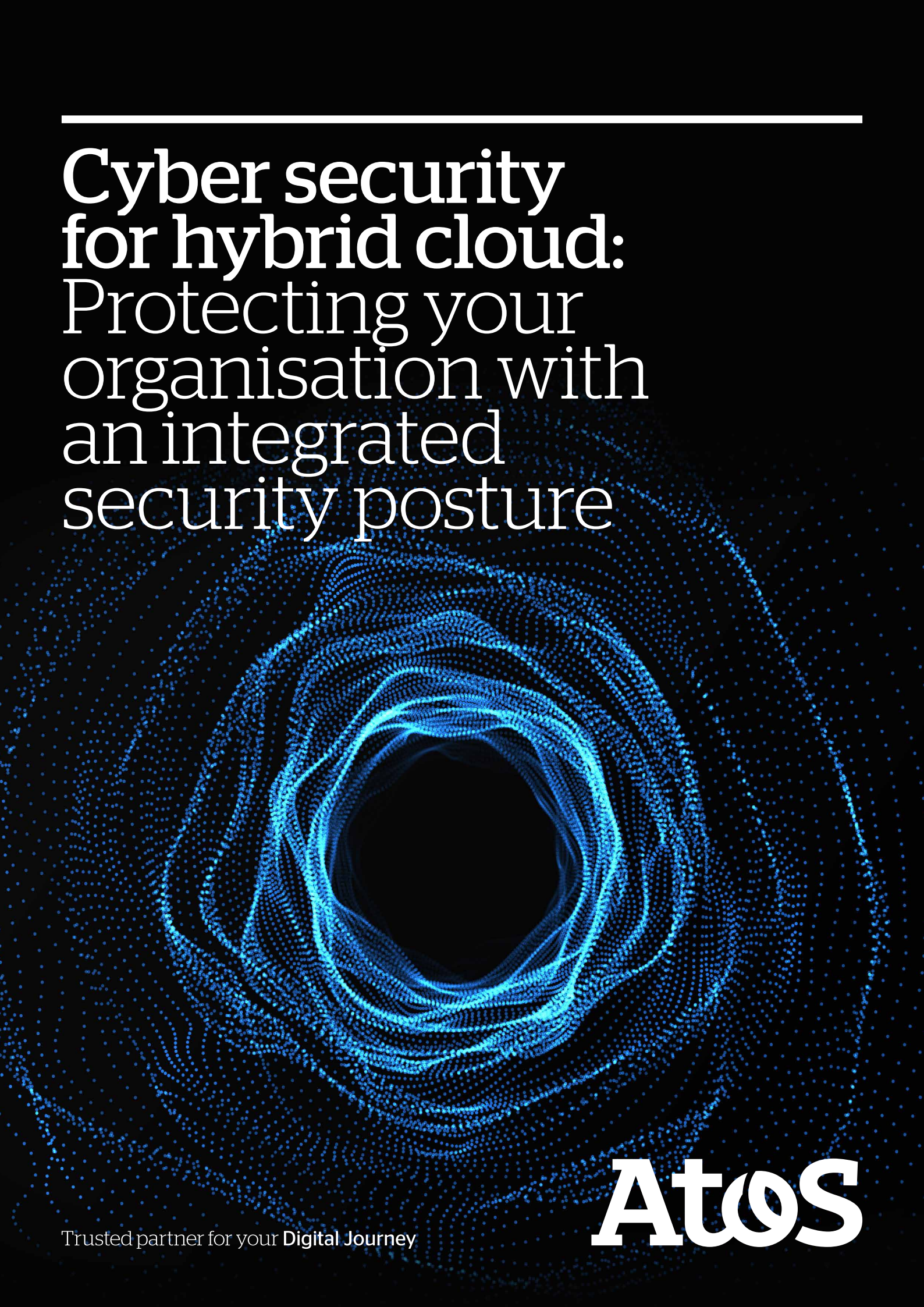
Cyber security for hybrid cloud: Protecting your organisation with an integrated security posture



Trusted partner for your **Digital Journey**

Atos

Executive summary

Organisations everywhere are using cloud services to drive a transformation in the way they operate. Many are well underway with their digital journey and investing in hybrid cloud as the best way to optimise their IT.

For hybrid cloud, while no additional security may be needed, integrating all security controls into one overall security posture is essential. And as the cyber threat evolves, cyber security must also evolve while acting as an enabler for digital transformation and innovation.

Atos' approach is to adapt and apply the National Cyber Security Centre's 10 steps to cyber security to the hybrid cloud environment. We help organisations invest in the right security controls in the right places quickly, while also laying the foundations for prescriptive security and future-proofing IT infrastructures as artificial intelligence technologies advance. Soon, innovative processing methods, such as edge-based processing and swarm computing will hold the keys to efficient computing. This must be combined with very rapid threat diagnosis and context-aware interpretation so that organisations can monitor, predict and pre-empt cyber threats as they emerge.

