Cybersecurity

Building trust in Hybrid Cloud

Trusted partner for your **Digital Journey**

Atos

Contents

The Cloud security challenge

The Cloud is a key enabler of digital transformation. It is transforming business, organizations and government, enabling new levels of speed, agility and focus. At the same time, cloud computing has spawned an alarming range of new security threats. These threats require new thinking from business leaders and even traditional IT professionals.

Migrating your business to cloud services can deliver significant cost and efficiency gains for organizations of all sizes. Cloud enables enterprises to reinvent their business models, forge better relationships with customers, take significant costs out of their operations and get successful innovations to market ahead of the competition.

Whether as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) or the latest trends in Container-as-a-Service (CaaS) and Function-as-a-Service (FaaS), cloud continues to evolve and provide organizations with the agility they need for today's fast-paced digital world.

As well as multiplying opportunities, cloud computing can also multiply risks. The rise of cloud has led to a new breed of security vulnerabilities and amplified existing ones.

As companies move towards a hybrid cloud environment, mixing on-premise infrastructure with multiple cloud providers and 'shadow IT', their traditional defenses may be overwhelmed. Because of heightened security concerns and the fear of the unknown, some organizations are not benefitting fully from the power of cloud computing.

While the major cloud service providers are experts at ensuring the security **of the Cloud**, security **inside the Cloud** is largely the responsibility of the customer. To make sure that they can manage these new responsibilities, enterprises need to transform their security organization, policies, processes and controls. They will also have to adopt new technologies and change their processes to adapt to this new world.

Cloud computing security is no longer just an IT issue. It is a strategic boardroom concern, with major consequences for shareholder value and corporate reputation. Because of the always-on nature of cloud computing, security breaches can have long-lasting impacts on how a company is perceived and on how it is valued by the market. If the C-Suite ignores cloud security at its peril.

New technologies and strategic thinking can counter today's security threats and secure the hybrid enterprise. With the right security policies, processes and partners, businesses can defend themselves against attack and maximize the value of their investment in the Cloud.

14 million Verizon customers' personal data stored on an Amazon S3 cloud server were exposed for at least nine days in 2017

68 million user account details leaked in a Dropbox data breach in 2012, or two-thirds of their customer base

1 in 4 IT professionals have experienced data theft from the public cloud (for both Software-as-a-Service and Infrastructure-as-a-Service)[1]

A hole in the S3 bucket

According to the Cloud Security Alliance, data breaches are the single most critical issue for cloud security. Many of these breaches are the result of a simple misconfiguration by customers of their security inside the Cloud. With a hybrid cloud security enforcement and monitoring program, these mistakes can be quickly identified and corrected.

"Increased use of cloud technology to store sensitive information will continue to tempt cyber attackers. They will take advantage of the fact that many businesses put too much faith in the cloud providers and don't stipulate how and where their data is stored."

The Cyber Threat to UK businesses, 2017-2018 report of the National Cyber Security Centre and the National Crime Agency

[1] Navigating a Cloudy Sky, report from McAfee, https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-security-report.html

Get off of my cloud!

Make no mistake. Securing the Cloud is more complex than you think. But a carefully considered cloud strategy can deliver comprehensive security while stimulating business and digital innovation.

As organizational data moves beyond the traditional perimeter, cloud computing has expanded the attack surface. Using Cloud services, companies will be sharing a platform with other organizations and potentially with criminal agents intent on harm.

To counter this threat, leading Cloud services companies offer their customers a common defense against attack. They will monitor cloud services and look out for any anomalies or cause for concern.

However, in a complex, multi-cloud world these systems are not enough to secure a company's environment.

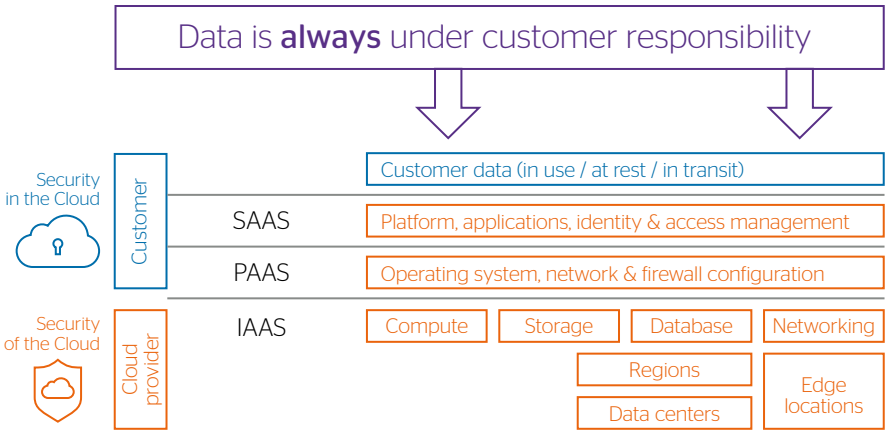
In this new environment, the native security features of the cloud provider can only ever be a start. Gartner has estimated that through 2022, at least 95% of cloud security failures will be the customer's fault.[2] While the cloud service provider can focus on the security of the Cloud, it must be the responsibility of the customer to ensure security inside the Cloud.

To achieve this, they will need not only transform technologies but also policies on risks, responsibilities and data ownership. Atos works with customers around the world to evolve towards this framework, adding a sophisticated layer of trust, control and monitoring that covers all the complexities of the multi-cloud world.

