

eSentire MDR for Cloud

On-Premises. In The Cloud. Hybrid. We're All-In To Protect You.

24/7 Managed Detection and Response for Cloud

We detect, investigate and respond to threats specific to multi-cloud environments leveraging our cloud-native XDR platform, proprietary MITRE ATT&CK-mapped detections, and our 24/7 Security Operations Centers (SOCs) staffed with Elite Threat Hunters and experienced Cyber Analysts.

Cloud Security Posture Management

We eliminate the risk of critical cloud misconfigurations by providing continuous cloud visibility, configuration management, asset tracking, and mapping to compliance frameworks including PCI, HIPAA, CIS, and SOC 2. Gain comprehensive visibility across your cloud infrastructure with anomaly-based threat detection and proactive, prioritized cloud threat response.

Cloud Workload Protection

We see and understand cloud changes at scale without requiring manual interventions by your team every time a new cloud service or technology is adopted. Our Cloud Workload Protection Platform (CWPP) offering runs natively in the cloud and provides continuous build to run-time threat detection, behavioral anomaly detection, and compliance across multi-cloud environments, workloads, accounts, containers, and Kubernetes.

Network on AWS

We extend our proprietary on-prem network detection capabilities into AWS for real-time deep packet inspection and response including firewall integration. Leverage behavioral-based anomaly detection and attack pattern analysis to identify and contain threats.

Cloud environments are incredibly dynamic. Most cloud threats stem from the misconfiguration and unaccounted use of the cloud platform itself. In addition, many security leaders are challenged with having the in-house resources necessary to build, optimize, and manage their multi-cloud environments without requiring continuous manual monitoring.

At eSentire, we prioritize the detection of cloud-based vulnerabilities, misconfigurations, and suspicious activity across any cloud environment – no matter where your users and data reside – so you can focus on scaling your business operations securely.

We protect your multi-cloud environments and cloud-based applications with 24/7 threat detection, investigation and response, combined with best-in-breed Cloud Security Posture Management and Cloud Workload Protection. Our cloud experts have a deep understanding of the refined tactics, techniques and procedures (TTPs) leveraged by attackers in multi-cloud environments. We provide seamless monitoring, scanning and control, delivering unmatched visibility, correlation and protection with MDR for Multi-Cloud environments across AWS, Microsoft and Google to protect your business from cloud-based threats including:



Misconfigurations



Rapidly Evolving Threat Landscape



Compliance and Legal Issues



Cloud/Hybrid Complexity



Lack of Visibility



Container Security



DevOps Security



Lack of Expertise

We Provide:

- ✓ 24/7 Cloud Visibility, Threat Detection, Investigation and Response
- ✓ 24/7 Data Correlation Across Cloud, Endpoint, Network and Log sources
- ✓ 24/7 Cloud Security Posture Management and Cloud Workload Protection
- ✓ Real-time Deep-packet Inspection of VPC Traffic in AWS and Response Action with Industry Leading Firewalls
- ✓ Managed Vulnerability Scanning Across Your Multi-Cloud Environment
- ✓ Proactive Elite Threat Hunting Expertise
- ✓ Threat Response Unit (TRU) Proprietary Novel Detections
- ✓ Deep Knowledge of TTPs Specific for Multi-Cloud Environments
- ✓ Actionable Insight and Data Correlation From Your Cloud Escalations
- ✓ Scalable, Reliable, Redundant Cloud-Native MDR Support

