
AWS Native Security from Atos

Protect your AWS deployments with
managed security services

Trusted partner for your Digital Journey



Protect your AWS deployments with managed security services

As companies are embracing cloud and mobile computing opportunities, remote workforce and automatized operations bring new risks. One of the biggest challenges of digital transformation is ensuring security across the entire digital landscape in order to help customers secure their environment by using AWS engineered dedicated security tools.

However, cloud security is a shared responsibility model: while AWS manages the security of the cloud, security in the cloud is the responsibility of the customer. In this context, misconfigurations are a primary vector for cloud resources to be compromised. AWS Native Security from Atos service is built around the native services that AWS brings to its customers to enhance their security.

AWS layered approach for security in the Cloud

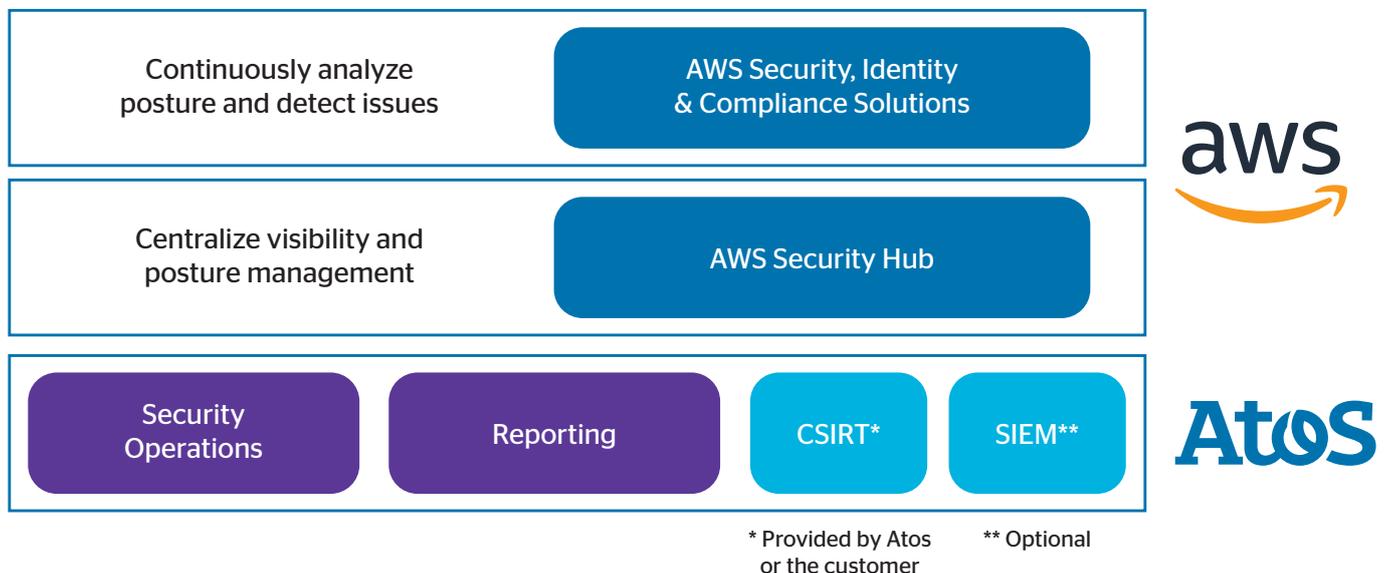
AWS security services can be mapped across 3 main stages to deploy a Cloud business:



Atos is combining all these native tools with Atos Cloud security expertise to provide an end-to-end security service.

AWS Native Security from Atos: trust through a single pane of glass.

AWS Native Security from Atos



AWS Native Security from Atos service uses AWS native security tools for security posture, threat detection and compliance. Data from these tools is sent to AWS Security Hub, providing a single pane of glass and making the data actionable. Atos further enhances these capabilities by adding SOC, reporting, Computer Security Incident Response Team (CSIRT) and optionally Security Information and Event Management (SIEM) and Managed Detection and Response (MDR) through Atos Alsaac.

Organizations can fully outsource their AWS security monitoring/response or hire an AWS MSSP to augment their own internal security staff.