57 million hackers accessed the cloud-based personal data of 50 million Uber customers and 7 million drivers in 2017

56% of organizations surveyed by McAfee had tracked a malware infection back to a cloud application

Security in cloud computing is based on a shared responsibility model. Depending on the model, be it IaaS, PaaS or SaaS, while the cloud service provider has responsibilities for the security of infrastructure, physical network and often also the operating system and application, it is the customer's responsibility to manage elements including user access, identity and the data itself.



Public Cloud Security - A Shared responsibility / A Trust relationship

The Treacherous 12

The Cloud Security Alliance (CSA) has identified the following 12 major security threats to cloud computing:

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Vulnerabilities

[2] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

Responding to the threat

When an organization migrates their business to the Cloud, it will have to assume new responsibilities and develop and adapt their processes and procedures to counter diverse and unfamiliar threats.

The XaaS models offer an increasing range of solutions tailored to the company's business, giving them the flexibility to choose what they want. Depending on the model chosen, the shared responsibility for the security of and in the cloud will vary. For instance, in an on-premise model, everything is on the customer responsibility from the cloud infrastructure to the data, whereas in a SaaS model only user access and data are concerned.

The cloud provider will have to handle the security of the applications in the cloud and the security of the cloud itself.

Empirical data suggest that many companies are finding it difficult to rise to this challenge. According to a survey by McAfee of 1,400 IT decision makers around the world, 28% of organizations do not feel they have complete control over who can access sensitive data when using IaaS, 25% for SaaS and 18% for private cloud.

Still, only 16% state that they store no sensitive data at all on the cloud.

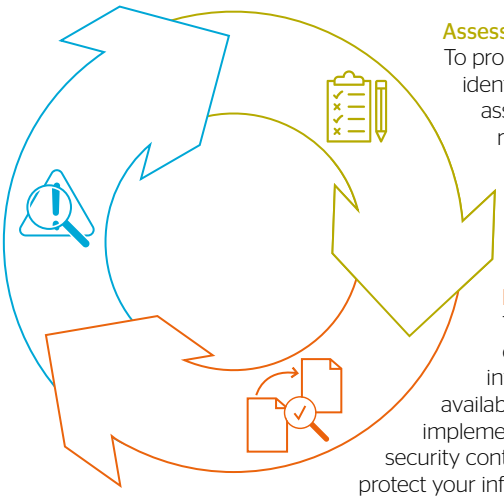
As they focus their resources on this latest threat, enterprises are devoting increasing proportions of their IT security budgets to cloud security. From 27% of IT security spending in 2017, the amount of expenditure allocated to cloud security is expected to rise to 37% in 2018[3].

Threats		Impacts	
Leaky buckets AWS S3	Shadow IT	Loss of IP	Loss of customer trust
Supply chain Target breach	APT	Degraded brand image	
	Weak ID	Violation of regulations	
Insecure API's	Data loss	Data loss	Financial cost
Unsantioned Cloud	DDOS	Business continuity disruption	
Cross workload attacks	Serverless attacks		
Orchestration attacks	Cross Cloud attacks		

A changing threat landscape

Along with technological innovation and cultural change, it is the growing maturity of the shared responsibility model that will increase confidence in cloud security and help organizations reap the full benefits of cloud computing.

To address the cloud security challenges, at Atos, we propose an approach in 3 steps: assess, protect, detect & respond.



Assess
To protect you must first identify the 'what', the associated risks and requirements

Protect
To maintain confidentiality, integrity and availability you must implement & update security controls in order to protect your information from threats and enable traceability

Detect & respond
To preserve a secure state it is crucial to ensure the real-time detection of security deviations and incidents and have the means to automate a response immediately

Cloud Security - An Integrated and Continuous Approach

"Our breach is their breach, and their breach is our breach."

CISO of large entertainment company, cited in *McAfee, Navigating a Cloudy Sky*

"Critical data in the cloud should be protected with the implementation of security controls by both the cloud provider and the enterprise."

***State of Cloud Security 2018*, report by the Cloud Security Alliance**

[3] McAfee, op. cit.

