

EVIDEN

Protect your AWS deployments with managed security services

Cyberthreats are increasing in both volume and sophistication every day. Protect your AWS deployments with AWS Native Security from Eviden.



Keep your cloud deployments safe under one umbrella with AWS Native Security from Eviden

New technologies create new vulnerabilities. As companies reach for business-enabling breakthroughs in AI, machine learning, data analytics, edge capabilities, and more, they must be aware of the emerging security trends that are accompanying these opportunities: In addition to protection from rapidly evolving malicious actors, today's organizations need data sovereignty, skilled talent, and protection for their hybrid and edge deployments.

Achieving these imperatives is a big job for today's IT departments. Modern infrastructures are complex, with dozens of disparate security tools to manage. Moving to the cloud – a transition most organizations are embracing – complicates things further. A managed security service provider (MSSP) can make all the difference. And for AWS deployments, there's no better MSSP partner than AWS Native Security from Eviden, the No. 1 worldwide MSSP by revenue as ranked by Gartner in 2022.

Addressing the cloud security gap with AWS Native Security from Eviden

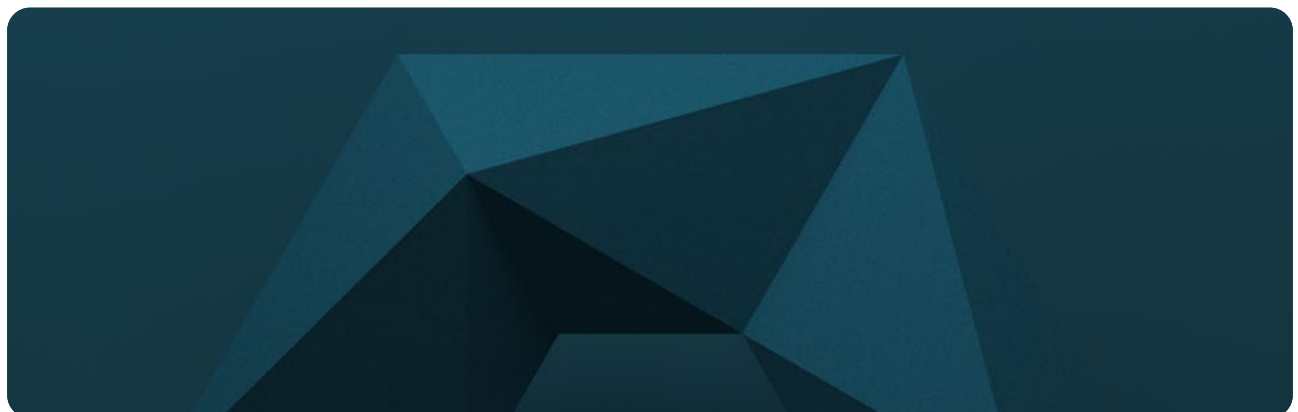
Although AWS manages the security of its cloud, the security of your deployments in the AWS cloud is your responsibility. As you expand your environment into the cloud to innovate and grow your business, you'll begin to collect multiple disparate security tools, creating a disjointed security posture – a situation ripe for misconfigurations that leave you open to compromise. Your IT department must establish a unified approach to security, but they're hampered by lack of visibility across your threat landscape and the complexity of tools that don't work together. Additionally, regulatory and compliance requirements in the cloud are fundamentally different than they were in your on-premises environment. And the burdens of these requirements across different countries and regions can be overwhelming.

Emerging cloud security trends highlighted by cloud leaders in a 2023 article in Eviden Digital Security Magazine add further complexity. Data sovereignty concerns are driving technological changes in data encryption and key management. The shortage of tech talent is driving an increased reliance on automation and machine learning. And operational technology breakthroughs are expanding the frontier of data protection farther than ever before.

With more data to protect, and more places in which to protect it, IT departments are stretched to their limit. That's why companies are increasingly turning to MSSPs to bridge the security gap and provide comprehensive security coverage for their cloud deployments. For AWS deployments, AWS Native Security from Eviden is uniquely positioned to deliver end-to-end security across AWS environments so that security teams can visualize, filter, and prioritize threat information with unified visibility.

