eSENTIRE

Better Together:
eSentire Managed Detection and Response and Managed Vulnerability Service

In 2016, Gartner launched its Managed Detection and Response (MDR) Guide, validating the category within the managed security services market. Gartner's recognition of MDR resulted from disparity between the evolving threat landscape and traditional MSSP capabilities. This new MDR category put traditional MSSPs on notice, but categories and criteria by which to measure MDR providers was absent. The 2018 Gartner MDR Guide reviews more providers, including MSSPs that now claim to deliver MDR, yet still lacks measurement criteria. This creates a confusing MDR vendor landscape and subjects unsuspecting buyers to unnecessary risk.

This chart, reflecting eSentire's collective service capabilities, was built to help your organization measure the MDR vendor landscape and visualize the risk associated with inclusion or removal of signals from network, endpoint, logs, and vulnerability data across key categories including:

- Visibility
- Advanced analytics
- Proactive threat hunting
- Correlation and forensic investigation
- Alerts, containment and response
- Vulnerability risk prioritization

"Clients should be wary of claims from traditional MSSPs on their ability to deliver MDR-like services. Delivering these services requires technologies not traditionally in scope for MSS, such as endpoint threat detection/response, or network behavior analysis or forensic tools."

- Gartner Managed Detection and Response Services Market Guide. May 2017.

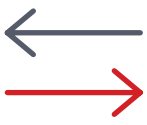
Analysts need visibility across a combination of sources including:

1. Web Traffic

2. Email Traffic

3. Cloud Access

4. Endpoints



5. Network Traffic

6. Policies and Violations

7. Vulnerabilities

		esLOG+	esENDPOINT	esNETWORK	Managed Vulnerability Service
MONITORING, MANAGEMENT AND CONTINUOUS TUNING	24x7x365 Monitoring	✓	✓	✓	Weekly Scanning (External Assets) Monthly Scanning (Internal Assets)
	Management	Co-managed	Fully managed	Fully managed	Co-managed
	Merge and manage the signal set into a standard configuration that is deployed to all boxes	Limited (we can tune esLOG+ but not the security devices that feed however we will make recommendations)	✓	✓	N/A
	Refinements and updates to account for client's specific environment are done continuously as their environment changes	✓	✓	✓	✓
VISIBILITY	**LOGS**				
	Monitors, captures and inspects logs from the following sources but not limited to:				
	• Security Events (IDS, Endpoint, DLP, VPN, Web Filters, Honeypots, Firewalls, IAM, etc.)	✓			
	• Network Logs (Routers, switches, DNS servers, WAP, WAN, Data Transfers, VPC, etc.)	✓			
	• Applications and Devices (Application Servers, Databases, Intranet Applications, Web Applications, SaaS Applications, Cloud Hosted Servers, etc.)	✓			
	• AWS (CloudTrail, Config, Inspector, S3, etc.)	✓			
	• Google Cloud Platform	✓			
	• Microsoft Azure (Active directory, Azure audit, Azure SQL, Office365)	✓			
	• Database (Amazon DynamoDB, SQL Server, MongoDB, MySQL, Oracle, etc.)	✓			
	• Web Server (Apache, Tomcat, IIS, Nginx)	✓			
	• DevOps (Docker, GitHub, Kubernetes, Jenkins, etc.)	✓			
	• IT Infrastructure (Configuration, Locations, Owners, Network Maps, Vulnerability Reports)	✓			
	• Operating System (Host Metrics, Linux, Windows, Windows Performance)	✓			
	Cloud deployment	✓			
	On-premises deployment	✗			

		esLOG+	esENDPOINT	esNETWORK	Managed Vulnerability Service
VISIBILITY	**ENDPOINT**				
	Monitors company assets at the endpoint level (host visibility)		✓		
	Inspection and recording of full endpoint telemetry		✓		
	On-premises deployment		✓		
	Cloud deployment		✓		
	NETWORK				
	Monitors ingress and egress chokepoints and decrypted spans			✓	
	Real-time inspection of network packet utilizing full packet capture (PCAP)			✓	
	On-premises deployment			✓	
	Cloud deployment			Coming soon	
	VULNERABILITIES				
	Business contextual risk prioritization				✓
	Remediation guidance and verification				✓
	Web Application scanning				✓
	PCI Environment scanning				✓
	On-premises deployment				
	Cloud deployment				✓
ANALYTICS AND DETECTION	**NETWORK**				
	Signatures and IoCs	✓	✓	✓	✓
	Machine-learning integration	✓	✓		✓
	Big data analytics integration	✓			
	Behavioral	✓	✓	✓	
	User behavior analytics	✓			
	Anomaly/suspicious based	✓	✓	✓	
	Monitoring and investigation of signals that are generated from any source that don't currently have a known explanation for why they would be firing	✓	✓	✓	

		esLOG+	esENDPOINT	esNETWORK	Managed Vulnerability Service
	NETWORK (CONTINUED)				
	Investigate and determine a root cause for a detection event that doesn't have an existing known explanation within a 20-minute SLO	✓	✓	✓	
	Threat intelligence integration (home grown)	✓	✓	✓	✓
	Threat intelligence integration (external integration)	✓	✓	✓	✓
HUNTING AND INVESTIGATION	**Proactive threat hunting**				
HUNTING AND INVESTIGATION	• Hypothesis-driven investigation (knowledge of a new threat actor's campaign based on threat intelligence gleaned from a large pool of crowdsourced attack data)	✓	✓	✓	
HUNTING AND INVESTIGATION	• Investigations that are based on known IoCs (Indicator of compromise)	✓	✓	✓	✓
HUNTING AND INVESTIGATION	• Analytics-driven investigations (based on advanced analytics and machine learning)	✓	✓	✓	
HUNTING AND INVESTIGATION	Confirmation of true positive (false positive elimination)	✓	✓	✓	✓
CORRELATION AND FORENSIC INVESTIGATION	Logs: can perform searches inside client logs to assist in providing more information during an investigation	✓			
CORRELATION AND FORENSIC INVESTIGATION	Network: can gather and interpret forensic data (PCAPs, netflow, metadata) from network choke points relevant to the investigation			✓	
CORRELATION AND FORENSIC INVESTIGATION	Endpoint: can gather and interpret forensic data (process flows, execution chains, etc) from affected hosts relevant to the investigation		✓		
CORRELATION AND FORENSIC INVESTIGATION	Evidence collection, dissection, processing and analysis	✓	✓	✓	✓
ALERT, CONTAINMENT AND RESPONSE	Alerting of suspicious behavior	✓	✓	✓	
ALERT, CONTAINMENT AND RESPONSE	Alerting of confirmed threats	✓	✓	✓	✓
ALERT, CONTAINMENT AND RESPONSE	Host level tactical containment		✓		
ALERT, CONTAINMENT AND RESPONSE	Network level tactical containment			✓	
ALERT, CONTAINMENT AND RESPONSE	Response plan for particular incident	✓	✓	✓	✓
ALERT, CONTAINMENT AND RESPONSE	Remediation guidance and co-remediation until threat is fully contained and eradicated	✓	✓	✓	✓
ALERT, CONTAINMENT AND RESPONSE	Portal with data visualization	✓	✓	✓	✓
ALERT, CONTAINMENT AND RESPONSE	24x7x365 SOC support	✓	✓	✓	✓

Eradicating threats takes more than alerts. LEARN MORE

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**.