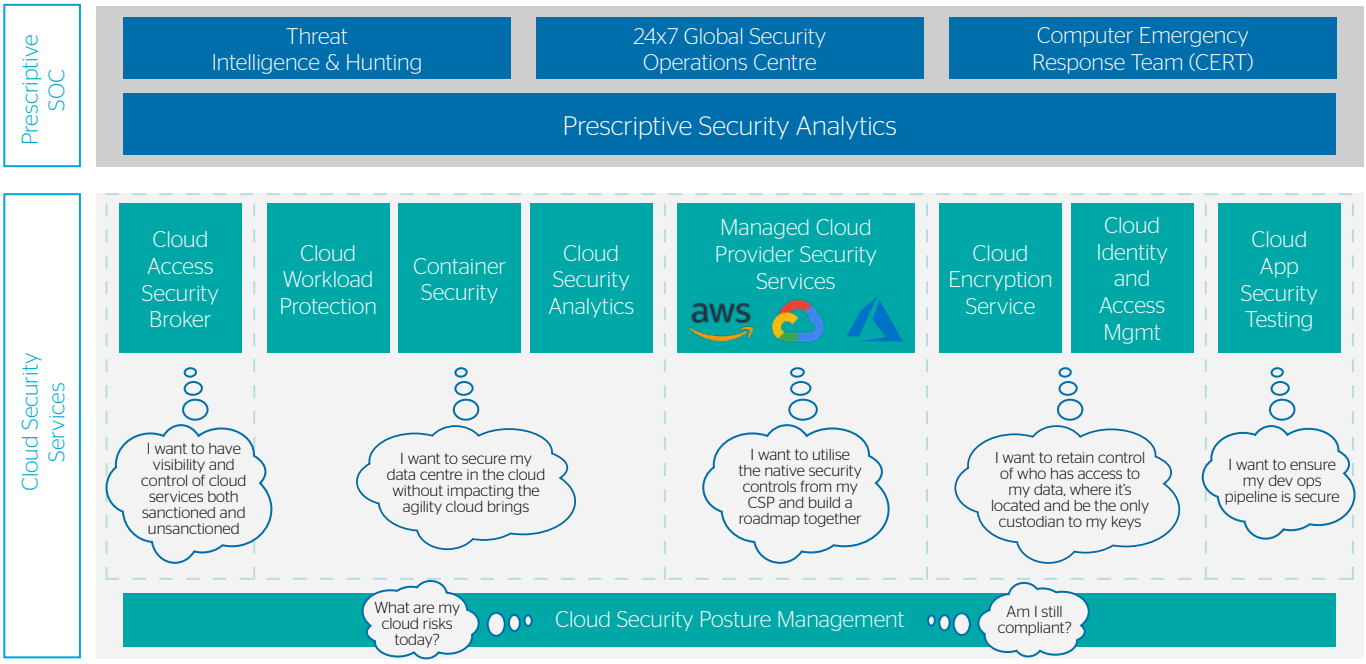
Cybersecurity goes hybrid

In today's hybrid, multi-cloud environment, it is imperative that enterprises integrate all their security controls into one overall security posture. Only with a robust approach to cybersecurity, protecting data that is shared across both public and private clouds, can the benefits of cloud be maximized.

The native security controls of cloud providers are useful, but they have their limits. They cannot protect you against the risks posed by employees using shadow IT. Nor do they manage the security of an organization's on-premises servers and infrastructure. And they cannot manage the security of an organization's owned workloads inside the cloud, whether they are virtual machines, containers or applications.

Gartner has said that in this new world, companies must change their line of questioning from "Is the cloud secure?" to "Am I using the cloud securely?"

Atos has built a secure hybrid cloud platform for these complex new ecosystems, answering these questions and adding an additional layer of security controls that covers both cloud computing and traditional environments.



Cloud Security Portfolio - Comprehensive coverage

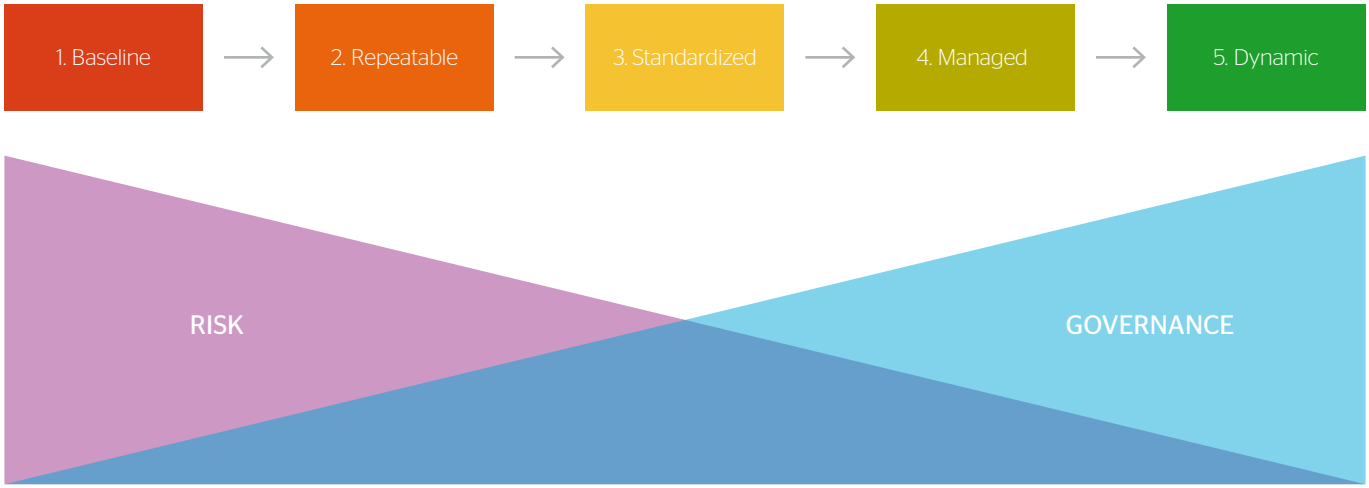
"The enterprise needs to train employees on basic security practices. Avoiding phishing attacks and proper password management practices can prevent many of the malware attacks such as ransomware and DDOS."

State of Cloud Security 2018, report by the Cloud Security Alliance

Cloud security maturity assessment

Before starting any Cloud project, the first step is to analyse the current situation in order to have a full visibility on the existing status. Observing and understanding will help to identify where sensitive data is stored, what is the scope of shadow IT, during this phase all external regulations and internal constraints also have to be taken into account.

During this assessment, with its consulting experts in security and Cloud, Atos will help you to get a cartography of your landscape, an initial risk evaluation and a maturity assessment. This will then be the foundations to define the best strategy for your specific context.



