esentire

BETTER TOGETHER
Managed Endpoint Defense & esENDPOINT

	MANAGED ENDPOINT DEFENSE		esENDPOINT		DIY	
	Managed Endpoint Defense	Client Responsibilty / Action Required	esENDPOINT	Client Responsibilty / Action Required	Included With CB Defense & CB Response	Client Responsibilty / Action Required
FOCUS	Optimized and adaptable threat prevention using next-gen antivirus platform		Hunt for threats that have bypassed preventative measures like next-gen antivirus			
STAGE	Pre-incident/stop malicious from happening		Post-incident/malicious suspected			
GOAL	Prevent incidents from happening and assist in response when they do occur		Minimize detection to containment/ remediation timeframe, determine root cause and corrective actions.			
Initial agent deployment		✓		✓		✓
Initial configuration (rules and policies)	✓		✓			✓
24x7 monitoring	✓	✓	✓			✓
PREVENTION WITH AUTOMATED BLOCKING						
Malware prevention	✓				CB Defense Only	
Exploit prevention	✓				CB Defense Only	
Ransomware prevention	✓				CB Defense Only	
Configurable tool, tactics and procedure blocking	✓				CB Defense Only	

	MANAGED ENDPOINT DEFENSE		esENDPOINT		DIY	
	Managed Endpoint Defense	Client Responsibilty / Action Required	esENDPOINT	Client Responsibilty / Action Required	Included With CB Defense & CB Response	Client Responsibilty / Action Required
DETECTION WITH SOC RESPONSE						
Evasive malware detection	Limited		✓		Limited	✓
Post exploitation detection	Limited		✓		Limited	✓
Adversary detection	Limited		✓		Limited	✓
Tactical threat containment (host isolation)		✓	✓			✓
Executive dashboard/portal	✓		✓		✓	
Dashboard/portal setup and customization			✓			✓
Records and stores full data record of endpoint	Limited		✓		✓	
Centralized recording of full endpoint telemetry			✓		CB response only	
CONTINUOUS TUNING						
Merge and manage the signal set into a standard configuration	✓		✓			✓
Refinements and updates to account for client's specific environment	✓	✓	✓			✓
SITUATIONAL AWARENESS						
Investigation of signals that don't currently have a known explanation			✓			✓
Determine a root cause for an event without explanation within 20 minute SLO			✓			✓
Process and binary search of centralized data	✓	✓	✓			✓

	MANAGED ENDPOINT DEFENSE		esENDPOINT		DIY	
	Managed Endpoint Defense	Client Responsibilty / Action Required	esENDPOINT	Client Responsibilty / Action Required	Included With CB Defense & CB Response	Client Responsibilty / Action Required
Behavioral detection	✓* (Limited to 110+ core behaviors)		✓		✓* (CB Defense, limited to 110+ core behaviors)	
Machine learning integration (unknowns/ file-less attacks such as Powershell)	Limited		✓		Limited	✓
Patterns/IoCs	✓		✓		✓	
Anomaly detection	Limited		✓		Limited	
Attack chain visualizations	✓		✓		✓	
Advanced analytics	✓		✓		✓	
CB threat intel feeds	✓		✓		✓	
Customized threat feeds			✓			✓
Proactive threat hunting			✓			✓
Basic forensics post Incident	✓		✓			✓
Full forensic investigation post incident			✓			✓
Correlation with network activity*			✓			Requires your own SOC
Correlation with logs*			✓			Requires your own SOC
DIY quarentine and isolation		✓		✓		✓
Alerting of suspicious behavior	✓	✓	✓			✓
Alerting of confirmed threats	✓	✓	✓			✓
False positive reduction	✓		✓		✓	
False positive elimination	✓	✓	✓			✓
Co-managed remediation	✓	✓	✓	✓		✓
Host reimaging		✓		✓		✓

About eSentire:

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire**.

About Carbon Black:

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,600 global customers, including one-third of the Fortune 100, trust Carbon Black to keep their organizations safe.