AWS Native Security from Eviden is built around the native services that AWS brings to its customers to enhance their security, many of which were designed in collaboration with Eviden. Our partnership with AWS and the technical integration of our service with AWS has gained us an AWS Level 1 MSSP Competency status. By working closely with AWS, we keep pace with potential security misconfigurations, threats, or unexpected behaviors, so you can quickly respond to potentially unauthorized or malicious activity occurring within your environment. AWS Native Security from Eviden provides the latest in data sovereignty solutions, and we even provide services to review our customers' processes, train their people, and provide support to keep their data secure – wherever in the world it resides.

AWS Native Security from Eviden: unified visibility under one umbrella.

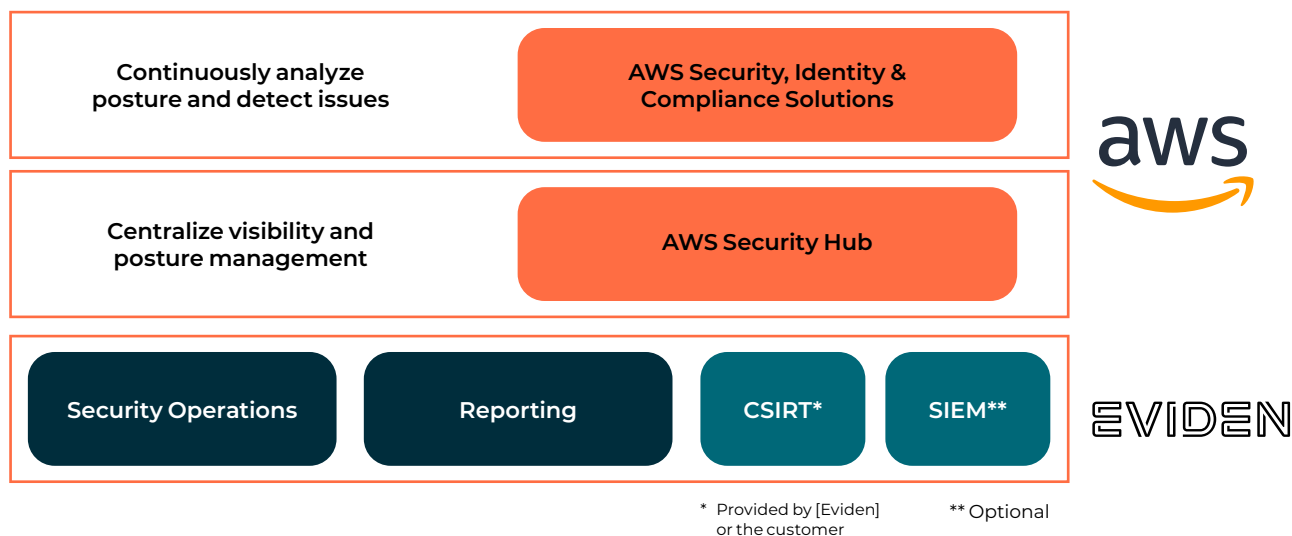


Complete coverage under one umbrella: Here's how it works

AWS Native Security from Eviden uses AWS native security tools for security posture, threat detection, and compliance. Data from these tools is sent to AWS Security Hub, which provides unified visibility and makes the data actionable. Eviden further enhances these capabilities

by adding security operations center (SOC) capabilities, reporting, and a computer security incident response team (CSIRT). Customers also have the option to add security information and event management (SIEM) and managed detection and response (MDR).

AWS Native Security from [Eviden]