Cloud maturity model

Level 1 (Baseline)	Level 2 (Repeatable)	Level 3 (Standardized)	Level 4 (Managed)	Level 5 (Dynamic)
Lack of clear cloud use and data security policies and blocking known services without regard to their risk profile, response to incidents is incomplete and slow with ad hoc process	Organization has begun to define acceptance criteria for selecting cloud services and has a whitelist of approved cloud services	Approved whitelist for all CSP categories at the department level. Clearly defined DLP and encryption policies with complete incident workflows and roles	Approved CSP list, policies, and workflows are updated quarterly by cloud governance committee using feedback from business	Clearly defined policies aligned with business objectives, continuously updated with adherence to strong process/ workflow and immediately incorporated feedback

360-degree visibility

In a multi-cloud world, it is essential for businesses to have visibility of exactly what data is held in the Cloud and which applications employees are using to access this data. Increasing trust in cloud computing will require not only a change in thinking but also the implementation of multiple technologies and processes. According to McAfee, today's leading methods for securing sanctioned environments include:

- data loss prevention (DLP) and encryption
- identity and access management
- regular audits of apps in use and assessments of potential risks
- blocking access to the unauthorized cloud service
- migrating the shadow IT to an approved and similar service

Companies are increasingly subscribing to Cloud Access Security Broker (CASB) services which give them visibility and control of shadow IT. A CASB sits between users and the services they are accessing for SaaS. It allows organizations to extend the reach of their security policies beyond their own infrastructure and into the Cloud.

The Atos CASB service gives enterprise customers the ability to:

- discover and remediate the risk from the use of shadow IT across the enterprise
- control and enforce data privacy and compliance across shadow IT through the sanctioning of cloud apps such Google Cloud Platform, G Suite, Office 365, Box, Salesforce, and ServiceNow, and IaaS platforms such as AWS and Azure
- protect enterprises' data through persistent protection, wherever it moves within the Cloud
- insert a frictionless security control point between the enterprise user and cloud service

Working with McAfee's CASB across all cloud services, Atos helps customers see what data is being shared with third parties via the Cloud so that they can take the required action based on this insight. Using the CASB approach, we can automatically categorize the risk level posed by each and every SaaS cloud service provider discovered.

Atos' expertise in McAfee's CASB technology enables companies to make hybrid cloud management and security a seamless experience that supports their digital transformation.

Complying with regulation

Compliance with both internal policies and industry regulation is a major driver of demand for the new generation of cloud security services.

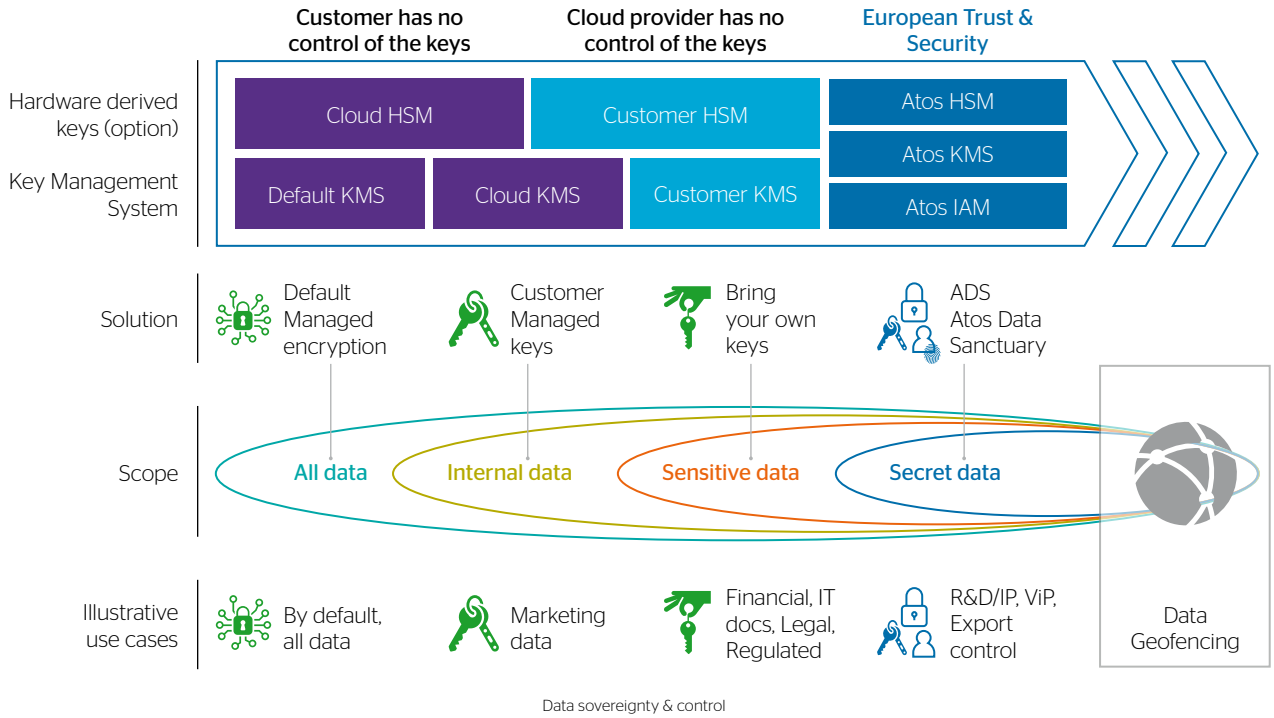
Across the world, new data regulations are coming into force. Non-compliance with the GDPR (General Data Protection Regulation) and the NIS (Network Infrastructure Systems) directive in the EU, or the CLOUD Act (Clarifying Lawful Overseas Use of Data) in the US, can result in heavy fines for organizations as well as a dramatic impact on reputation. Now more than ever, cloud security has become a vital business requirement. With a holistic, hybrid approach, an enterprise can assess its vulnerabilities, implement the right controls, and ensure continuous compliance across its operations.

Lock up your data

The process of encryption converts data into code that conceals the data's original meaning to prevent it from being accessed, understood or used. While cloud providers can deliver this service, the key to unlock the data remains in their possession.

