Cloud Catalyst

Securing cloud data for major enterprises

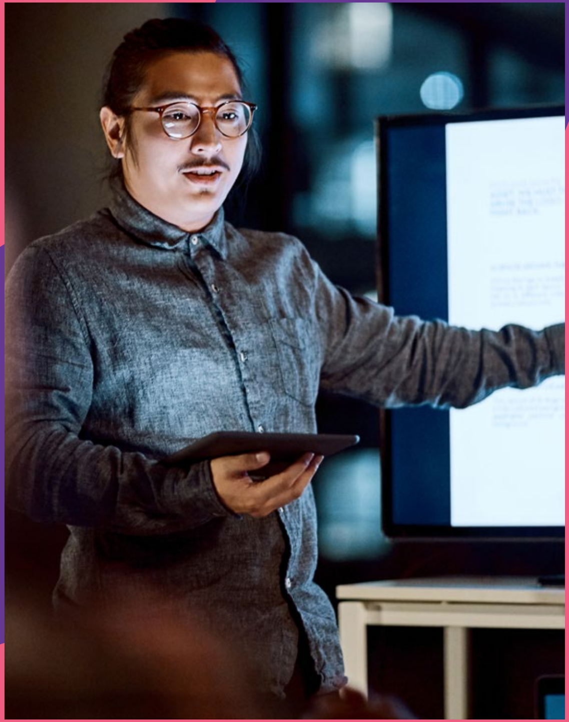
Atos and AWS join forces to challenge security concerns to deliver customers cloud confidence.

Atos | aws

In today's technology-driven world, cloud computing has become a cornerstone of business transformation. The benefits of cloud adoption, including scalability, cost-efficiency, and accessibility, are undeniable.

However, with the growing reliance on cloud data storage, enterprise organizations, across the world, also face heightened security threats.

In this executive briefing, we delve into the pressing concerns around cloud data security and how Atos and AWS are collaborating to deliver robust solutions that inspire confidence in cloud-based operations.



The dilemma of data security

Safeguarding sensitive data is paramount. While enabling unprecedented operational performance, cloud also brings to light a nervousness for many about ensuring the confidentiality, integrity, and availability of data.

Worries over unauthorized access, data breaches, and data sovereignty can create major roadblocks for organizations considering the migration of critical systems and workloads to the cloud.

Atos, a global leader in managed infrastructure, has partnered with Amazon Web Services (AWS), to migrate customers' critical systems and workloads to the world's leading cloud.

Atos CloudCatalyst brings together Atos' expertise in cybersecurity and risk management with AWS' state-of-the-art cloud infrastructure, enabling customers to fortify their data security in the cloud.

Addressing compliance and regulatory requirements

Large organizations, operating across diverse industries, must adhere to a multitude of compliance and regulatory frameworks. Cloud data storage must also comply with industry-specific regulations, data privacy laws, and regional governance policies. Failing to meet these requirements can result in hefty fines and reputational damage.

Together, Atos and AWS offer a range of industry-tailored security services and solutions, designed to meet these compliance and regulatory requirements. Atos leverages AWS' security framework – including solutions like Amazon Macie – to tailor a solution that's right for the business. Atos can help customers to ensure that their cloud data aligns with specific standards and policies, even in highly regulated sectors such as finance, healthcare, and government.

We offer a comprehensive set of compliance certifications, attesting to the platform's adherence to industry-specific security standards. For instance, AWS complies with the Health Insurance Portability and Accountability Act (HIPAA) for healthcare organizations, the Payment Card Industry Data Security Standard (PCI DSS) for handling credit card information, and the Federal Risk and Authorization Management Program (FedRAMP) for government agencies.

With such certifications, AWS provides enterprises with the confidence that their cloud environment meets the necessary compliance requirements.

Cloud data encryption and privacy

The threat of data breaches remains front of mind for customers contemplating cloud adoption, storing sensitive information on third-party cloud servers can raise questions around data encryption and privacy, particularly during data transmission.

Atos partners with the customer to ensure the security solution is right for them. Our advanced encryption protocols safeguard data, both in transit and at rest. By encrypting data before transmission and during storage, customers can rest assured that their sensitive information remains secure and unreadable to unauthorized entities. This encryption-centric approach ensures data privacy, even in the event of a security breach.

A comprehensive Key Management Service (KMS) gives control of the encryption keys used to protect data. This service enables customers to create and manage encryption keys, implement key rotation policies, and even integrate with Hardware Security Modules (HSMs) for additional security.

By giving full control over encryption keys, we ensure that sensitive data remains secure throughout its lifecycle.

Managing insider threats

Insider threats, whether unintentional or malicious, are another critical issue faced by large organizations. Employees with access to cloud data could inadvertently leak sensitive information or intentionally exploit vulnerabilities.

To combat insider threats, we implement robust Identity and Access Management (IAM) solutions, to manage user access and permissions effectively. AWS IAM ensures that only authorized personnel can access specific data and applications, reducing the risk of insider data breaches.

