Data Sheet

eSentire | CrowdStrike

eSentire Cloud-Native Application Protection Platform (CNAPP)

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, to ensure that nothing goes unseen across your multi-cloud environment.

Identity-based Approach

Understand and reduce over permissioned users and entities to ensure a least privilege approach to cloud entitlements. Reduce the potential blast radius of compromised users and identify unused entities.

Seamless Integration

Protect your workloads as you deploy changes rapidly. This eliminates the need to compromise on performance or introduce friction, allowing you to build and deliver applications confidently.

High Touch Response

24/7 monitor plus deep investigation and contextual enrichment of security events. Our Security Operations Center (SOC) leverages AI-driven automation and human expertise to prioritize effective response recommendations.

Your Challenges

Leading organizations are increasingly adopting cloud and hybrid environments, containerization, and Kubernetes orchestration. This approach allows you to build highly scalable, agile applications that can be quickly spun up or down in response to changing demand. But as a security leader, this creates a complex and dynamic environment where your team can struggle to detect, contain, and respond to new cyber threats. As a result, many security leaders are challenged with:

- **Multi-Cloud Complexity:** As organizations increasingly adopt multi-cloud environments, managing security across different cloud providers can become complex and challenging.
- **Visibility:** A lack of visibility into cloud workloads and containers can lead to blind spots in security, making it difficult to detect and respond to threats in a timely manner.
- **Configuration Management:** Misconfigured cloud workloads and containers can create security vulnerabilities and expose sensitive data, leading to potential data breaches.
- **Compliance:** Ensuring compliance with industry regulations and standards such as PCI DSS, HIPAA, and GDPR can be challenging in cloud environments due to the dynamic and fast-paced nature of cloud workloads and containers.
- **Container Security:** Containers, while providing benefits such as portability and scalability, can also introduce new security risks such as container escape attacks, unpatched vulnerabilities, and insecure container images.

- **Identity and Access Management:** Managing identities and access in a cloud environment can be challenging, as users and applications may have varying levels of access to cloud workloads and containers. This can create security gaps and increase the risk of unauthorized access.
- **Integration:** Integrating cloud workload and container security with existing security tools and processes can be difficult, as cloud environments may have different APIs and configurations than traditional on-premises environments.
- **24/7 In-house Expertise:** Cloud security requires different foundational expertise vs on-premises or even hybrid programs, making training, communications, and resourcing top priorities.

Our Solution

eSentire's Cloud-Native Application Protection Platform (CNAPP) delivers continuous proactive and runtime threat detection, monitoring, anomaly detection, and compliance across multi-cloud environments, workloads, containers, and Kubernetes. Our approach provides a single platform solution that helps your DevOps and IT Security teams quickly develop applications while staying safe by leveraging both proactive and run-time security in their cloud environments.

Our CNAPP solution includes foundational security tooling like Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWPP), and VM/container runtime monitoring capabilities to assess the security and compliance posture of cloud-native infrastructure, workloads, and the underlying user and entity permissions. eSentire CNAPP also includes access to non-managed shift-left technologies like CI/CD pipeline integration, Infrastructure as Code security, and a myriad of vulnerability analysis options to ensure that security is integrated across your environment.

Additionally, eSentire Managed Detection and Response balances the people, platform and intelligence to deliver 24/7 protection through threat detection, threat hunting, and threat response with a Mean Time to Contain of 15 minutes. Our multi-signal approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity and vulnerability data that enables complete attack surface visibility. The eSentire Open XDR Cloud Platform identifies suspicious behavior early and prevents attackers from establishing a foothold while our expert Elite Threat Hunters can initiate human-led investigation and containment at multiple levels of the attack surface.

How We Help	Your Outcomes
✓ Comprehensive visibility into cloud workloads across multiple cloud platforms and hybrid environments	✓ Reduced multi-cloud complexity and management
✓ Agented runtime analysis of VM and containerized workloads	✓ Enhanced protection of critical data and workloads in multi-cloud or hybrid environments
✓ 24/7 monitoring and alerting for cloud security incidents	✓ Streamlined management and security operations for workloads no matter where they are located
✓ Deep integration of security signals from your cloud environments and external threat intelligence	✓ Prioritized risk remediation guidance so you can focus resources and efforts on addressing the most critical security risks first
✓ Identify and reduce over-permissioned users and unused entities	✓ Improved incident response and faster resolution of security threats, resulting in enhanced security effectiveness and resilience
✓ Ability to analyze and identify patterns or narratives that may indicate the presence of an attack	✓ Discover potential vulnerabilities early on in your development cycle
✓ Detect, investigate, and provide remediation guidance for critical security vulnerabilities across your multi-cloud environment	✓ Better utilization of existing security tools and processes through seamless integration
✓ Centralized monitoring of workloads from a single UI/ pane of glass	✓ Maintain compliance with industry regulations and standards, reducing the risk of fines and other penalties
✓ Continuous compliance monitoring and reporting across multi-cloud environments	

Simplify Multi-Cloud Security with CrowdStrike

We are proud to provide our CNAPP service with CrowdStike, expanding our deep expertise across AWS, Azure, and Google Cloud with further visibility, differentiated identity-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 CrowdStrike platform in a Bring Your Own License (BYOL) scenario for eSentire management, or partner with us for a Co-Managed Offering.

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. We perform multi-signal investigation and prioritize threat response recommendations with informed guidance in alignment with your team.

Additional service benefits include:

- Network and process visibility for VM and containerized workloads
- Rapidly identify and prioritize misconfigurations with visibility across multi-cloud environments (AWS, Azure, Google Cloud)
- Meet compliance mandates and ensure complete attack surface protection mapped to industry compliance frameworks like PCI DSS, HIPAA, CIS, and SOC 2
- Identity-based approach to cloud security understands permissions, where they're leveraged, and how they can be reduced
- Complete multi-signal threat investigation visibility within the eSentire Atlas User Experience
- 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
- Detection, investigation, and containment of threats to virtual machine (VM) workloads and containers up to 10x faster
- A 342% return on investment, 100:1 alert reduction, and 80% faster investigation capability

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.

Ready to Get Started?

We're here to help! Connect with an eSentire Security Specialist to learn how we can help you build a more resilience security operation and prevent disruption.

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**.