

Unify Cloud Security with Atos

Let us be your shield while you conquer the cloud



Atos

Multi-cloud security is more needed than ever.



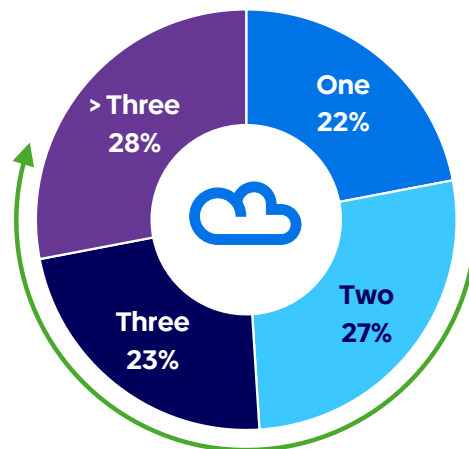
44%

of organizations have experienced a **cloud data breach** with 14% having had one in past year



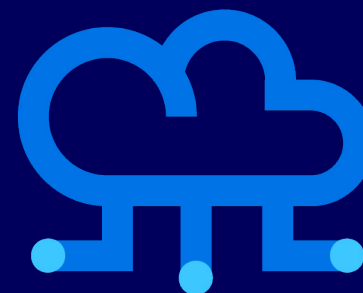
61%

of organizations cite **security and compliance** as the primary barriers to cloud adoption



78%

of cloud organizations, use two or more cloud providers



What strategies should be used to ensure a comprehensive **secure cloud migration** from the start, including **design** and **integration**?

- How do you ensure secure, scalable, and cost-effective cloud infrastructure while **preventing** misconfigurations?
- How do you automatically detect threats and **protect** cloud assets for efficient organization and security?
- How do you **preserve** a consistent security posture, rapid issue detection, swift compliance implementation, and prompt response to suspicious activity?

¹Sources: [2025 Fortinet State of Cloud Security Report](#), [2024 Thales Cloud Security Study](#)

Get off my cloud!

When an organization transitions to the cloud, it must take on new responsibilities and adapt its processes and procedures to address a range of diverse and unfamiliar threats.

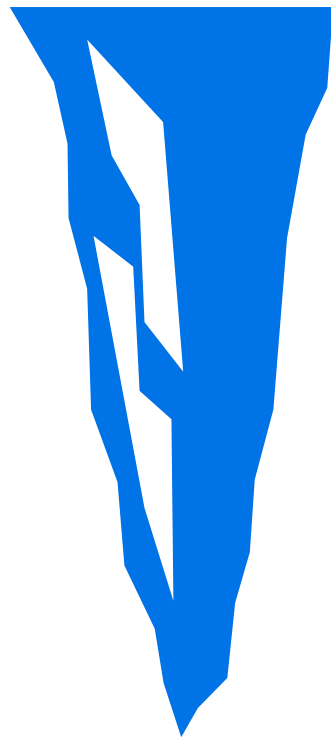
Atos offers specialized cybersecurity services, from consulting to managed services, tailored to these complex ecosystems, providing robust security controls that span both cloud and traditional environments. Below are some of the common challenges we help our customers overcome.