The main functionalities covered by the AWS Native Security from Atos service are:

- **Consolidated security view** based on **Security Hub**: With Security Hub, you have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, as well as from AWS Partner solutions to give you a comprehensive view of security alerts and compliance status.
- **Flow logs Audit**: Security analysis will be continuously performed based on **VPC Flow Logs** for log auditing. Alerts are sent to the responsible administration group at Atos or Customer.
- **Configuration Compliance** based on **AWS Config**: it tracks the configuration of resources within an AWS account based on a set of Rules to check security compliance.
- **Security Assessment** based on **Amazon Inspector**: the assessment findings are prioritized by severity level and Atos security experts will recommend appropriate mitigation actions.
- **Alerting and reporting**: Standard reports are generated that include the security status of each AWS account. Atos experts can provide recommendations with regards to type of alarms, metrics, and reports to be generated depending on customers need and will help reduce alert fatigue.
- **Threat Detection** based on **GuardDuty**: It continuously monitors for malicious activity and unauthorized behaviour. It also supports automated threat response and results can be stored for 90 days or longer if required.
- **IAM Security Controls**: To identify the resources that are shared with an external entity. You can review the findings to determine whether the access is allowed or that it is unintended and a security risk. The key principle here is ensuring that users have appropriate levels of permissions to access the resources they need, but no more than that. **IAM Analyser, IAM**.
- Atos SOC. When it comes to Security Monitoring, several tools are supporting: **AWS Security Hub, Cloud Watch** and **Amazon Simple Notification Service (SNS)**.

Provided by Atos or the customer:

- **CSIRT**: CSIRT integration enhances the AWS Foundation security incident response and remediation service capabilities:
 - Identify a suspicious activity in one or more resources
 - Perform the initial assessment to obtain more information about the suspicious activity
 - Use the remediation steps to conduct the technical procedure to address the issue.

On top of these mandatory modules there are three optional modules:

- **Atos SIEM integration**: SIEM integration provides a means for normalized log export from the AWS Native Security from Atos solution and ingestion with provided SIEM. To improve visibility and anomaly detection that may indicate a misconfiguration or a security issue (e.g. zero-day vulnerabilities). SIEM also allows to route, escalate, and manage events or findings.
- **3rd party ticketing integration**: option to integrate with ServiceNow (Customer or Atos instance), providing incident or ticket creation based on findings raised by other service modules.



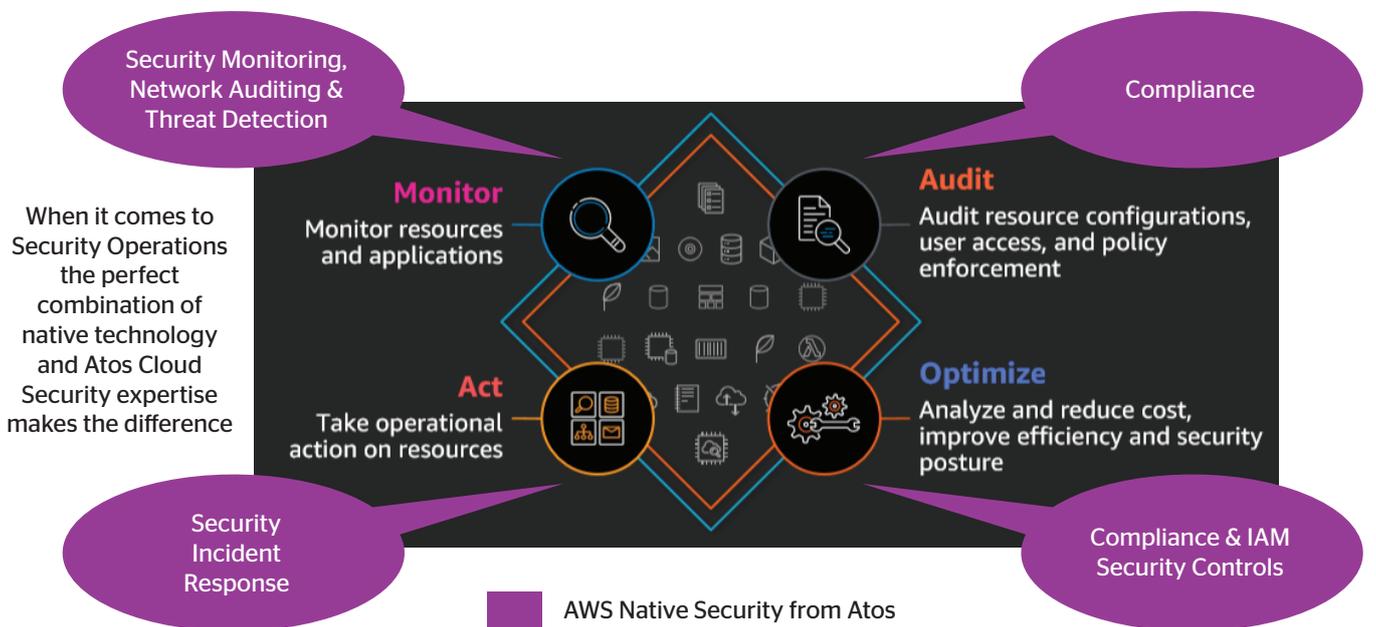
Why choose Atos MDR Services?

