# 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 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* |

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

CYLANCE



20181217-1479