	How We Help	Your Outcomes
 Managed Detection And Response For Cloud	<ul style="list-style-type: none">• 24/7 threat detection mapped to MITRE ATT&CK framework• Rapid human-led threat investigations• Purpose-built detections and automated disruptions from the XDR Cloud Platform• Detection engineering from eSentire's Threat Response Unit (TRU)	<ul style="list-style-type: none">• Reduced risk of data loss and exfiltration• Improved cloud visibility and MITRE coverage• Reduced risk of security incidents across your multi-cloud environment• Improved cloud visibility and MITRE coverage• Reduced threat actor dwell time• Alleviate resource constraints• Improved cyber resilience
 Cloud Security Posture Management	<ul style="list-style-type: none">• 24/7 deep visibility and cloud control• Security rules and best practices governing and controlling your multi-cloud environment• Detect, investigate and remediate critical misconfigurations, security vulnerabilities, policy violations and Indicators of Compromise• Behavior-based anomaly detection driven via machine learning and behavioral analytics• Proactively identify and address potential security violations, prioritized by their risk profile, to limit cloud misconfigurations and reduce cyber risk• 24/7 security posture management (cloud and Kubernetes)• Map findings to popular compliance frameworks like CIS, PCI, HIPAA, SOC2, and others	<ul style="list-style-type: none">• Maximize ROI on multi-cloud environments• Enforcement of critical security rules• Cloud security program that scales• Reduced cloud knowledge gaps• Improved time to value in managing risks at the administration level of your multi-cloud environment• Rapid threat detection while reducing alert fatigue• Reduced cybersecurity incidents in your multi-cloud environment• Benchmark your cloud application configurations against industry and organizational standards• Get guardrails for your developers to avoid common misconfigurations

	How We Help	Your Outcomes
 <p>Cloud Workload Protection</p>	<ul style="list-style-type: none"> • Proactive protection of your cloud resources no matter where they reside • Detect, investigate, and remediate critical security vulnerabilities across your multi-cloud environments • Comprehensive cloud coverage • Deep integration of security signals from your cloud environments and external threat intelligence 	<ul style="list-style-type: none"> • Complete visibility into your workloads and container events • Unparalleled detection and response capability for workloads with real-time attack narratives • Prioritized risk remediation • Discover potential vulnerabilities early on in your development cycle
 <p>MDR for Network on AWS</p>	<ul style="list-style-type: none"> • Real-time agent-less deep-packet inspection of VPC traffic across AWS environments • Advanced insights and behavioral analysis • Continuous integration of the latest threat intelligence and rulesets • Proprietary global IP blocklist that is continuously updated and published to all network sensors • Detection and automated blocking of known and elusive attackers • Multi-signal visibility for stronger threat correlation and investigation 	<ul style="list-style-type: none"> • Escalated levels of response actions including email alerts, TCP Reset and integration with industry leading firewalls • All detections and response actions are mapped and stored, according to MITRE framework • Decrease threat actor dwell time • Detection and automated blocking of known and elusive attackers • Satisfaction of compliance requirements • Reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)

You're in the Cloud. We're All-in to Protect You.

Whatever the cloud brings to your business, we're all-in to keep you ahead of disruption.



Cloud Experts

Go boldly towards your business ambitions knowing our SOC Cyber Analysts and Elite Threat Hunters always have your back. Powered by our cloud-native XDR platform, multi-signal threat intelligence and unique behavior-based cloud insights we're all in to protect you 24/7.



Reduce Cloud Risks

Eliminate critical misconfiguration and runtime risks with continuous visibility, vulnerability monitoring, asset tracking, proactive threat hunting and novel detection models across AWS, Azure and Google Cloud platforms.



Proactive Threat Response

Contain cloud attacks faster, before they become business disrupting events, with automated response capabilities, deep multi-signal investigation and prioritized threat response that others simply cannot match.

Our Best-of-Breed Technology Ecosystem Approach

Our MDR for Cloud Ecosystem includes:



Simplify Multi-Cloud Security with Lacework

We are Lacework's first global Managed Detection and Response partner and are proud to provide our Cloud Workload Protection service with Lacework, expanding our deep expertise across AWS, Azure, and Google Cloud with further visibility, differentiated behavior-based threat detection and context-rich insights to fuel our multi-signal threat investigations. Through this partnership you can leverage your existing investment in the Lacework platform in a Bring Your Own License (BYOL) scenario for eSentire management, or partner with us for a completely Managed Offering.

The Lacework Polygraph® Data Platform automatically learns and understands behaviors across an organization's cloud environment using machine learning, artificial intelligence, and cloud behavioral analytics. From there, eSentire's 24/7 SOC Cyber Analysts and renowned Threat Response Unit (TRU) stop active threats before they become business disrupting events with a Mean Time to Contain of less than 15 minutes. If an automated block is not possible, we perform multi-signal investigation and prioritize threat response recommendations with informed guidance in alignment with your team.