AWS IAM provides fine-grained control over user access permissions, to define access policies based on roles and responsibilities. Through AWS IAM, organizations can implement the principle of least privilege, granting users only the necessary permissions required to perform their tasks.

Additionally, AWS IAM supports Multi-Factor Authentication (MFA), adding an extra layer of security by requiring users to provide multiple forms of authentication before accessing sensitive data or applications.

We also offer federated access to users via IAM Identity Center, making it easy to centrally manage federated access to multiple accounts and business applications, and to provide users with single sign-on access to all their assigned accounts and applications from one place.

Continuity and disaster recovery

Business continuity is paramount for major enterprises. Where cloud brings about concerns over data availability, during unforeseen events or system failures, we offer robust disaster recovery solutions.

These ensure data replication and backup in multiple geographical locations and, in the event of a disaster, customers can quickly restore their critical data and continue to operate seamlessly.

Our disaster recovery solutions, include cross-region replication and backup capabilities. Services like AWS Backup enable automation of the backup of data across multiple services, ensuring that critical data is safeguarded against data loss.

We also offer disaster recovery architectures like Pilot Light and Warm Standby, enabling our customers to maintain partial or fully operational environments in separate regions, ready to be quickly activated in the event of a disaster.

Atos also has a managed back-up solution for disaster recovery that leverages AWS Elastic Disaster Recovery as a cost-effective and scalable solution, optimizing expenses by eliminating idle recovery site resources and charging only when the full disaster recovery site is operational. This ensures swift recovery of applications in their most recent state or from a specific point in time.

The service's design, which includes a staging area for data replication, minimizes costs by utilizing affordable storage and minimal compute resources.

AI-driven security intelligence

Today's complex cyber security landscape demands advanced security measures. Organizations must be equipped with AI-driven security intelligence to detect and respond to potential threats proactively.

Atos is spearheading trusted generative AI security solutions, with initiatives like our AI Center of Excellence, where we are building advanced solutions related to AI security. Atos also leverages the core capabilities of AWS Bedrock to build trusted AI security solutions for our clients. We integrate AI-driven security intelligence into services to provide continuous threat monitoring and automated incident response. Through machine learning algorithms and behavioral analysis, customers can identify and mitigate potential security risks before they escalate.

GuardDuty, is a managed threat detection service that uses machine learning to analyze data from AWS CloudTrail, VPC Flow Logs, and DNS logs to identify suspicious behavior and potential threats. GuardDuty provides actionable alerts to security teams, enabling them to take immediate action and prevent security incidents.

Another notable security feature is the inclusion of software firewalls in the

>>

AI-driven security intelligence (continued)

configuration of compute instances within the EC2 and AWS environment. Customers can define stateful and stateless firewalls in their Virtual Private Cloud (VPC) and subnets to enhance security at the network level.

Cloud Security Posture Management (CSPM) functionality, aggregates, organizes, and prioritizes security findings from across our services and partner solutions in a centralized dashboard. This significantly helps customers to continuously monitor and improve their security posture.

Amazon Inspector, an automated security assessment service, enhances the vulnerability management process. Inspector examines applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Inspector produces a detailed list of security findings prioritized by level of severity.

Amazon Security Lake centralizes security data from various sources into a purpose-built data lake stored directly in our customers' accounts. This significantly enhances data visibility across accounts, streamlining data management, at scale, and optimizing it for efficient storage and query.

This comprehensive approach to security data management is a game-changer for customers aiming to enhance their security operations.

The promise of shared responsibility

Understanding the shared responsibility model in cloud security is crucial. While cloud service providers are responsible for the security of the cloud infrastructure, enterprises must also take ownership of securing their data and applications. This can be a significant challenge. Atos can help enterprise customers to navigate the challenges that arise with these new responsibilities and help mitigate security risks.

Together, Atos and AWS emphasize a collaborative security approach, where we work with our customers to create a secure cloud environment. Atos assists enterprises in designing robust security frameworks, while AWS ensures that the cloud infrastructure adheres to industry-leading security practices.

Securing a future built on cloud

As major enterprises continue their digital transformation journey, concerns around cloud data security remain at the forefront. However, the strategic partnership between Atos and AWS has demonstrated that these concerns can be effectively addressed, and security enhanced, through our cutting-edge solutions and collaborative approach.

By leveraging Atos' cybersecurity expertise and AWS' cloud infrastructure capabilities, customers gain access to a comprehensive suite of security services tailored to meet industry-specific compliance requirements.

With advanced encryption protocols, robust AWS IAM solutions, AI-driven security intelligence, and disaster recovery capabilities, the Atos-AWS alliance offers a holistic approach to safeguarding cloud data for large corporations.

As the cloud landscape continues to evolve, our partnership sets an example of how industry leaders can work together to provide robust and innovative solutions, inspiring confidence in cloud-based operations and unlocking the full potential of cloud computing.

Securing cloud data for major enterprise features contributions from:
Eric Terrell, Atos: Head of Technology, AWS Practice
Jaydev Goswami, AWS: Sr Enterprise Solutions Architect

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

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.