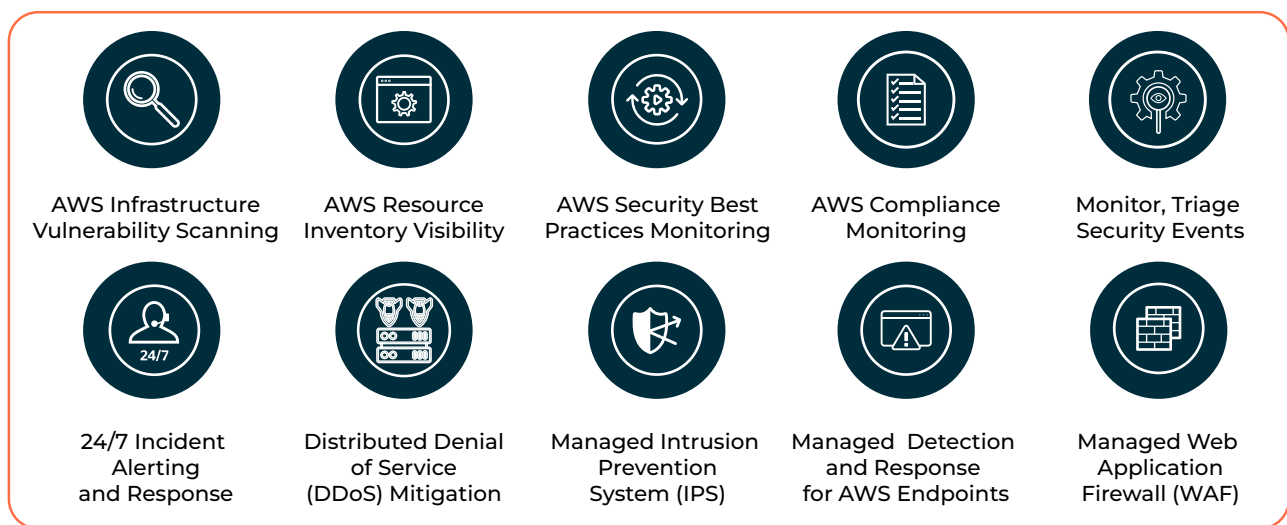


Core services from AWS, seamlessly delivered by Eviden

AWS Native Security from Eviden accelerates your journey to AWS by delivering security confidence via direct integrations with key AWS security services:

- AWS Infrastructure Vulnerability Scanning.** This service performs an automatic scan of AWS infrastructure resources for vulnerabilities, including assessment of configuration and policies applied against identity and access management (IAM). It also analyzes IAM resource policies according to AWS and Eviden joint security best practices and the principle of least privileged access, helping redefine permissions for a higher level of security assurance by using AWS IAM Access Analyzer configuration.
- AWS Resource Inventory Visibility.** This service continuously scans and reports on all AWS resources and their configuration details. IAM Security Controls provide assessment of IAM configuration status based on AWS security best practices.
- AWS Security Best Practices Monitoring.** This service detects when AWS accounts and the configuration of deployed resources do not align to security best practices.
- AWS Compliance Monitoring.** Our Configuration Compliance service allows us to assess, audit, and evaluate the configurations of the AWS resources based on existing template or custom rules, using AWS native security services. We design, implement and maintain configuration rules according to your needs and map your AWS resources to support operational best practices including those from CIS, NIST, PCI DSS, FEDRAMP and many more.
- Monitoring and Triage of Security Events.** We use Amazon GuardDuty to provide threat detection by continuously monitoring for malicious activity and unauthorized behavior. The service aggregates security alerts and findings from various AWS services in a standardized format. The solution can be combined with our MDR platform, Alsaac, which supports Amazon Security Lake and Open Cybersecurity Schema Framework (OCSF) formatted virtual private cloud (VPC) logs and utilizes AI models for detecting threats. With this service, you can understand your overall security posture, with AWS Security Hub integrating multiple tools and services – including threat detection from Amazon GuardDuty, vulnerabilities from Amazon Inspector, sensitive data classifications from Amazon Macie, and resource configuration issues from AWS Config.

- **24/7 Incident Alerting and Response.** This service generates standard reports that include the security status of each AWS account. The service's threat detection provides continuous threat monitoring and alerting. Amazon GuardDuty continuously monitors and analyzes your AWS account and workload event data in AWS CloudTrail, VPC Flow Logs, and domain name service (DNS) logs. This service also provides design and implementation of Amazon GuardDuty and remediation strategy.
- **Distributed Denial of Service (DDoS) Mitigation.** A system backed by technology and security experts monitors 24/7 for DDoS attacks against your AWS applications.
- **Managed Intrusion Prevention System (IPS).** This service protects your environment from known and emerging network threats that seek to exploit known vulnerabilities.
- **Managed Detection and Response (MDR) for AWS Endpoints.** Eviden's MDR service provides advanced threat defense by proactively hunting, validating, containing, and responding to current threats. It is built on the Alsaac platform, which performs continuous analysis of an organization's data to detect attacks in real time and near-real time. The MDR service also integrates endpoint detection and response (EDR) solutions from partners, providing superior protection against endpoint threats. This service combines monitoring of endpoints and collection of relevant data with analytics techniques to identify breaches and automated response capabilities to those attacks, making it a managed endpoint detection and response (M-EDR) service.
- **Managed Web Application Firewall (WAF).** This service provides a firewall managed system designed to protect web-facing applications and APIs against common exploits.