- ✓ Rapidly identify misconfigurations with visibility across multi-cloud environments (AWS, Azure, GCP)
- ✓ Get 24/7 workload security for virtual machines, container environments and Kubernetes
- ✓ Meet compliance mandates and ensure complete attack surface protection mapped to industry compliance frameworks like PCI, HIPAA, CIS and SOC 2
- ✓ Patented machine learning and behavioral analytics automatically detect anomalies in cloud user behavior and platform API interactions
- ✓ Proactive response from our 24/7 SOC Cyber Analysts to resolve critical misconfigurations, open IPports, unauthorized modifications, and other issues that leave cloud resources exposed

Managed Detection and Response For Your Multi-Cloud Environment

We understand each cloud platform is unique and has different uses in a multi-cloud strategy. We deliver 24/7 Managed Detection and Response, Cloud Workload Protection and Cloud Security Posture Management, and across AWS, Microsoft and GCP.



MDR for AWS

We hunt and investigate threats across AWS services including but not limited to:

- AWS Simple Storage Service (S3)
- AWS Elastic Compute Cloud (EC2)
- AWS Relational Database Service (RDS)
- AWS Virtual Private Cloud (VPC)
- AWS WAF
- AWS Shield Advanced
- AWS GuardDuty
- AWS CloudTrail

We're certified as an AWS L1 MSSP.



MDR for Microsoft

We hunt and investigate threats across Microsoft Cloud services including but not limited to:

- Microsoft Sentinel
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Cloud
- Azure Active Directory
- Azure Blob Storage

We're a Microsoft Security Solutions Partner.



Google Cloud

MDR for Google

We hunt and investigate threats across Google Cloud services including but not limited to:

- GCP Cloud Storage
- GCP Compute Engine
- GCP Cloud IAM
- GCP Cloud SQL
- GCP Cloud KMS
- Google Cloud IAM
- Google Workspace Security Center

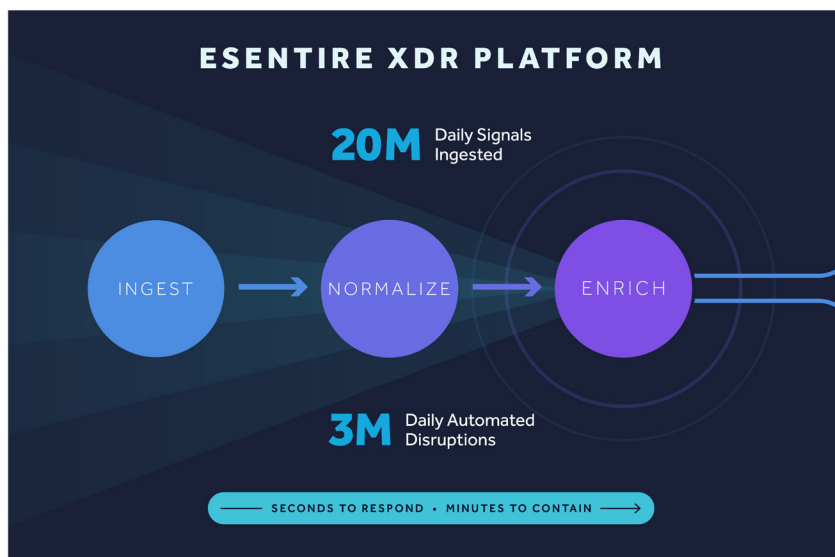
MDR Built To Scale With Your Growing Multi-Cloud Environment

The eSentire XDR Cloud Platform makes eSentire's Managed Detection and Response service possible. Patented machine learning eliminates noise, enables real-time detection and response and automatically blocks known and unknown threats. Our distributed, cloud-native platform was built to provide security, reliability, and redundancy at scale and on demand to grow with your business and cloud security needs.

MDR SIGNALS

- NETWORK
- ENDPOINT
- LOG
- CLOUD
- IDENTITY
- VULNERABILITY

ESENTIRE XDR PLATFORM



24/7 SOC

eSentire experts hunt, contain and respond to attackers.

15min Mean Time to Contain



INSIGHT PORTAL

Access investigation analysis, critical KPIs and reporting

Detection Engineering Driven By Industry Experts

eSentire's Threat Response Unit (TRU) delivers counter-threat research and proprietary content to stay ahead of attackers targeting multi-cloud environments. TRU builds proprietary detectors, and runbooks across AWS, Microsoft, and Google environments, all mapped to the MITRE ATT&CK framework. We publish original research and security advisories so you're up-to-date on the latest cyber landscape and cloud security risks.