The Atos Managed Detection and Response (MDR) is built on the power of AI, big data analytics, and high-performance computing to bring you multi-vector threat detection and full-service response at remarkable speeds.

You get the power of 15 next-generation SOCs that are dedicated to preventing breaches on public, hybrid, and private clouds by proactively hunting, containing, and responding to threats.

Atos & AWS: bringing greater combined value

The combined Atos and AWS proposition bring value on the following aspects:



Source: AWS

Atos extends these native security capabilities with proper cloud security skills to cover all security areas.

With regards to security monitoring, network auditing and threat detection, Amazon Guard Duty native service is used to monitor event sources such as VPC flow logs, DNS logs and CloudTrail events that can be monitored in Cloud Watch. The security hub delivers continuous security checks based on industry standards and best practices such as GDPR, NIST, SOC2, and PCI. These checks provide a security score and help identify specific accounts and resources that require attention.

Additional Atos CSIRT service and optional Atos SIEM that can help identifying the root cause of a security incidents and mitigating the impact. The Atos SOC team will use it as well, taking advantage of both the correlation capabilities and long-term storage of the raw data in order to make easier the enrichment of the potential security incidents detected.

For compliance, AWS Config native tool is used to assess, audit, and evaluate the configuration of AWS resources. To complement this, Atos Cloud security experts process profile recommendations to the organization regarding the proper security policy and metrics to consider and adjust to be automated and identified by the native tools.

Atos and AWS 10 joint managed security services

 	 	 	 
AWS Infrastructure Vulnerability Scanning	AWS Resource Inventory Visibility	AWS Security Best Practices Monitoring	AWS Compliance Monitoring
 	 	 	 
Monitor, Triage Security Events	24/7 Incident Alerting and Response	Distributed Denial of Service (DDoS) Mitigation	Managed Intrusion Prevention System (IPS)
 	 		
Managed Detection and Response for AWS Endpoints	Managed Web Application Firewall (WAF)		

AWS Native Security from Atos: for which use cases?

These use cases are met with Atos MSS for AWS 24/7:

Use case	 Configuration compliance	 Security Assessment	 Threat Detection	 Excessive privileges
Situation	Your organization is using multiple AWS resources and is concerned about the compliance of its infrastructure in AWS.	Your organization has multiple applications deployed on AWS but is concerned about security vulnerabilities and following best practice.	Your organization has multiple workloads in AWS and is concerned about not being able to see all security events related to them.	Your organization is concerned that its identity and access management policies in AWS are not aligning to best practices and the principle of least privilege.
Solution	Atos experts leverage AWS Config to continuously audit and assess the overall compliance of your AWS resource configurations against your organizations policies and guidelines.	Atos experts combine AWS Inspector automated security assessment capabilities to detect vulnerabilities and deviations from best practice with prioritization of findings to improve the security and compliance of applications deployed on AWS.	Atos experts combine the power of AWS GuardDuty with its continuously behavior monitoring capabilities, with Atos cybersecurity expert analysis of your AWS account and workload event data to detect and alert on relevant findings related to potential security threats.	Atos experts leverage AWS IAM Access Analyzer to check resource policies are deployed according to security best practices such as principle of least privileged in order to improve overall security posture.

Accelerate modernization and transformation

Atos **Digital Cloud Services**, supporting AWS, can complement the security approach by offering a smart way to transform your business, increasing speed of innovation to create new applications and enhancing competitive advantage with customized and bespoke service patterns to address individual business challenges.

Atos Digital Cloud Services harnesses the native security capabilities of the public cloud and offers Atos security services to enhance the security and governance of the customers' complete cloud stack.

Why Atos and AWS

Thanks to its strong partnership with AWS, Atos can help customers capitalize on their investment into the AWS cloud and can support customers in several ways:

- Benefit from a cloud and cybersecurity expertise.
- Enhance security processes maturity, including monitoring, responding, and mitigating threats.
- Cover the entire security landscape beyond AWS, especially for organizations that have multiple cloud environments from different vendors.
- Maintain an effective cloud security posture in a continuous process, with a 24/7 fully managed service and flexible to be utilized for either supplementing internal security staff or outsourcing.
- Reduce alert fatigue for in-house security teams by using Atos security automation to reduce workload.



About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos operates under the brands Atos and Atos|Syntel. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us

atos.net

atos.net/career

atos.net/en/solutions/cyber-security/aws-managed-security-services

Let's start a discussion together