Pulling it all together under a resilient, reliable umbrella: The Eviden difference

There's a reason why Eviden was the No. 1 global MSSP by revenue in 2022. AWS Native Security from Eviden offers the most comprehensive approach to security analytics in the cloud, leveraging our unique partnership with AWS to ensure that your workloads and data are secure – wherever they are.

With AWS Native Security from Eviden, you gain:

- **A consolidated security view based on AWS Security Hub.** Security Hub gives you unified visibility while aggregating, organizing, and prioritizing your security alerts and findings from multiple AWS services, as well as from AWS partner solutions, to give you a comprehensive view of security alerts and compliance status reports.
- **An audit of flow logs.** By using **VPC Flow Logs**, the solution performs continuous security analysis for log auditing, with alerts sent to the responsible administration group at Eviden or to the customer.
- **Configuration compliance based on AWS Config.** Address your compliance concerns by tracking the configuration of resources within an AWS account based on a set of rules.
- **Security assessment based on Amazon Inspector.** Your security assessment findings are prioritized by severity level, with Eviden security experts available to recommend appropriate mitigation actions.
- **Alerting and reporting.** You receive standard reports that include the security status of each AWS account. Eviden experts can provide recommendations on the type of alarms, metrics, and reports to be generated depending on your need, with guidance to help reduce alert fatigue.
- **Threat detection based on Amazon GuardDuty.** Our threat detection continuously monitors for malicious activity and unauthorized behavior and supports automated threat response. Results can be stored for 90 days, or longer if required.
- **IAM Security Controls based on IAM Access Analyzer.** When identifying the resources that are shared with an external entity, you can review this service's findings to determine whether access is allowed or whether it is unintended and a security risk.
- **Eviden SOC.** This service relies on several tools for security monitoring: **AWS Security Hub, AWS CloudWatch, AWS Secure Data Lakes, and Amazon Simple Notification Service (SNS).**

Customers also have the option of adding CSIRT capabilities from Eviden, if they do not have these capabilities in-house:

- **CSIRT.** CSIRT integration enhances the AWS Foundation security incident response and remediation service capabilities. With CSIRT, you can:



Identify a suspicious activity in one or more resources.



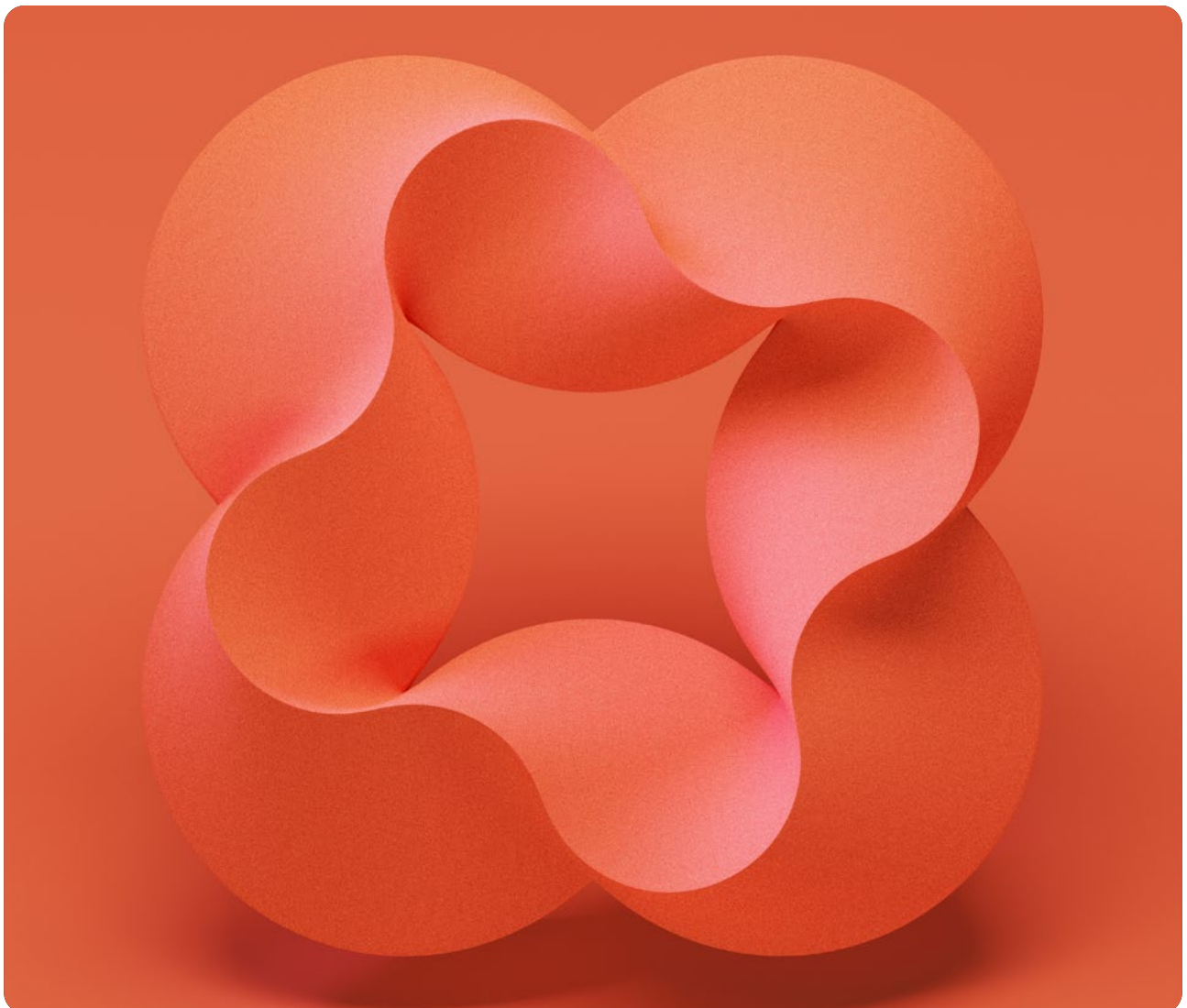
Perform an initial assessment to obtain more information about the suspicious activity.