Many customers would like to protect their sensitive data from cloud service providers, where they may be vulnerable to the threat of a brute force attack – a sustained attack that tries all possibilities, one by one, until it is successful. The deployment of encryption protects data from any form of access by anyone apart from the customer.

Partnering with an end-to-end provider such as Atos adds a new layer of trust and security to cloud computing. While the data goes to the Cloud, the ability to unlock it stays with the client. As a result, only the customer can see their data. Furthermore, Atos can disable the download of corporate data from the Cloud to unmanaged devices, protect sensitive data from being uploaded to cloud services, and use geofencing to determine the jurisdictions where sensitive data is stored and managed.



Only the right persons access the right resources

A successful encryption is based on a strong IAM control in order to ensure the entitled users have access to the decryption keys and nobody else.

Managing centrally who has access to what and enforcing policies such as least privilege is vital. One of the challenge set by the migration to the cloud is that for each new service included in the cloud, the more people will be provided with different credentials and access policies.

It makes it difficult to have a comprehensive visibility and management of each resources, increasing the risks faced by the organization.

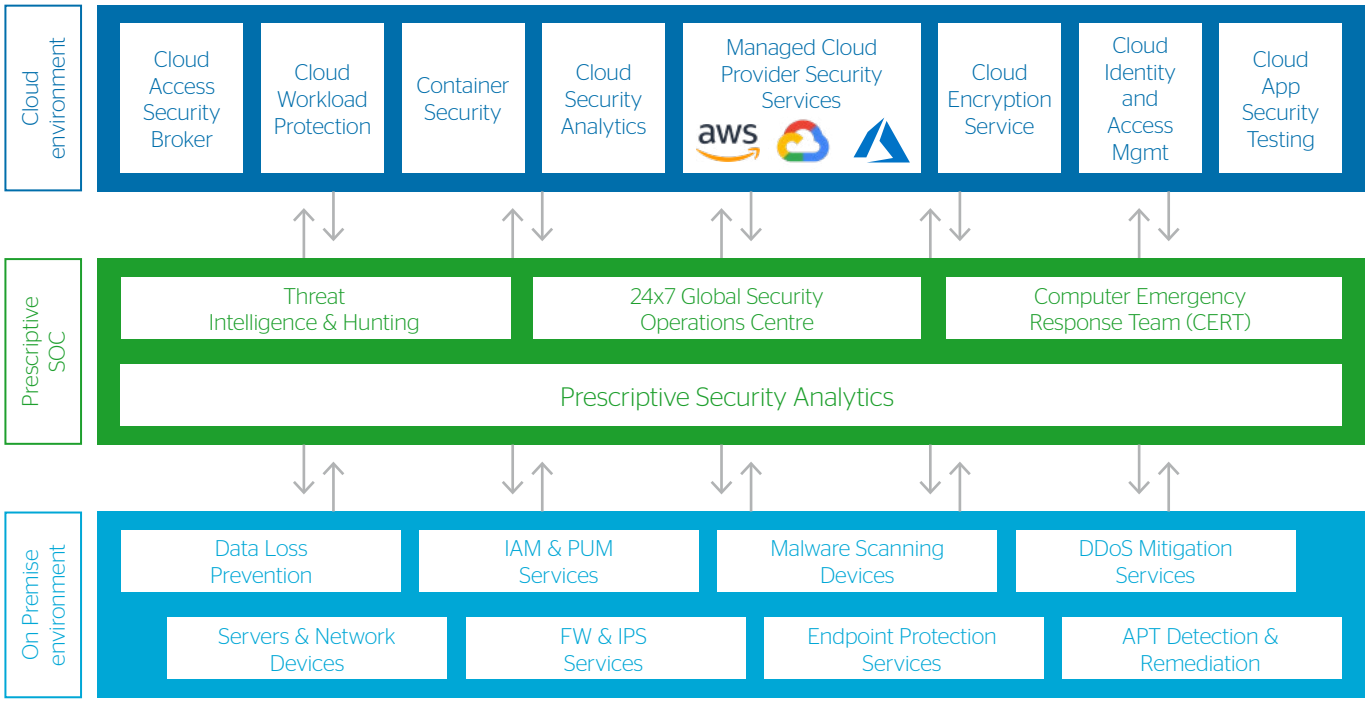
A cloud identity and access management solution helps handling the security policies required for each application. Federated identity management connects identity management systems together: with single sign-on, a single user authentication is enough to connect across many applications, even when they have different authentication protocols, eliminating the burden of entering credentials every time. Through identity provisioning, users are allowed to access the applications needed for their work, granting them a role with the appropriate authorizations. Finally, multi-factor authentication ensures a high-level of security by confirming the user's identity and adapting the level of authentication required to the level of risk posed.

SOC it to the attackers

Gartner has predicted that by 2020, 60% of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk[4]. As data moves out of the data center and into the cloud, mobile and SaaS environment, a new cybersecurity approach is needed to address risks and threats in technologies and assets that are no longer under the direct ownership or control of the organization.

Atos has a worldwide network of SOCs worldwide providing end-to-end cybersecurity services and solutions to national and global clients across all sectors, 24x7. Those SOC are a secure facility which functions as the central hub for cybersecurity incident prevention, detection and response.

A hybrid SOC enables monitoring of cloud services, IaaS, shadow IT and legacy infrastructure, around the clock, 365 days a year. Atos SOC also use Artificial Intelligence and Big Data analytics to help customers swiftly predict and thwart security threats.



