eSENTIRE

Understanding Why Multi-Signal MDR Matters

Cloud adoption, business applications and remote users continue to expand at exponential rates. Your cybersecurity team is fighting a losing battle to keep pace with your business requirements and growing attack surface. While traditional security controls and MSSPs were once effective, they are no match for the growing speed and sophistication of modern threats.

Expanding Surface		Precise Attackers	Limited Resources
94%	**80%**	**54%**	**87%**
of workloads are forecasted to be in the cloud[1]	of organizations will allow users to continue to work remote[2]	of attackers can breach an organization in under 15 hours[3]	Of organizations report not having enough security resources[4]

Officially recognized by Gartner in 2016, Managed Detection and Response has exploded in popularity answering the challenge to rapidly identify advanced threats and contain them before business disrupting damage can occur. Unfortunately, the number of vendors and the variety of coverage has resulted in industry-wide confusion. While most MDR vendors claim to deliver complete protection, the fact is many provide limited signal visibility and response, leaving you unprotected against critical parts of the attack surface.

For example, one of the most popular subcategories of MDR, Managed Endpoint Detection and Response, provides coverage at the host level (endpoint) while leaving the perimeter, user, application and data layer without critical visibility and response capabilities. The significance of endpoint protection is undisputed, but keep in mind it is only one layer of a complete defense in depth approach.

On the other hand, MDR providers reliant upon logs through the usage of SIEMs may have greater visibility across the attack surface but lack the ability to contain and respond across different signal sources. Managed Detection and Response services are successful when containment can be initiated. The right mix of operational technologies and personnel must be in place for that to be effective so we can stop attackers before they accomplish their objectives.

[1] CISCO Global Cloud Index, [2] Gartner HR Survey 2020, [3] Nuix Black Report, [4] 451 Research

It's important to remember that MDR providers can only detect and respond to what they can see. For uncovered layers of the attack surface, security teams must have the people, process and technology to monitor, detect and respond to advanced and evasive threats. The critical decisions you must address are:

- What is the scope of our attack surface now and in the future?
- What level of coverage do we require across each layer of the attack surface?
- Do we have the resources to monitor, detect and contain attackers for areas that would be otherwise uncovered by an MDR provider?

At eSentire, we believe a multi-signal approach is paramount to protecting your complete attack surface. Whether your environment is in the cloud, on-premises or somewhere in between we have the visibility to see what other MDR providers will miss. Leveraging a proprietary cloud-based XDR platform and expert human threat hunters, our Managed Detection and Response services identify and stop attackers ANYWHERE your environment or users reside.

eSentire Multi-Signal Coverage

	MDR Signals	Visibility	Investigation	Response
24/7 Investigation and Response	Network	●	●	●
	Endpoint	●	●	●
	Log	●	●	●
	Cloud	●	●	●
Context Drivers	Insider	●	●	
	Managed Vulnerability Service	●	●	

Our multi-signal approach ingests endpoint, network, log, cloud, asset and vulnerability data that enables complete attack surface visibility. Enriched detections from the eSentire Threat Response Unit are applied to captured data identifying known threats and suspicious activity across every layer of the attack surface.

Automated blocking capabilities built into our eSentire Atlas XDR Cloud Platform prevent attackers from gaining an initial foothold while our expert Elite Threat Hunters can initiate manual containment at multiple levels of the attack surface. Through the use of host isolation, malicious network communication disruption, identity-based restriction and other measures, we can stop the attacker at any level.

Network: Protects from brute force attacks, active intrusions, unauthorized scanning and additional suspicious activity with real-time detection and response. Leverages behavioral based anomaly detection and attack pattern analysis to identify and neutralize threats traditional technologies miss. Captures summary meta data and full network packages.

Endpoint: Protects your assets from ransomware, trojans, spyware, root kits and more by combining elite threat hunting with next-generation anti-virus & endpoint detection and response capabilities to eliminate blind spots traditional prevention misses. Captures full endpoint telemetry.

Log: Ingests and stores logs across AWS, O365, DevOps and more. Aggregates meaningful and actionable intelligence from your network assets, endpoints, applications and cloud services providing critical threat visibility and detection while satisfying regulatory requirements.

Cloud: Comprehensive cloud security that identifies risks, monitors cloud platforms and stops attacks across software applications (SaaS) and cloud infrastructure (IaaS) through 24/7 Threat Hunting and proprietarydetection capabilities mapped to the MITRE ATT&CK(R) Framework. SaaS identifies known and elusive threats across Microsoft O365 and Google Workspace. IaaS available to protect AWS, Azure and GCP.

Insider Threat: Identifies malicious insider activity across unavoidable attack stages leveraging proprietary machine learning processes and elite threat hunters that contain attackers before they can disrupt business operations. Collects Netflow, Proxy and DNS Data.

Managed Vulnerability Service: MVS continuously identifies vulnerabilities across your on-premises and cloud environment with integrated eSentire experts that act as extension of your team providing analysis and remediation guidance. We schedule and execute scans, manage the platform and refine your risk profile while prioritizing and actioning remediation plans.

At eSentire we recognize that the attack surface is continuously evolving and expanding. While our MDR service protects your organization from modern attacks and the vectors they target, we are continuously analyzing and developing new services and detections to outpace the adversaries. Our Threat Response Unit (TRU) works tirelessly developing and testing advanced detections against emerging and hypothetical threats. Our product development team stays on the cutting-edge identifying new technologies and paths to gaining greater visibility that empowers our XDR platform and expert threat hunters. In our twenty year history, we pride ourselves on the fact that no eSentire client has experienced a business disrupting breach. With over 1000 customers across 70 countries, we are recognized globally as the Authority in Managed Detection and Response. We don't just claim to deliver complete response - we prove it. **Connect with an eSentire Security Specialist today to learn how we can support your organization with Multi-Signal Managed Detection and Response.** ▶

If you're experiencing a security incident or breach contact us ☎ 1-866-579-2200

eSentire Inc., is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Thre at Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.