Use the remediation steps to conduct the technical procedure to address the issue.






In addition to these baseline modules, customers can add one of two optional modules:

- **Eviden SIEM integration.** SIEM integration provides a means for normalized log export from the AWS Native Security from Eviden solution and ingestion with provided SIEM. This integration can improve visibility and anomaly detection that may indicate a misconfiguration or a security issue (such as zero-day vulnerabilities). SIEM also provides the routing, escalation, and management of events or findings.
- **Third-party ticketing integration.** This option allows you to integrate with ServiceNow (the customer's or Eviden' instance), providing incident or ticket creation based on findings raised by other service modules.



Eviden and AWS: Working together to provide resilient security protection for your AWS deployments

We've built our partnership with one goal in mind: To provide advanced security protection in the cloud for our customers. Together, we bring market-leading technology, a deep understanding of legacy infrastructure, and the experience to de-risk cloud migration. With Eviden and AWS, you can:




 <p>Optimize your investment in the AWS cloud.</p>	 <p>Maintain an effective cloud security posture in a continuous process, with a 24/7 fully managed service that is flexible enough to be utilized for either supplementing internal security staff or outsourcing.</p>
 <p>Benefit from our extensive cloud and cybersecurity expertise.</p>	 <p>Reduce alert fatigue for in-house security teams by using Eviden security automation to reduce workloads.</p>
 <p>Enhance the maturity of your security processes, including monitoring, responding, and mitigating threats.</p>	


When it comes to security operations, the unique combination of AWS native technology and Eviden cloud security expertise makes AWS Native Security from Eviden a clear choice for delivering end-to-end security across your AWS environments.

