Data Sheet

eSentire

eSentire Microsoft Defender for Cloud

Continuous proactive and runtime threat detection, monitoring, and remediation across multi-cloud environments, workloads, containers, and Kubernetes.

24/7 Visibility & Threat Detection

Complete visibility into workload and container runtime events enabling more accurate detection, threat hunting, investigation, and response in real-time.

Identity-based Approach

Understand and reduce over-permissioned users to reduce the blast radius of compromised identities via Microsoft Entra ID.

Seamless Integration

Protect workloads as you deploy changes rapidly — with no rip-and-replace. eSentire Atlas Platform layers directly on top of Microsoft Defender for Cloud.

High Touch Response

Our Security Operations Center (SOC) leverages AI-driven automation and human expertise to deliver 24/7 monitoring and deep contextual investigation, enrichment and response.

Your Challenges

Organizations running Microsoft Azure workloads are adopting hybrid and multi-cloud architectures, containerization, and Kubernetes at scale. This creates a complex, fast-moving environment where security teams struggle to detect, contain, and disrupt cyber threats before they cause business disruption. Security leaders are often challenged with:

- **Multi-Cloud Visibility & Coverage:** Blind spots across Azure, AWS, and GCP workloads, containers, and Kubernetes environments create undetected attack paths that Defender for Cloud alone can't close.
- **Configuration & Compliance:** Misconfigured resources, over-permissioned Entra ID identities, and dynamic cloud sprawl undermine PCI DSS, HIPAA, NIST, and GDPR posture
- **Detection-to-Response Gap:** Defender for Cloud's native alerting lacks the 24/7 investigation, managed remediation, and specialized cloud expertise needed to disrupt threats before they establish a foothold.
- **Integration Complexity:** Stitching multi-cloud telemetry into a unified, continuous response workflow requires expertise and integrations most internal teams don't have at scale

Our Solution

eSentire Microsoft Defender for Cloud continuously exposes, detects, and disrupts threats across Azure workloads, containers, and Kubernetes. Where Microsoft Defender for Cloud provides native CSPM and alerting, eSentire's Atlas Platform wraps it in a fully managed Attack Defend and Respond operating model with 24/7 expert response and adversarial validation.

Atlas integrates bidirectionally with Microsoft Defender for Cloud ingesting its signals and returning enriched threat context, validated exposures, and response actions back into your Microsoft environment. No rip-and-replace necessary so your existing Microsoft Defender for Cloud investment works harder.

How We Help

- 24/7 SOC triage and response: Comprehensive visibility and coverage on every Defender for Cloud Servers, Containers, and Storage alert.
- Adversarial Validation & Remediation: Hands-on validation of Microsoft Defender for Cloud findings — moving beyond alerting to managed response and confirmed closure.
- Identity & Compliance Posture: Continuous risk scoring via Microsoft Entra ID integration to reduce over-permissioned entities, paired with compliance monitoring across PCI DSS, HIPAA, NIST, CIS, and SOC 2.

Your Outcomes

- Reduce your multi-cloud complexity with one managed security program across your entire Microsoft and multi-cloud stack.
- Protect existing tech investments since Microsoft Defender for Cloud works harder with Atlas Platform; no rip-and-replace required.
- Prioritize your risk remediation; only reachable, exploitable findings drive action, eliminating CVSS-only noise.
- Maintain compliance with PCI DSS, HIPAA, GDPR, and NIST; reducing risk and audit burden.

The eSentire Difference

Most vendors managing Microsoft Defender for Cloud stop at log ingestion — surfacing alerts and leaving your team to act. eSentire goes one step further. CWPP alerts, agentless snapshot analysis of VMs and containers, and CSPM findings are ingested directly into the Atlas platform, where our AI investigator cross-correlates and dynamically ranks threats in the context of your environment. When a threat is confirmed, we isolate the endpoint or identity before the attacker can move.

Additional service benefits include:

- Network and process visibility for VM and containerized workloads across Azure and multi-cloud
- Rapidly identify and prioritize misconfigurations with continuous visibility across AWS, Azure, and Google Cloud via Defender for Cloud + Atlas unified posture
- Meet compliance mandates mapped to PCI DSS, HIPAA, NIST, CIS, and SOC 2 with continuous evidence generation
- Identity-based approach via Microsoft Entra ID understands permissions, unused entities, and privilege reduction opportunities
- Complete multi-signal threat investigation visibility within the eSentire Atlas Portal, combining Defender for Cloud + all connected tools
- Proactive response from our 24/7 SOC Cyber Analysts to resolve critical misconfigurations, open attack paths, unauthorized modifications, and exposed cloud resources
- Detection, investigation, and containment of threats to Azure VM workloads and containers up to 10x faster

You're in the Cloud. We're All-in to Disrupt Attackers.

Cloud Experts

Go boldly towards your business ambitions knowing our SOC 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.

Controlled Autonomy

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.

Ready to Get Started?

Connect with an eSentire Security Specialist to see Managed, Detection & Response working across your Microsoft environment.

LET'S TALK SECURITY →

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

eSentire is a leader in Controlled Autonomy SecOps, protecting 2,000+ organizations across 35+ industries around the world. Founded in 2001, the company's Controlled Autonomy SecOps operating model pairs agentic AI operatives with engineered human-judgment controls, delivering expert-depth security outcomes at machine speed without ceding accountability to opaque automation. Powered by the unified agentic AI Atlas Platform, eSentire's Atlas AI + 24/7 expert human SOC coverage delivers offensive capabilities that preempt exposures before attackers do, detect, and respond to stop threats in real time. For more information, visit **www.esentire.com** and follow **@eSentire**.