Security of the Cloud



Cloud
provider

Physical and logical infrastructure



Cloud
customer

Category	Your Concern	How Atos Protects You	How we helped our clients
Data Security	Struggling to locate and protect sensitive data?	Assessing and prioritizing data risks, then deploying encryption, data loss prevention, and access controls.	For a French cancer research organization, we strengthened data sovereignty with an encryption key control solution in AWS for patient's data privacy and security.
Application Security	Are SaaS apps, multi-cloud, and APIs exposing gaps?	Conducting continuous security assessments and application vulnerability scans.	For the Hôpital Privé de l'Est Lyonnais of the Ramsay Santé group, France's leading private healthcare provider, we carried out crisis exercises to identify best practices and areas for improvement via detailed consultant reports.
IAM	Too many excessive access rights creating risks?	Delivering IAM solutions and enforcing cloud access governance.	For a Netherlands-based insurance company, we monitored, analyzed, and identified compromised identities across the customer's hybrid environment by leveraging Microsoft Defender for Identity.
Configuration Management	Are misconfigured cloud resources putting your environment at risk?	Securing cloud configurations and continuously monitoring for misconfigurations.	For a multinational telecommunications company, we worked for their customers to benefit from new levels of managed security services, including web and email security, EDR, threat intelligence services.
Compliance	Struggling to meet compliance demands?	Delivering expertise and tools to ensure regulatory alignment.	For Accor, a French multinational hospitality, we provided a secure, PCI-DSS compliant GCP landing zone with expert security and cloud architects.
Detection and Response	Overwhelmed by constant security alerts?	Offering 24x7x365 monitoring, threat detection, and incident response services	For Dentsply Sirona, Dentsply Sirona Inc. an American dental equipment manufacturer, we delivered Managed Security Services powered by Google SecOps and SCC Premium, enabling rapid detection of potential threats and enhanced overall visibility into their security posture.

Security in the Cloud

How we supported the largest sports event in 2024

For [Paris 2024](#), our teams delivered services around three core capabilities: cybersecurity planning and preparation, products and services and operations. While their information system was hosted in the cloud, 55 billion cybersecurity events were analyzed for zero incidents impacting the Paris 2024 Games.

Unified cloud security

At Atos, our approach to cloud security emphasizes enforcing **unified trust and compliance** across all security domains, ensuring seamless protection for multi-cloud environments. Our comprehensive strategy integrates key focus areas designed to address the unique challenges of modern cloud ecosystems:



Cloud Service Provider Security

Microsoft

Managed
CloudSecOps
Protection

Google

Managed
CloudSecOps
Protection

AWS

Managed
CloudSecOps
Protection

We leverage the advanced security capabilities of cloud hyperscalers such as AWS, Azure, and GCP to deliver deeply integrated managed security services that align with your operational needs.



Multi-Cloud Protection Platforms

Managed CNAPP

Security
Posture Mgt

Artifacts
scanning

Container
security

Cloud
Workload
Protection

Least
Privilege

Vuln. Mgt

Managed SASE

Security Web
Gateway

CASB

FWaaS

ZTNA

SD-WAN

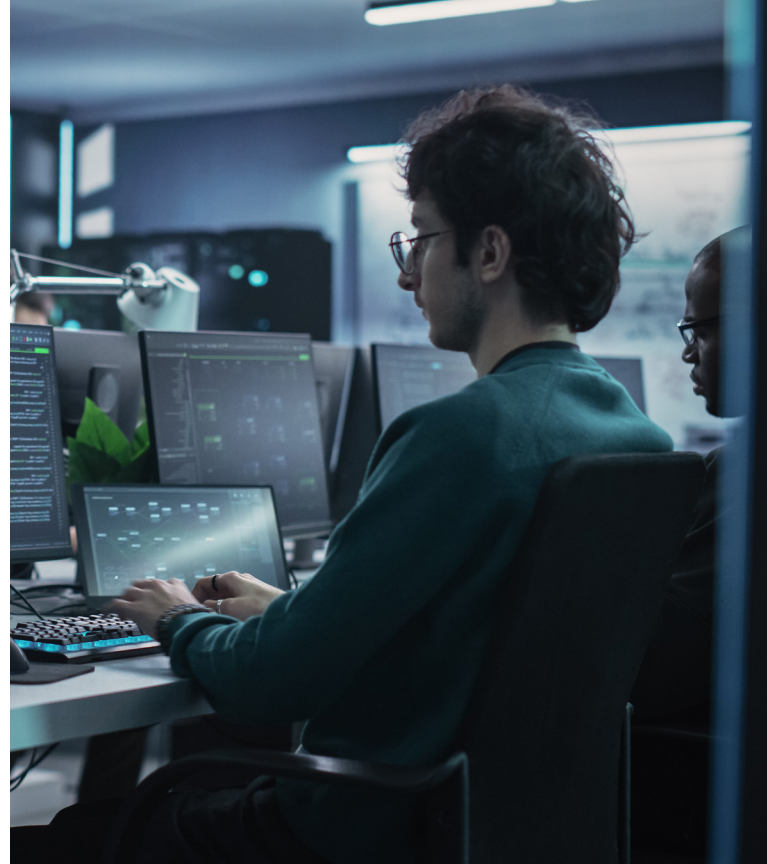
We address multi-cloud security needs by wisely integrating cybersecurity pure player solutions with cloud service providers capabilities to bring the best of them in a unified managed security service.



