<table>
<thead>
<tr>
<th>Feature</th>
<th>Symantec</th>
<th>COMODO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Security</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Endpoint Security</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Log Data Collection/Correlation</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Cloud-based SIEM and Big Data Analytics</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Live Remote Inspection</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Customizable Policy Creation</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Preemptive Containment</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Incident Investigation &amp; Response</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Memory Snapshotning</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>File Retrieval</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Kill Processes Remotely</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Alert Prioritization Based on Controllability</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Vulnerability Reporting (e.g., reporting on unpatched CVEs)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Incident Response Platform (IRP) or orchestration integration?</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Threat Intelligence Integration (TIP, upload, webservice)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Integration with automated malware analysis solutions</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Time-series Analysis</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Event Chaining and Enrichment on Endpoints</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Telemetry Data Itself Can Be Extended In Real Time</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>DNS Monitoring</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>File Access/Modification</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>USB Device Control</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Protection Against Undetected Malware</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Memory Protection and Exploit Prevention</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Machine Learning/Algorithmic</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Signature-based Anti-malware Protection</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Security Orchestration, Analysis, and Response (SOAR) Integration</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>YARA/REGEX/Elasticsearch/IOC</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Mobile Threat Defense</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Dragoon Enterprise EPP Capabilities</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>DRAGON ENTERPRISE Features Breakdown</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Incident Analysis</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Breach (Case) Management</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Global, Real-time Support (24/7/365)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Information Sharing with Industry</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Retention Period for full access to data</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Integration with On-premises Network/Cloud Sandbox</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Local Endpoint Sandboxing/Endpoint Emulation</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Protection Against Malware</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Fileless Malware Protection</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Remote Scripting Capabilities</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>MULTI-DETECTOR</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Advanced Threat Intelligence</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Signature-based Malware Protection</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Machine Learning/Algorithmic</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Signature-based Anti-malware Protection</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Security Orchestration, Analysis, and Response (SOAR) Integration</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>YARA/REGEX/Elasticsearch/IOC</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Mobile Threat Defense</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Dragoon Enterprise EPP Capabilities</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>DRAGON ENTERPRISE Features Breakdown</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Incident Analysis</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Breach (Case) Management</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Global, Real-time Support (24/7/365)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Information Sharing with Industry</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Retention Period for full access to data</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Integration with On-premises Network/Cloud Sandbox</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Local Endpoint Sandboxing/Endpoint Emulation</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Protection Against Malware</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Fileless Malware Protection</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Remote Scripting Capabilities</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>MULTI-DETECTOR</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Advanced Threat Intelligence</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>