TTPs. Many of these TTPs were covered

in the MITRE ATT&CK framework, but some were not. The illustration below shows how CylancePROTECT and CylanceOPTICS work together across the life cycle of the attack. The illustration highlights areas where:

- CylancePROTECT can block a threat (green shield icon)
- CylanceOPTICS can detect the progression of an attack (CylanceOPTICS icon without shield)
- CylanceOPTICS can autonomously block the progression of an attack (dark grey shield icon)

Our solution enables autonomous actions on the host and can correlate and contextualize threat information across the environment. It delivers actionable intelligence to analysts and can drive automated, playbook-driven responses. CylanceOPTICS also provides the ability to dive into any issues across the enterprise for enhanced on-demand threat hunting.

How Our Products Worked Together During a FIN 5 Attack



## Enabling Security Operations and SOAR

Cybersecurity solutions must quickly deliver high-confidence results while working with other security tools and following security operations processes. Security orchestration, automation, and response (SOAR) has been one of the fastest-growing areas of security in the past several years. When done correctly, SOAR tools can be incredibly powerful and allow security operations teams to automate end-to-end responses enriched by all the tools in the ecosystem.

Unfortunately, many benefits of SOAR are degraded by low-quality data provided from security solutions. In fact, many modern SOAR playbooks require a human-dependent phase where an analyst must investigate multiple data sources before acting. BlackBerry Cylance's ability to deliver high-confidence threat verdicts in near real-time enables SOAR to run fully automated playbooks at machine speed. This empowers SOAR to deliver on its mission instead of merely functioning as a data analytics and aggregation platform.

## Conclusion

Organizations need the ability to reliably detect known and unknown threats, respond to them, and extend the cybersecurity fight across all phases of attack. BlackBerry Cylance applies a proven, AI-based approach that brings unrivaled speed and accuracy to endpoint protection, threat detection, and mitigation. Handling threat intelligence on the endpoint enables systems to detect and stop threats at machine speed instead of simply documenting their progress from the cloud. This transformative leap improves endpoint protection platforms, and endpoint detection and response, while making enterprises significantly safer.

If you have questions about any of the content in this document or would like to learn more, contact us at [www.cylance.com](http://www.cylance.com).

## About BlackBerry Cylance

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



**+1-844-CYLANCE**  
[sales@cylance.com](mailto:sales@cylance.com)  
[www.cylance.com](http://www.cylance.com)