Hybrid environments

[4] https://www.gartner.com/newsroom/id/3337617

Cloud security in action

The development of secure hybrid cloud services is transforming business technology at an unprecedented pace. Whatever the main security concerns of your organization, with the right technologies and the right processes you can defuse the threat.

Privacy & cybersecurity	Continuous compliance	Data Sovereignty & Control
Detect compromised resources and insider threats	Uncover Shadow IT usage and understand content flowing into and out of the cloud	Protect sensitive data from being uploaded to prohibited cloud services geo-region
Protect against unauthorized sharing of sensitive data	Achieve compliance with both internal policies and industry regulations	Protect data from cloud service provider access by encrypting with own keys
Protect data from inadvertent disclosure	Determine your current security posture and risks dynamically	Retain control of identity and access rights of your cloud assets

No blind spots

There can be no control without visibility. However, according to a recent report from McAfee, almost one third of organizations who use SaaS are experiencing difficulty in getting a clear picture of what data is in their cloud applications.

The need to restore visibility and reassert ownership and control has become a major driver for hybrid cloud security solutions. With real-time monitoring and analytics, a business gains global visibility into the consumption of IT resources inside and outside the organization.

Only when a company has visibility across all platforms can it implement consistent policies for its processes.

By implementing a hybrid security approach, an enterprise can uncover the usage of shadow IT by its employees. It can understand exactly what content is flowing into and out of the cloud.

It can also identify any unsanctioned cloud services that are being used on the enterprise network and move quickly to close any breaches of policies and regulations.

By 2020, 60% of large companies will use CASB services to increase visibility and protect against threats[5].

Defusing threats

By embracing the secure hybrid cloud, enterprises can achieve the levels of protection against threats that they need. For example, they can protect data from inadvertent disclosure or unauthorized sharing and detect compromised accounts and threats from insiders. Organizations can stop unwanted devices, users and versions of applications from accessing cloud services. A secure hybrid cloud can protect data that belongs to a company's intellectual property, whether that be proprietary software code or sensitive corporate information.

[5] Gartner *Magic Quadrant for Cloud Access Security Brokers*, November 2017

Creating value with a secure hybrid cloud

A secure hybrid cloud architecture can provide an enterprise with even more effective protection than on-premises infrastructure, enabling organizations to embed and automate many of their security controls and audits.

With new security paradigms in place, the hybrid cloud model becomes a driver of overall business strategy. It enables organizations to achieve their strategic goals, such as reducing time-to-market, securing the digital and mobile workplace, and delivering Continuous Integration and Continuous Delivery (CICD).

Automation is a critical part of the cloud security equation. In the legacy environment, many major security breaches occur when the IT team forgets to patch a web server in an on-premises data center.

In the hybrid cloud world, security audits, controls, patching and configuration management can all be automated, reducing the risk significantly. With the continuous updating of virtual infrastructure and code, the business of securing your company becomes both more efficient and more effective.

An automated approach, removing the potential for human error, is key to managing change at scale, and could very well prevent the next highly visible breach – provided the right processes and the right technologies are in place.

Thanks to this capability for real-time monitoring and security analytics, and the ability to respond rapidly to threats, an organization can enjoy full visibility over its operations and detect possible vulnerabilities across different cloud environments and different jurisdictions.

With a secure, automated cloud platform, enterprises will be able to adopt different approaches to application development, achieve their strategic goals and objectives and create new value for customers and stakeholders.

On the cutting edge

The principles of programmable infrastructure, or Infrastructure as Code (IaC), can generate significant benefits from a security perspective, enhancing visibility and compliance control. Not to be confused with IaaS, by using Infrastructure as Code organizations can code and automate external and internal audits and compliance testing. It represents the next, more secure generation of infrastructure management.

Meanwhile, new possibilities are emerging for defusing the security risks of Advanced Persistent Threats (APTs). A combination of the nuke-and-pave approach, in which each workload has a lifecycle of only a few hours and 'canary testing' whereby deploying a new environment to 5%-10% of end users, the potential longevity and capability of any such threat is dramatically reduced.

Through 2020, public cloud IaaS workloads will suffer at least 60% fewer security incidents than those in traditional data centers [6].

[6] Gartner: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

The Atos advantage

Atos is Europe's number one security provider. Our customers enjoy the full benefits of our global network of 14 Security Operations Centers (SOCs), best-of-breed cloud security technologies and long-standing partnerships with major cloud service providers.

Atos is a trusted partner in securing legacy infrastructure and cloud operations. 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.