Features

24/7 Monitoring

Human-led investigations and correlation from expert analysts in our two global Security Operations Centers (SOCs) across modern enterprise environments.

Automated Policy Enforcement

Apply over 400 integrated best-practice policies and automatically enforce them at scale across your multi-cloud environment via Cloud Security Posture Management technology.

Rapid Remediation of Cloud Threats

Experienced Cyber Analysts facilitate timely remediation of identified threats and policy violations, reducing your risk exposure.

Integrated eSentire Threat Intelligence

eSentire's curated and applied Threat Intelligence delivers near real-time protection against emerging threats observed by our SOC.

Native Cloud Infrastructure and Cloud Application Security Tool Support

Drive ROI by leveraging existing investments in tools such as Azure Security Center, AWS Guardduty, Google Workspace Security center and more for threat detection.

Multi-Cloud Infrastructure Awareness

Automatically identify and track your cloud assets and changes to your AWS, Azure and GCP environments.























eSentire in Action

	24/7 MDR With Azure Sentinel & Azure Active Directory (AD)	Threat Detection and Investigations in Google Cloud Platform (GCP)	Real-time MDR With Network on AWS
The Challenge:	Threat actors commonly try to remove important security controls like multi-factor authentication (MFA) to gain or maintain access to a user account they have targeted.	Cloud infrastructure providers like GCP provide significant geographic regional control on where their data is stored. Threat actors can use this to their advantage as a means of evading detection, by creating cloud instances in unused geographic service regions.	Many in-house security teams don't have visibility across their AWS network traffic, which means they can't monitor potential cyber threats across their full AWS environment.
Detection:	24/7 SOC Cyber Analysts are alerted via Azure Sentinel whenever MFA requirements are removed and follow a proprietary runbook to streamline the investigation process.	eSentire has a proprietary GCP detector and investigative runbook designed to regularly scan for cloud administrative activity in typically unused GCP regions and our 24/7 SOC Cyber Analysts are alerted if such activity is identified.	Through eSentire MDR for Network, we leverage native AWS traffic mirroring to perform deep packet inspection based on signature and behavior-based detections using both industry standard commercial detections and proprietary detections developed by our TRU team.
Response:	A sudden change in MFA requirements is very unusual and a potential indicator of compromise. With the right context established and the eSentire XDR platform's direct integration with Azure AD, our analyst can suspend the credentials of the user who removed the MFA policy, minimizing the risk of any other important security policies being tampered with.	Our analysts alert would alert you and confirm if the activity is expected or not. If not, SOC analysts would recommend the user's credentials be suspended, perform further investigative work to determine if any other malicious admin activities happened, and find the initial intrusion source.	Escalating levels of response are available to align with compliance and shared responsibility models. E-mail alert with instructions for your security team, TCP-RST at the VPC level, or API integration with industry leading firewalls are all available.

Why Multi-Signal MDR Matters

Our multi-signal approach ingests endpoint, network, log, cloud, asset and vulnerability data that enables complete attack surface visibility. Automated blocking capabilities built into our eSentire 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 attackers at multiple vectors and minimize the risk of business disruption.

At eSentire we recognize that the attack surface is continuously evolving and expanding. While our MDR service protects your organization from modern attackers and the vectors they target most often, we are continuously analyzing and developing new services & detections to outpace the adversaries. In our 20+ history, we pride ourselves on the fact that no eSentire client has experienced a business disrupting breach. With over 2000+ customers across 80+ countries, we don't just claim to deliver complete response. We prove it, and are proud to earn our global reputation as the Authority in Managed Detection and Response, each and every day.

	MDR Signals	Visibility	Investigation	Response
24/7 Investigation and Response	 NETWORK			
	 ENDPOINT			
	 LOG			
	 CLOUD			
Context Drivers	 INSIDER			
	 MANAGED VULNERABILITY SERVICE			

Ready to get started?

We're here to help! Submit your information and an eSentire representative will be in touch to demonstrate how eSentire Multi-Signal MDR stops threats before they disrupt your business.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US  1-866-579-2200

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit www.esentire.com and follow [@eSentire](https://twitter.com/eSentire).