Data Sheet

eSENTIRE

# 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-Native Application Protection (CNAPP)

We gain visibility into all portions of your cloud environment to implement proactive and runtime security. You can leverage configuration hardening, agentless workload protection of virtual machines and containers, and vulnerability assessment functionality. We also curtail user privileges and over-permissive cloud entitlements to keep your identities safe and secure.

### CNAPP with Runtime Monitoring

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 CNAPP offering runs natively in the cloud and provides continuous proactive and runtime threat detection, behavioral anomaly detection, and compliance across multi-cloud environments, workloads, accounts, containers, and Kubernetes.

### MDR for 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-Native Application Protection Platform. 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
- Over-Privileged Identities
- Lack of Expertise

# We Provide:

- 24/7 Cloud Visibility, Threat Detection, Investigation and Prioritized Remediation Recommendations & Support
- 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
- 24/7 Security Posture Management (Cloud and Kubernetes)
- Actionable Insight and Data Correlation From Your Cloud Escalations
- Threat Response Unit (TRU) Proprietary Novel Detections
- 24/7 Workload Security (Virtual Machines, Containers and Kubernetes)
- 24/7 Data Correlation Across Cloud, Endpoint, Network and Log Sources
- Proactive Elite Threat Hunting Expertise
- Deep Knowledge of TTPs Specific for Multi-Cloud Environments
- Scalable, Reliable, Redundant Cloud-Native MDR Support

| | How We Help | Your Outcomes |
|---|---|---|
| **24/7 Managed Detection and Response for Cloud** | • 24/7 threat detection mapped to MITRE ATT&CK framework<br>• Rapid human-led threat investigations<br>• Purpose-built detections and automated disruptions from the XDR Cloud Platform<br>• Detection engineering from eSentire's Threat Response Unit (TRU) | • Reduced risk of data loss and exfiltration<br>• Improved cloud visibility and MITRE coverage<br>• Reduced risk of security incidents across your multi-cloud environment<br>• Improved cloud visibility and MITRE coverage<br>• Reduced threat actor dwell time<br>• Alleviate resource constraints<br>• Improved cyber resilience |
| **Cloud-Native Application Protection Platform (CNAPP)** | • Comprehensive visibility into cloud workloads across multiple cloud platforms and hybrid environments<br>• 24/7 monitoring and alerting for cloud security incidents<br>• Deep integration of security signals from your cloud environments and external threat intelligence<br>• Identify and reduce over-permissioned users and unused entities<br>• Ability to analyze and identify patterns or narratives that may indicate the presence of an attack<br>• Detect, investigate, and provide remediation guidance for critical security vulnerabilities across your multi-cloud environment<br>• Centralized monitoring of workloads from a single UI/pane of glass<br>• Continuous compliance monitoring and reporting across multi-cloud environments | • Reduced multi-cloud complexity and management<br>• Enhanced protection of critical data and workloads in multi-cloud/ hybrid environments<br>• Streamlined management and security operations for workloads no matter where they are located<br>• Prioritized risk remediation guidance so you can focus resources and efforts on addressing the most critical security risks first<br>• Improved incident response and faster resolution of security threats, resulting in enhanced security effectiveness and resilience<br>• Discover potential vulnerabilities early on in your environment<br>• Better utilization of existing security tools and processes through seamless integration<br>• Maintain compliance with industry regulations and standards, reducing the risk of fines and other penalties |

| | How We Help | Your Outcomes |
|---|---|---|
| **CNAPP with Runtime Monitoring** | • Runtime monitoring of VM and containerized cloud workloads<br>• Proactive protection of your cloud resources no matter where they reside<br>• Identify and reduce over-permissioned users and unused entities<br>• Ability to analyze and identify patterns or narratives that may indicate the presence of an attack<br>• Detect, investigate, and provide remediation guidance for critical security vulnerabilities across your multi-cloud environment<br>• Comprehensive cloud coverage<br>• Deep integration of security signals from your cloud environments and external threat intelligence<br>• 24/7 monitoring and alerting for cloud security incidents<br>• Continuous compliance monitoring and reporting across multi-cloud environments | • Complete visibility into your workloads and container events<br>• Unparalleled detection and response capability for workloads with real-time attack narratives<br>• Prioritized risk remediation<br>• Discover potential vulnerabilities within your cloud environment and workloads |
| **MDR for Network on AWS** | • Real-time agent-less deep-packet inspection of VPC traffic across AWS environments<br>• Advanced insights and behavioral analysis<br>• Continuous integration of the latest threat intelligence and rulesets<br>• Proprietary global IP blocklist that is continuously updated and published to all network sensors<br>• Detection and automated blocking of known and elusive attackers<br>• Multi-signal visibility for stronger threat correlation and investigation | • Escalated levels of response actions including email alerts, TCP Reset and integration with industry leading firewalls<br>• All detections and response actions are mapped and stored, according to MITRE framework<br>• Decrease threat actor dwell time<br>• Detection and automated blocking of known and elusive attackers<br>• Satisfaction of compliance requirements<br>• 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

