FEATURES BREAKDOWN	COMODO DRAGON ENTERPRISE	Kaspersky
EPP Capabilities		
Signature-based anti-malware protection	✓	✓
Machine learning/algorithmic file analysis on the endpoint	✓	✓
Machine learning for process activity analysis	✓	✓
Process isolation	✓	✓
Memory protection and exploit prevention	✓	✓
Protection Against Undetected Malware	✓	✗
Application whitelisting	✓	✓
Local endpoint sandboxing/endpoint emulation	✓	✗
Script, PE, or fileless malware protection	✓	✓
Integration with on-premises network/cloud sandbox	✓	Requires Additional Product(s)
Real-time IoC search capabilities	✓	✓
Retention period for full access to data	No limit	1 month
Endpoint Firewall	✓	✓
FW Learning Mode	✓	✗
Automatically creates network traffic rules	✓	✗
URL Filtering	✓	✓
Host Based IPS	✓	✓
USB device Control	✓	✓
Full Device Control (Device Control based on Device Class product ID, Vendor ID and Device Name)	✓	✓
Agent self-protection/remediation or alerting when there is an attempt to disable, bypass, or uninstall it	✓	✓
Ransomware protection	✓	✓
Protect/block ransomware when "Offline" or "Disconnected" from the internet?	✓	✗
VDI support	✓	✓
Manage, and maintain, an application control database of known "trusted" applications?	✓	✓
Multi-tenant cloud based service	✓	✓
EPP management console available as an on-premises virtual or physical server/application	✓	✓
Consolidated EPP management console to report on, manage, and alert for Windows macOS clients and mobile	✓	✓
Data loss prevention	✓	Requires Additional Product(s)
Mobile Device Management	✓	Requires Additional Product(s)
Mobile threat Defense	✓	Requires Additional Product(s)
Vulnerability and patch management	✓	✓
Network/Cloud sandboxing	Cloud Sandbox	Cloud Sandbox
Security Orchestration, Analysis and Response (SOAR) Integration	✓	✓
Network discovery tool	✓	✓
Remote Access	✓	✗
Remote scripting capabilities	✓	✗
Default Deny & Containment		
Default Deny Security with Default Allow Usability	✓	✗
Run unknown files with Auto Containment Protection	✓	✗
Create Virtual environment for any unknowns	✓	✗
Virtualize file system, registry, COM on real endpoints	✓	✗
EDR		
Telemetry (observables)		
Interprocess Memory Access	✓	✓
Windows/WinEvent Hook	✓	✓
Device Driver Installations	✓	✓
File Access/Modification/Deletion	✓	✓
Registry Access/Modification/Deletion	✓	✓
Network Connection	✓	✓
URL Monitoring	✓	✓
DNS Monitoring	✓	✓
Process Creation	✓	✓
thread Creation	✓	✓
Inter-Process Communication (Named Pipes, etc) up to this	✓	✓
Telemetry data itself can be extended in real time	✓	✗
Event chaining and enrichment on the endpoints	✓	✗
Detection/Hunting/Reporting		
Adaptive Event Modelling	✓	✗
Behavioral analysis (e.g. analysis over active memory, OS activity, user behavior, process/application behavior, etc.)	✓	✓
Static analysis of files using capabilities such as machine learning (not including signature based malware detection)	✓	✓
Time-series analysis	✓	✗
Integration with automated malware analysis solutions (sandboxing)	✓	✗
threat Hunting interface or API for searching with YARA/REGEX/ElasticSearch/IOC	Yes without Yara	IOC and Yara
Support for matching against private IOC	✓	✗
threat Intelligence integration (TIP, upload, webservice connector, etc) to enrich and contextualize alerts	✓	✓
Linking telemetry (observable data) to recreate a sequence of events to aid investigation	✓	✓
Process/attack visualization	✓	✓
Incident Response Platform (IRP) or orchestration integration?	✓	✓
Vulnerability reporting (ex. reporting on unpatched CVEs)	✓	✓
Alert prioritization based on confidence, able to define thresholds for alerting.	✓	✓
Alert prioritization factors system criticality	✓	✓
Able to monitor risk exposure across environment organized by logical asset groups	✓	✓
Reporting interface identifies frequent alerts that may be appropriate for automating response	✓	✓
Response		
Remote scripting capabilities	✓	✗
Quarantine and removal of files	✓	✓
Kill processes remotely	✓	✓
File retrieval	✓	✓
Network isolation	✓	✓
Filesystem snapshotting	✓	✓
Memory snapshotting	✓	✓
MDR		
Managed endpoints		
Manage customer endpoints and policies	✓	✓
Incident Investigation & Response	✓	✓
Preemptive containment	✓	✗
Application profiling (AI support)	✓	✓
Customizable policy creation	✓	✓
Central monitoring of all endpoints	✓	✓
Live remote inspection	✓	✗
Tuning of monitoring rules for reduction of false positives	✓	✗
Forensic analysis	✓	Requires Additional Product(s)
Managed network		
Cloud- based SIEM and Big Data Analytics	✓	Requires Additional Product(s)
Log data collection/correlation	✓	Requires Additional Product(s)
Threat intelligence integration	✓	Requires Additional Product(s)
Network profiling (AI support)	✓	Requires Additional Product(s)
Available as virtual or physical	✓	Requires Additional Product(s)
Integrated file analysis (cloud sandbox)	✓	Requires Additional Product(s)
Full packet capture	✓	Requires Additional Product(s)
Protocol analyzers for 40+ different protocols such as TCP, UDP, DNS, DHCP, HTTP, NTLM, etc. w/full decoding capability	✓	Requires Additional Product(s)
Managed cloud		
Includes ready-to-use cloud application connectors for:		
Azure	✓	Requires Additional Product(s)
Google Cloud Platform	✓	Requires Additional Product(s)
Office 365	✓	Requires Additional Product(s)
AWS	✓	Requires Additional Product(s)
Threat detection for cloud applications	✓	✗
Log collection from cloud environments	✓	Requires Additional Product(s)
Generating actionable incident response from cloud application	✓	✗
Threat intelligence and Verdict		
inHolistic security approach Combined network, endpoint, cloud	✓	✗
Internal security sensor logs (IOCs)	✓	✓
Expert Human Analysis	✓	Requires Additional Product(s)
ML & Behavioral Analysis and Verdict	✓	✓
Open source threat intelligence feeds	✓	✓
Information sharing with industry	✓	✓
Clean web (phishing sites, keyloggers, spam)	✓	✓
Deep web (C&C servers, TOR browsers, database platform archives—pastebins)	✓	✓
Cyber Adversary Characterization	✓	✓
Security operations center (SOC)		
Global, real-time support (24 / 7 /365)	✓	✓
Dedicated cybersecurity expert	✓	✓
Breach (case) management	✓	✓
Security monitoring	✓	✓
Incident analysis	✓	✓
Incident response (handling)	✓	✓
Extensive threat hunting (scenario-based)	✓	✓