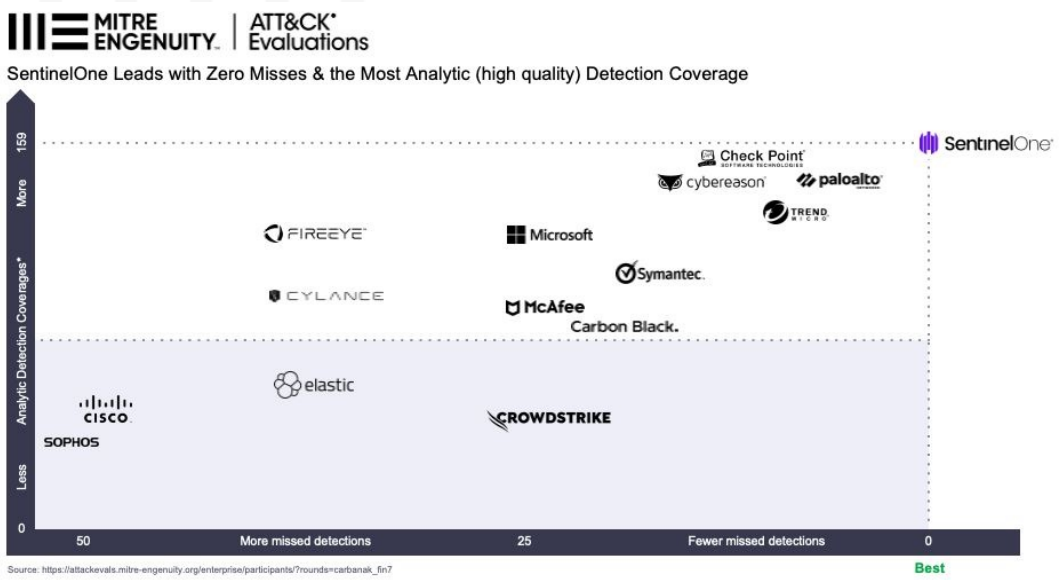
CAPTURE CLIENT VS KASPERSKY ENDPOINT TOTAL SECURITY FOR BUSINESS

	Feature	SonicWall Capture Client	Kaspersky Total Security for Business
SentinelOne / Gartner peerinsights / AV-TEST Approved Corporate Endpoint Protection	Endpoint Protection & Detection	✓ On-device Static AI - Yes ✓ On-device Behavior AI - Yes ✓ Exploits, Malicious Scripts – Yes, AI + Full Context ✓ Lateral Movement – Yes, AI + Full Context	✓ On-device Static AI – Yes x On-device Behavior AI - Partial / Limited Behavioral AI x Exploits, Malicious Scripts – Partial: Legacy Signatures + Cloud x Lateral Movement – Partial: Legacy Signatures + OS Events x Kaspersky is still heavily reliant on signatures for detection on the endpoint, and cloud lookups when those fail. This is the aging (and ineffective), legacy-AV, model.
	Response	✓ Remediation - Automated ✓ Rollback - Automated	x Remediation: Manual / Limited Automation ✓ Rollback: Yes: Proprietary non-VSS feature
	Device Control	✓ USB Control - Yes ✓ Bluetooth Control - Yes	✓ USB Control – Yes x Bluetooth Control – No
	1-Click Endpoint Quarantine	✓ Automatically puts the device in Network Quarantine when an active threat is detected reducing response time and ensure productivity. ✓ Block and Quarantine attacks before they spread.	x No Such feature is offered
	Application Vulnerability	✓ Visibility into applications that have high-risk vulnerabilities ✓ Administrators can prioritize patch efforts & also blacklist processes launched by unauthorized applications.	✓ Yes – Application Vulnerability is offered as a part of the total Protection.
	Network Control	✓ Host based firewall – yes	✓ Host based firewall – Yes
	Threat Hunting	✓ Storyline based threat hunting ✓ Deep Visibility for all endpoint activity ✓ Automated threat hunting and custom alerts	x Threat Hunting is Manual x High Level IOC based
SONICWALL	Cloud ATP Analysis	✓ Capture ATP provides cloud-based multi-engine sandbox and helps detect and block threats with Real-Time Deep Memory Inspection. ✓ Sonicwall CATP proved highly effective against 98.9% of previously unknown threats while having mere 1.7% false positives in accordance to a latest report from ICSA Labs.	✓ Yes – as an Add- on product increasing cost and maintenance overhead.
	Content Filtering	✓ Block malicious sites IP addresses, and domains ✓ Increase user productivity by throttling bandwidth or restricting access to objectionable or unproductive web content.	✓ Yes – Content Filtering is offered with this package.
	Firewall Integration	✓ Integrates with Sonicwall firewall to enforce capture client deployment preventing rouge endpoints gaining access to corporate network. ✓ Reduces admin overhead to push certificates on Endpoints to enable DPI SSL functionality as it can be done via policy using Capture Client Cloud Console. ✓ Periodically send logged on user info from capture client endpoints to sonicwall firewalls via SSO integration. ✓ End user network threat notifications can be provided to managed endpoints.	x No Integration with SonicWall Firewalls.
	Unified Management	✓ Capture Security Center (CSC) is a single console to manage network security, endpoint security & other SonicWall solutions for all offerings basic and Advanced. ✓ Integrated analytics between Firewall & Endpoint provides a seamless investigation experience.	✓ Yes – Has a Cloud based Management Console. x Their Agent-less Virtualization product for VMware only works against file-based attacks (limitation of VMware API they use to integrate with) x To handle large amounts of remote client's customers, have 2 options: • Implement a Connection Gateway in the DMZ (requires 1 gateway per 250-500 clients) • - OR - Implement a separate Administration Server in the DMZ. The Customer now must deal with 2 consoles, 2 databases, 2 systems to maintain.