Watch AWS Native Security from Eviden in action: Use cases

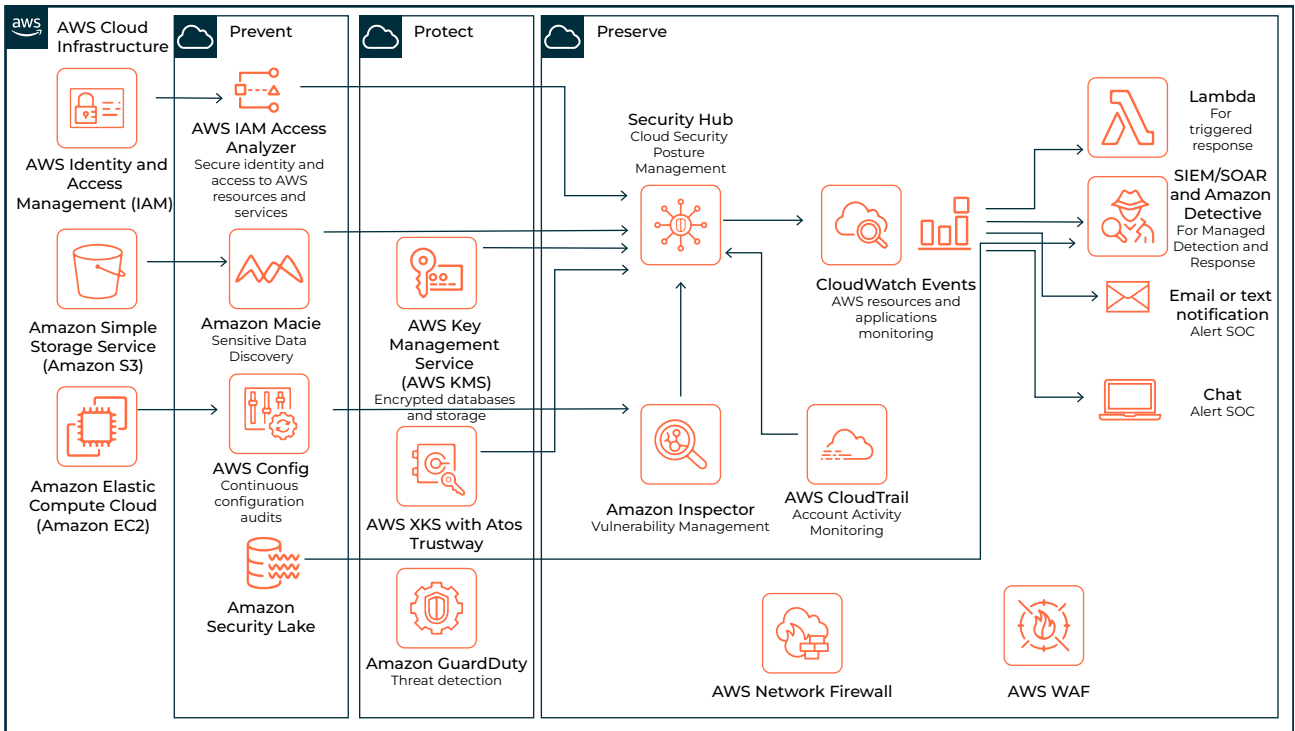
With our Prevent, Protect, and Preserve approach, Eviden ensures security in the cloud with AWS at every step of your cloud transformation journey. By leveraging the native security capabilities of AWS along with our own industry-leading best practices, we provide the peace of mind and security your business deserves. As a recognized AWS Well-Architected and Security Competency partner, we bring our expertise to every aspect of your cloud security, ensuring that your business operates with the highest level of security and agility in response to potential threats.

The following security use cases are real-world examples we can help you with. These use cases demonstrate the value that AWS Native Security and Eviden managed security services can bring to your organization.

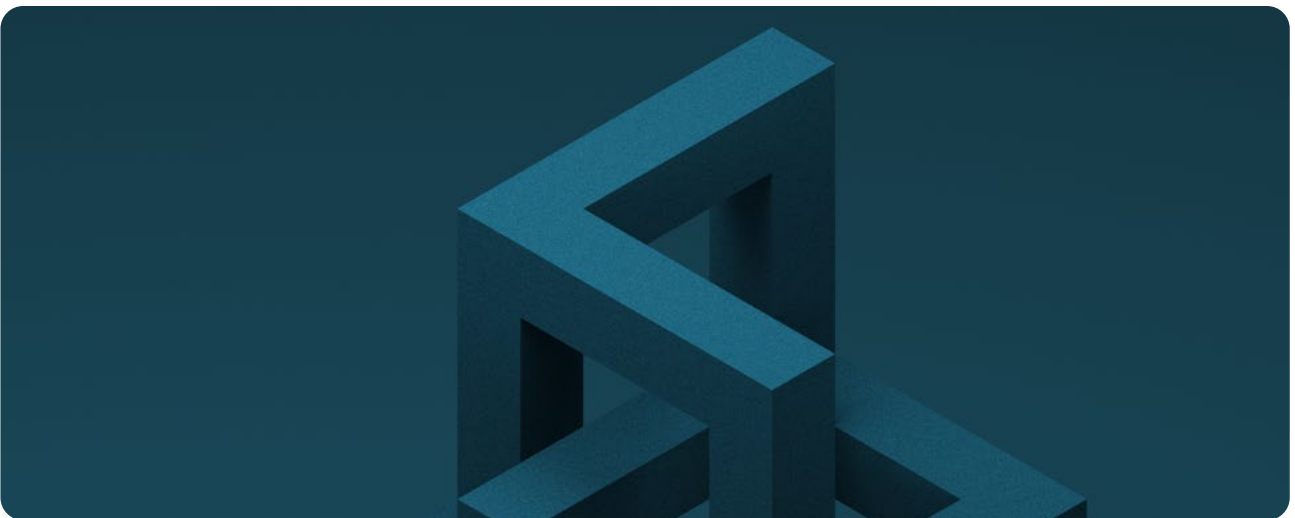
Use case	 Prevent	 Protect	 Preserve
Situation	You want to prevent misconfigurations from happening in your AWS cloud infrastructure.	You need to dynamically detect threats and protect your cloud assets.	Your hybrid and multi-cloud context requires you to preserve your security posture at all times.

