CYLANCE

The Future of EDR Is Here

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

There is no doubt that organizations stand to benefit from endpoint detection and response (EDR) technologies, which enable 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.

CYLANCE OPTICS

As the first AI driven EDR solution, CylanceOPTICS delivers self-contained, automated, machine learning threat detection modules that have been designed to uncover threats that would be nearly impossible to find with static behavior rules. We invite you to learn more about the distinct evolution in individual traits that indicate CylanceOPTICS is the future of EDR.

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 your 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 to determine 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*

5 Unmistakable Characteristics of Evolved EDR

01
Can be installed on any endpoint in minutes

02
Requires no hardware or expensive data streaming

03
Does not require constant updates

04
Enables zero-latency detection and response by storing and analyzing data locally on the endpoint

05
Delivers self-contained, automated, machine learning threat detection modules that uncover otherwise hard to find threats

Learn more about the future of EDR at cylance.com/optics