SOLUTION BRIEF

eSentire MDR for Cloud for DevOps Security

Integrate security into your CI/CD pipelines to ensure security, compliance, and automation of cloud workloads and infrastructure and enhance cyber resilience.

The primary goal of the DevOps methodology is to streamline software development and delivery. However, the pressure to meet tight deadlines often leads to compromises on security measures which, in turn, compromises the ability to effectively protect cloud workloads from potential security gaps and vulnerabilities.

When implementing DevOps practices, IT Security teams must grapple with a unique set of challenges, such as:

- **Integration of Security Processes in CI/CD Process:** Integrating cybersecurity seamlessly into the CI/CD process requires the implementation of secure development practices at every pipeline stage to include code reviews, vulnerability scanning, and security testing.
- **Container Vulnerabilities and Orchestration Risks:** Containers have become an essential part of modern DevOps workflows, but they can introduce security risks if not properly managed. Vulnerabilities in container images or misconfigurations in container orchestration platforms like Kubernetes can lead to data breaches or unauthorized access.
- **Management of Credentials and Access Controls:** Effectively managing sensitive credentials and access controls is essential for preventing unauthorized access to production environments and maintaining the security of cloud workloads.
- **Visibility and Control over the CI/CD Pipeline:** Maintaining visibility and control over the entire CI/CD pipeline is crucial, involving monitoring and auditing security compliance to swiftly detect and respond to any security incidents or vulnerabilities during deployment.
- **Balancing Speed and Security:** DevOps teams must find a balance between speed and security, as the pressure to deliver software updates rapidly can sometimes compromise security measures, potentially leading to security gaps, misconfigurations, vulnerabilities, or policy violations in deployed cloud workloads.

Introducing eSentire MDR for Cloud

At eSentire, we protect your multi-cloud environments and cloud-based applications with 24/7 threat detection, investigation, and response, combined with best-of-breed Cloud Security Posture Management and Cloud Workload Protection. 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 DevOps securely.

eSentire MDR for Cloud enhances cloud security, increases efficiency and productivity, improves threat detection and response, with streamlined compliance management, and actionable insights and reporting. These outcomes support your team in achieving a robust and secure cloud infrastructure while enabling you to focus on delivering high-quality software applications.

How We Help	Your Outcomes
Enhanced Container Security	✓ Identifies vulnerabilities in container images ✓ Ensures continuous security for DevOps, cloud security, and IT operations teams
Strengthened Software Development and Deployment	✓ Integrates container image assessment into CI/CD pipeline ✓ Minimizes the risk of deploying insecure container images ✓ Enhances overall software development and deployment security
Improved Cloud Environment Security	✓ Automatically scans and hardens cloud-based infrastructure through IaC Security ✓ Reduces potential misconfigurations and vulnerabilities
Enhanced Kubernetes Cluster Security	✓ Enables comprehensive audit logging for Kubernetes clusters ✓ Enhances cluster security ✓ Ensures compliance adherence ✓ Early detection of security threats and anomalous behaviors
Safeguarded File and Directory Integrity	✓ Implements File Integrity Monitoring (FIM) ✓ Protects critical file and directory integrity ✓ Detects and reports unauthorized modifications promptly ✓ Prevents potential security breaches
Effective Detection and Response to Advanced Threats	✓ Provides advanced threat detection capabilities ✓ Identifies anomalous activities and indicators of compromise ✓ Offers expert guidance for incident mitigation ✓ Minimizes risk of future attacks
Enhanced Cyber Resilience	✓ Embeds security into every stage of the development process ✓ Promotes early vulnerability detection ✓ Enables continuous monitoring and improvement ✓ Facilitates well-prepared incident response
Comprehensive Visibility and Informed Decision-Making	✓ Access to a unified dashboard for comprehensive security posture visibility ✓ Provides detailed reports, threat intelligence, and compliance audits ✓ Empowers informed decision-making and compliance adherence

How eSentire MDR for Cloud Proactively Protects Your Organization

Organizations building their applications using containerization technology / Kubernetes require security tools to protect those surface areas. eSentire provides complete Shift Left Security for IaC templates and container images from a single platform, ensuring that vulnerabilities, secrets, and misconfigurations are detected as early as possible.

By partnering with eSentire, you can leverage our specialized expertise, advanced technology, and comprehensive services to integrate robust security practices into your cloud workload, enhancing cyber resilience and mitigating potential security risks from build to runtime.

Features:

Container Vulnerability Assessment: Secure containerized applications by identifying vulnerabilities within container images, empowering DevOps, cloud security, and IT operations teams to maintain continuous security.

Container Image Assessment via CI/CD Pipeline Integration: Strengthen the software development and deployment process by integrating container image assessment, minimizing the risk of deploying insecure container images, and enhancing overall security.

Infrastructure as Code Security (IaC): Improve cloud environment security by automatically scanning and hardening infrastructure through analyzing automation templates, reducing potential misconfigurations and vulnerabilities.

K8s Audit Logging: Enhance Kubernetes cluster security by enabling comprehensive audit logging, enabling compliance adherence, and providing early detection of potential security threats or anomalous behaviors.

File Integrity Monitoring (FIM): Safeguard the integrity of critical files and directories by implementing file integrity monitoring, enabling the prompt detection, and reporting of unauthorized modifications, thus preventing potential security breaches.

Advanced Threat Detection and Response Guidance: Strengthen your security posture by effectively detecting and responding to advanced threats, with expert guidance on mitigating current incidents and minimizing the risk of future attacks.

Comprehensive Visibility and Detailed Reporting: Enhance your understanding of cloud security by accessing comprehensive and detailed reports, enabling informed decision-making, and facilitating compliance adherence.

Ready to get started?

We're here to help! Submit your information and an eSentire representative will be in touch to help you build a more resilient cloud security operation today.

CONTACT US

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

eSENTIRE