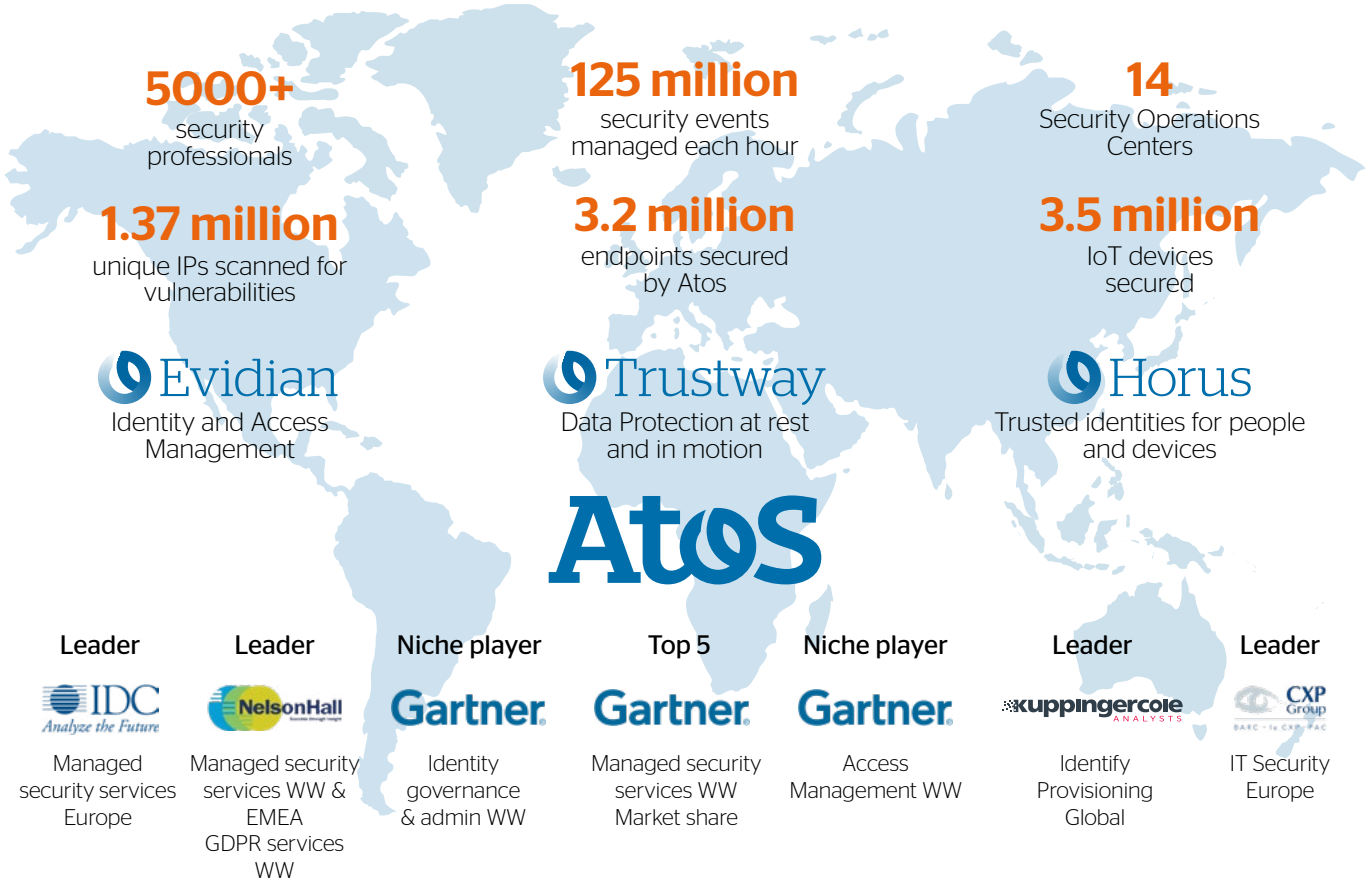
Cybersecurity is a critical part of the four offerings of our Digital Transformation Factory – Orchestrated Hybrid Cloud, Atos Business Accelerators, Atos Codex and Atos Digital Workplace. These offerings are supporting the digital strategies of customers around the world, providing them with a secure, scalable and open platform for growing their digital business ecosystem.

In everything that we do, our approach is distinguished by its underlying focus on business outcomes. We understand the risks faced by each business, customizing an appropriate cloud security strategy for each different customer. We work closely to diagnose threats, advise on investment choices and embed a culture of cyber maturity in our customers' operations and workforce.

Our approach is use-case driven and tailored to clients' specific needs. Whether you want to increase your visibility of shadow IT, comply with GDPR, enhance the security of your data, or predict new threats, we have the services and solutions you need.

Working with all the major Cloud Service Providers, we add an end-to-end layer of security control that covers all cloud environments as well as your on-premises infrastructure. We are also members of the Cloud Security Alliance (CSA), the world's leading organization dedicated to defining standards, certifications and best practices to help ensure a secure cloud computing environment

Deploying our own technologies on identity and access management and encryption and cooperating actively with leading technology companies such as McAfee, we help organizations reassert control over their data and we also provide critical support in the event of any incident.



Rising to the next challenges

Powered by cloud computing and automation, business technology is leaving behind the world of servers and data centers and entering an exciting but challenging new era. Enterprises need to adapt their security processes and technologies to keep up with these innovations and reap the benefits of a server-free world.

While many organizations are still coming to terms with the security implications of IaaS, PaaS, CaaS and SaaS, information technology is already moving into a new paradigm of Function as a Service (FaaS).

In the FaaS framework, which is now offered by all major cloud service providers, companies can run code and create microservices without the need to provision or manage server resources.