Use case	 Prevent	 Protect	 Preserve
Our approach	<p>Proactively deploy security controls that ensure your cloud architecture is secure by design, in order to minimize your exposure to security risks and embed a culture of security by design.</p> <p>Use case:</p> <p>For organizations planning to migrate their workloads to the AWS cloud but that want to ensure that their cloud architecture is designed with security in mind.</p> <p>To achieve this goal, the organization follows a security strategy that:</p> <ol style="list-style-type: none"> 1. Identifies the security and compliance requirements associated with cloud workloads and data being processed. 2. Establishes security standards and procedures that safeguard data confidentiality, availability, and integrity. 3. Implements best practices throughout the development process in order to shift left security. 4. Deploys security architecture with secure landing zones that follow Well Architected standards. 	<p>Dynamically augment security controls with automation in order to protect against unknown threats, detect threats as they happen, and safeguard your identity and data assets within the AWS cloud environment.</p> <p>Use case:</p> <p>For organizations that have deployed their workloads into AWS and want to ensure that their cloud infrastructure is protected against potential security threats.</p> <p>To achieve this goal, the organization follows a security plan that:</p> <ol style="list-style-type: none"> 1. Deploys security controls such as workload protection to protect against threats. 2. Detects threats as they happen in real time. 3. Creates security policies that provide the appropriate levels of access, permissions, and protection for cloud resources. 4. Enables advanced threat protection for cloud apps and APIs to understand sophisticated threats. 5. Enables private services isolation from public-facing websites and data. 	<p>Continuously monitor, detect, and respond to evolving threats in order to preserve a secure posture across all your cloud environments.</p> <p>Use case:</p> <p>For organizations that have migrated or modernized workloads to AWS cloud and want to ensure that their data remains secure at all times by continuously assessing their security posture and response to threats.</p> <p>To achieve this goal, the organization follows a continuous monitoring and management approach that:</p> <ol style="list-style-type: none"> 1. Deploys posture analysis and monitoring across the cloud stack to understand in real time the current state and any deviations. 2. Anticipates and responds to evolving threats by adjusting your posture accordingly. 3. Turns learning into action by improving preventative and protective measures. 4. Automates continuous compliance that dynamically resolves policy violations and misconfigurations.

AWS provides built-in security features for cloud infrastructure to assist organizations in meeting their specific security requirements. This includes a wide range of security tools and features spanning network security, access control, configuration management, and data encryption.



Eviden offers managed security services that utilize and configure AWS's native security tools for improving security posture, threat detection, and compliance assurance. Eviden enhances these capabilities by providing SOC, reporting, CSIRT, SIEM, and MDR services through Eviden Alsaac. All AWS telemetry data is sent to Eviden's MDR service, which is staffed 24/7 by global security professionals in Eviden's 16 SOCs. This service is designed to prevent misconfigurations and protect and preserve your security posture across identity, data, network, and endpoints.



About AWS

Since 2006, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud. AWS has been continually expanding its services to support virtually any workload, and it now has more than 200 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 99 Availability Zones within 31 geographic regions, with announced plans for 15 more Availability Zones and five more AWS Regions in Canada, Israel, Malaysia, New Zealand, and Thailand. Millions of customers – including the fastest-growing startups, largest enterprises, and leading government agencies – trust AWS to power their infrastructure, become more agile, and lower costs. To learn more about AWS, visit aws.amazon.com.

Connect with us



eviden.com

Eviden is a registered trademark of BULL SAS. © Copyright 2023, BULL SAS. Confidential information owned by BULL SAS, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from BULL SAS.

ECT-230329-JR-BR-AWS + EVIDEN SECURITY