Simplify Multi-Cloud Security with our MDR for Cloud Ecosystem:

- Rapidly identify misconfigurations with visibility across multi-cloud environments (AWS, Azure, GCP)
- Get 24/7 workload security for virtual machines, container environments and Kubernetes
- Reduce over-permissioned users and entities to enforce least-privileged access
- Meet compliance mandates and ensure complete attack surface protection mapped to industry compliance frameworks like PCI, HIPAA, CIS and SOC 2
- Proactive response from our 24/7 SOC Cyber Analysts to resolve critical misconfigurations, open IP ports, unauthorized modifications, and other issues that leave cloud resources exposed

Through our best-of-breed partnerships you can leverage your existing investments in a Bring Your Own License (BYOL) scenario for eSentire management, or partner with us for a completely Managed Offering.

tenable

eSentire has been named Tenable's Top MSSP Partner for North America five years in a row. Tenable One's Cloud platform utilizes an identity-first approach to cloud security that understands and identifies issues with user and entity permissions assignment – one of the leading causes of cloud compromise. We also offer CSPM, CWPP, Cloud Infrastructure Entitlement Management, and vulnerability analysis capabilities to maintain visibility across your cloud environment.

CROWDSTRIKE

eSentire delivers CNAPP through CrowdStrike, enabling identity-based cloud threat detection, deep visibility for VM and container workloads, and strong context-rich insights to fuel multi-signal investigations. Customers can leverage CrowdStrike in a BYOL or co-managed scenario.

WIZ

eSentire delivers comprehensive cloud security through Wiz, spanning Wiz Essentials, Wiz Advanced, Wiz Defend, and Wiz Sensor. With agentless, log ingestion, and sensor-based runtime monitoring, our SOC analysts gain full visibility across your cloud environment — correlating risks across misconfigurations, vulnerabilities, network exposures, and identity entitlements to detect and respond to threats faster. eSentire's Wiz service is delivered as a BYOL solution.

# 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. MDR for Cloud delivers 24/7 threat detection and investigation and CNAPP across AWS, Microsoft and GCP.

aws

**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.**

Microsoft

**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 with MXDR status.**

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

# 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 Guarduty, 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.

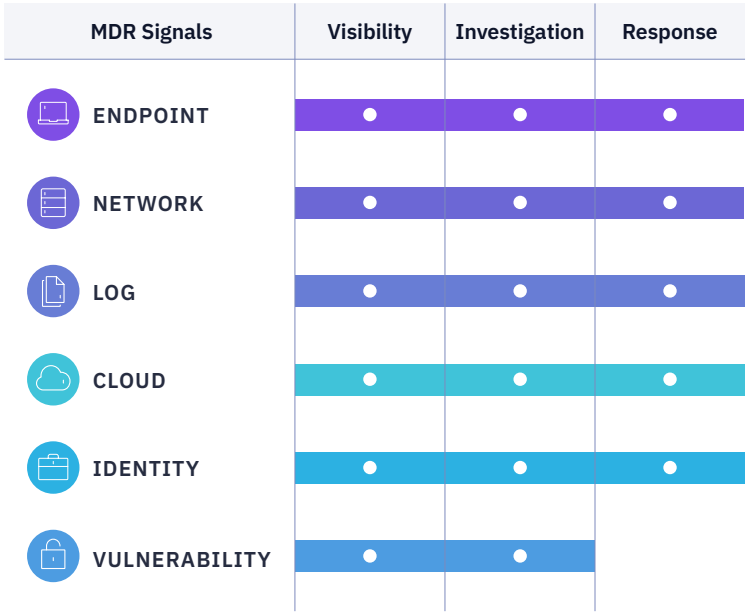
# eSentire in Action

| | 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. |

# Multi-signal MDR is Paramount for Complete Attack Surface Protection

To drive deep investigation and data correlation, analysts need visibility across a combination of sources. Our **multi-signal MDR** approach ingests endpoint, network, log, cloud, identity, and vulnerability data to enable complete attack surface visibility.

Automated blocking capabilities built into our **Atlas XDR 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 attack vectors and minimize the risk of business disruption.




## 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 Continuous Threat 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**.