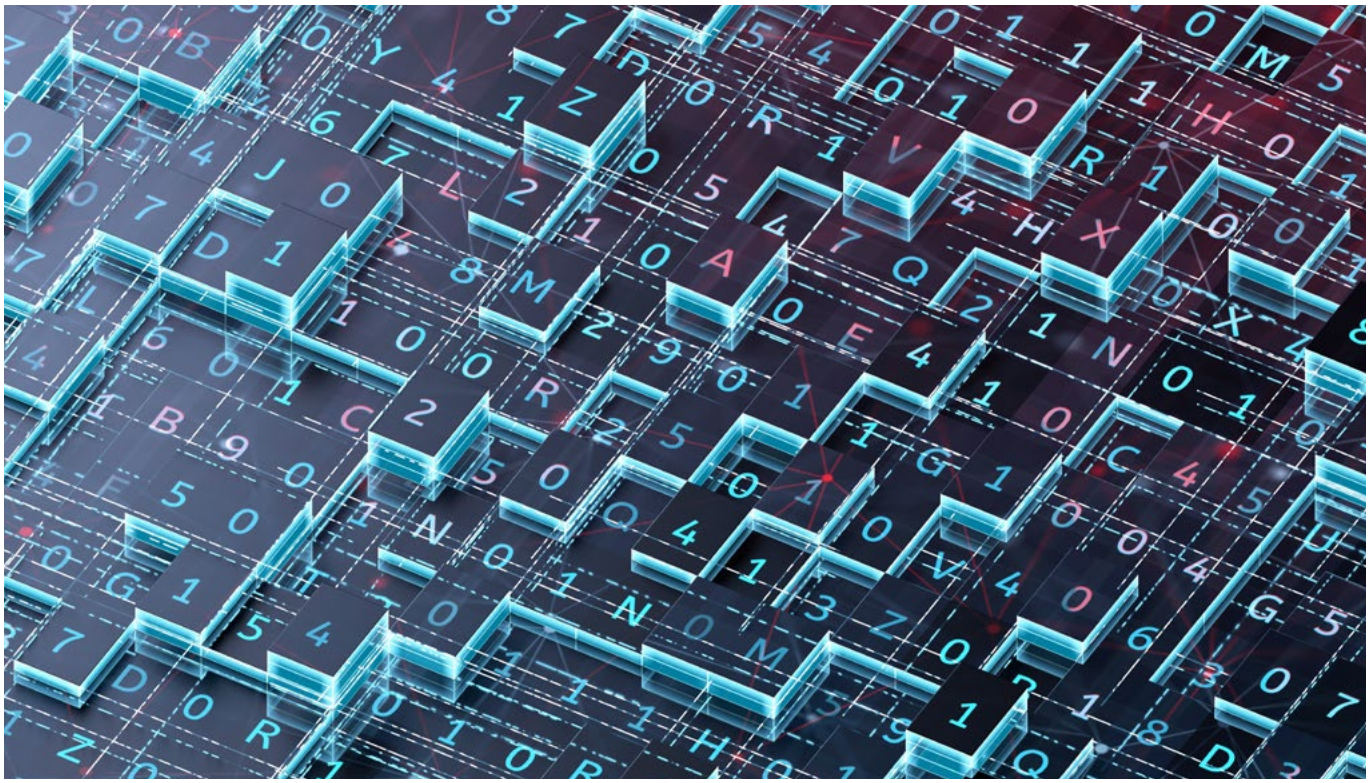
The security implications of FaaS and microservices are clear. This next generation of cloud computing increases the scope of the attack surface to an even greater extent than legacy cloud. In a serverless world, new approaches will be required to secure microservices. At the same time, FaaS may accelerate the evolution of DevOps into NoOps, potentially reducing the role of IT operations and raising new questions for security.

Meanwhile, new challenges are emerging, driven by the need for continuous delivery in application development and of a 'Shift left' mentality, in which security controls are integrated as early as possible in the development cycle. The rapid growth of the Internet of Things will exert even more pressure on security professionals to keep up with the pace of software development and innovation.

Organizations will need to find ways to maintain rigorous security controls even while optimizing their development and delivery lifecycles for speed. Some early adopters are pioneering a new DevSecOps approach, to introduce security early in the lifecycle, automating and embedding the appropriate controls into application development.

By undertaking secure by design approaches, in which source code is analyzed for flaws as it is developed, and open source libraries are checked for vulnerabilities during the development lifecycle, the DevSecOps approach is raising the bar for security. In addition to application security testing and software composition analysis, the emergence of DevSecOps could also transform compliance reporting, software development kits for IAM and encryption, and other frontline security challenges.

As the threat landscape continues to change, the security strategies of all organizations can expect to experience severe tests. Enterprises need a trusted security partner who can adapt to the changing environment and protect the full digital value chain. Only with a secure multi-cloud platform can businesses take full advantage of a new era in information technology.



A hybrid cloud security checklist

When reviewing the security profile of a hybrid cloud environment, organizations should consider the following questions.

- What type of cloud are you using (SaaS, IaaS, etc...)?
- Do you know where your data is stored?
- Do you know what type of data is stored in the Cloud?
- Are you dealing with personal data in the Cloud?
- What are the security & privacy risks applying to your organization?
- How about Shadow IT?
  - What visibility do you have on Shadow IT?
  - How do you control access to Shadow IT?
- Is your staff (internal/partner) "cyber aware"
- Are your current security controls providing sufficient visibility, context and insight to the threat facing your sensitive data across the hybrid cloud?
- How could automation reduce time taken to diagnose, react and recover from security incidents that could affect your hybrid cloud?
- Are you leveraging native cloud provider capabilities to their fullest potential to help you improve your security?
- How ready are your organization's leadership board, security and commercial teams to manage the consequences of a high-profile cyber attack?
- How well do you understand the cyber threat facing your organization, not just the data you process, but also the stakeholders you work with and the supply chain that you operate in?
- Taking account of GDPR, NIS and other regulations, are you investing in the right places to achieve the correct levels of security for how your sensitive data should be protected across the hybrid cloud?

Contributors

Vasco Gomes
Global CTO Atos Cybersecurity Products
Atos Senior Expert – Cybersecurity

Zeina Zakhour
CTO Cybersecurity
Distinguished expert Cybersecurity
Member of scientific community

Amo Matharu
Global Cloud Security
Programme Director

Vision paper

About Atos

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue of € 13 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies and industry knowledge, Atos supports the digital transformation of its clients across all business sectors.
The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, Unify and Worldline. Atos is listed on the CAC40 Paris stock index.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together

CT_190117_AS_BDS_Hybrid-Cloud-Vision-Paper