SENTINELONE IS #1 IN THREAT DETECTION (SOURCE: MITRE ATT&CK 2020 EVALUATIONS)



MITRE Carbanak+FIN7 Evaluations

	Telemetry Detections (Out of 174)	Telemetry + Analytic Detections (Out of 174)	Overall Detection Rate
SentinelOne	164	174	100.00%
paloalto	154	169	97.13%
TREND MICRO	162	167	95.98%
Check Point	161	162	93.10%
cybereason	153	160	91.95%
Bitdefender	150	158	90.80%
Symantec.	143	159	91.38%
vmware Carbon Black	152	154	88.51%
Cynet	140	153	87.93%
CROWDSTRIKE	141	152	87.36%
F-Secure.	137	152	87.36%
McAfee	148	151	86.78%
Microsoft	148	151	86.78%
eset	143	147	84.48%
Fidelis Cybersecurity	147	147	84.48%

	Telemetry Detections (Out of 174)	Telemetry + Analytic Detections (Out of 174)	Overall Detection Rate
BlackBerry	134	141	81.03%
elastic	138	140	80.46%
REAQTA	119	135	77.59%
FIREEYE	117	136	78.16%
CYCRAFT	128	130	74.71%
Uptycs	124	127	72.99%
opentext	122	125	71.84%
CISCO	112	122	70.11%
MICRO FOCUS	56	122	70.11%
SOPHOS	114	118	67.82%
FORTINET	113	117	67.24%
Malwarebytes	99	116	66.67%
GoSecure	84	100	57.47%
AhnLab	80	90	51.72%

eSecurity Planet

KASPERSKY CAUTIONS (SOURCE: GARTNER EPP MAGIC QUADRANT - MAY 2021)

- The EDR emphasis is very much on protection and automated response; as a result, Kaspersky doesn't provide response capabilities that are as extensive as other vendors in this research. For example, it does not offer prebuilt playbooks (other than automatic remediation) or the ability to create response playbooks.
- Kaspersky Anti Targeted Attack, a separate product, is required to carry out more extensive threat hunting actions involving analysis of network activity.
- Despite a wide range of products covering cloud workloads, email and operational technology (OT), there is more limited correlation of information between these solutions and XDR capabilities than is provided by the leading vendor solutions in this research.
- Kaspersky products were involuntarily not represented in the last MITRE ATT&CK evaluations (Enterprise 2020 and ICS 2020 evaluations). During the finalization stage of the Enterprise 2020 evaluation, Kaspersky says MITRE notified it that its participation had been discontinued. MITRE has not publicly explained why.