Digital Sovereignty

Cloud Encryption Services

Our Cloud Encryption Services are designed for specific applications or business processes that require a higher level of control over data encryption mechanisms in order to mitigate targeted sovereignty risks. These services are part of the comprehensive Atos Digital Sovereignty approach.



Recognizing that cloud environments remain critical, we deliver comprehensive and unified security services to protect them. We ensure project success through structured phases (discovery, implementation, operationalization, management, and continuous support).

The Atos advantage

Securing the Cloud can be more complex than expected. But a carefully considered cloud strategy can deliver comprehensive security while stimulating business and digital innovation. Atos is a trusted partner in securing legacy infrastructure and cloud operations, recognized as a leader in managed security services worldwide by Gartner. We help our customers invest in the right controls in the right places, quickly and effectively, designing, building and operating end-to-end security across the organization.

Your cloud security, truly from end-to-end

We manage security seamlessly across multiple cloud platforms (AWS, Azure, Google Cloud, Alibaba, etc.) and hybrid environments (combining on-premises and cloud infrastructure), from the discovery phase to the management phase. We not only leverage hyperscalers' security features but also pure player cybersecurity solutions to bring you the best security coverage in a unified delivery.



- 2023 Global GSI Security Partner of the Year finalist
- 2023 GSI Partner of the Year for North America
- Global Systems Integrator (GSI) Partner of the Year for EMEA in 2022
- Launch partner for several security programs from AWS (Amazon Security Lake and AWS KMS External Key Store (XKS) in 2022)
- AWS Well-Architected Partner
- Several Competency status: AWS level 1 Managed Security Service Provider, AWS Digital Sovereignty, AWS Generative AI
- AWS Security Incident Response Specialization

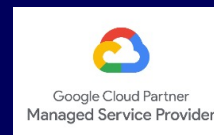


- 850+ Microsoft consultants in our global delivery centers
- Microsoft Intelligent Security Association (MISA) member
- Microsoft MXDR certified
- Microsoft's advanced specialization in cloud security, threat protection and information protection and governance, Microsoft 365 information security and governance
- Azure Expert and GOLD certified partner

Member of
Microsoft Intelligent Security Association



- Google Cloud Premier partner
- Google Cloud MSSP
- 13 years of partnership
- Specialized in managed security services for GCP
- 6 years Google Partner of the Year (3 for Security)
- 3,600+ Google certifications



A business-aligned approach

Our approach prioritizes your business goals, tailoring cloud security strategies to address your unique risks. For complex environments, we offer customizable solutions, while more streamlined and cost-effective packages are available for simpler needs.* You benefit from the experience of 6,500+ security professionals safeguarding your business who process 31 billion security events every day.

* Available for Microsoft Defender for Endpoint, Microsoft Defender for Cloud and Microsoft Sentinel

A step ahead in digital sovereignty

With Atos, navigating digital sovereignty considerations for business processes and cloud adoption is simpler than ever:

- Understand the sovereignty implications on your business processes
- Prioritize your sovereignty efforts and determine where to start
- Migrate complex business processes to the cloud while maintaining compliance.

About Atos

Atos Group is a global leader in digital transformation with c. 72,000 employees and annual revenue of c. € 10 billion, operating in 68 countries under two brands – Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. 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.

Find out more about us

atos.net

atos.net/career



Atos is a registered trademark of Atos SE. July 2025. © Copyright 2025
Atos SE. Confidential Information owned by Atos group, 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 of Atos.