About this document

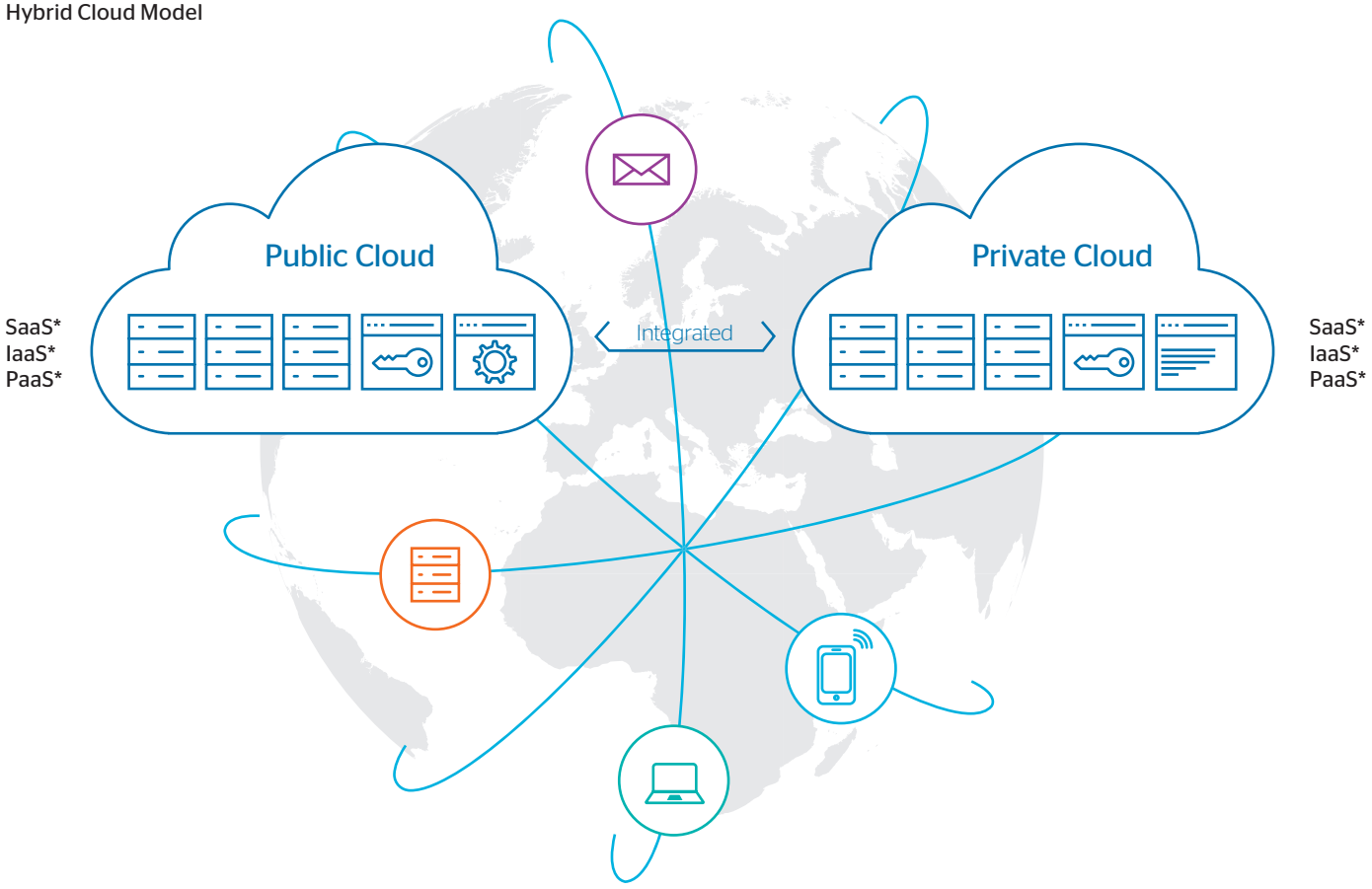
This document is for business leaders and technical decision-makers. It provides insight and guidance for any organisation at any stage of the journey to hybrid cloud. On page 03-05 is an overview of the cyber security challenge and why organisations need to take action.
On pages 06-09 you'll find more detailed guidance on Atos' approach and which controls and technologies to apply for an effective cyber security posture that protects and supports your business.

Context: cyber security on your journey to hybrid cloud

Supported by hybrid cloud, digital transformation enables organisations to reinvent their business models and realise multiple benefits, from forging better relationships with customers, to sharing and using more information in real-time, to taking significant costs out of their operations. Using cloud, CIOs can spend more of their IT budgets on business outcomes, with agile technology infrastructures that are virtualised in cyber space.

For any organisation, reaping all the benefits of cloud requires a robust approach to cyber security to protect data that is shared across public and private cloud environments at an acceptable cost.

Hybrid Cloud Model



Sensitive data is produced by, collected from and shared everywhere.
They key is protecting the data whilst enabling it to be used where needed.

* Software as a Service
* Infrastructure as a Service
* Platform as a Service

An evolving cyber security landscape

What started as a simple extension of traditional security principles into the cloud has become more complex with new and incumbent cloud vendors launching competing, siloed cloud security technologies and controls.

For any organisation, it is critical to bring all these technologies and controls into an integrated security posture rather than maintaining standalone applications and data in siloed cloud environments.

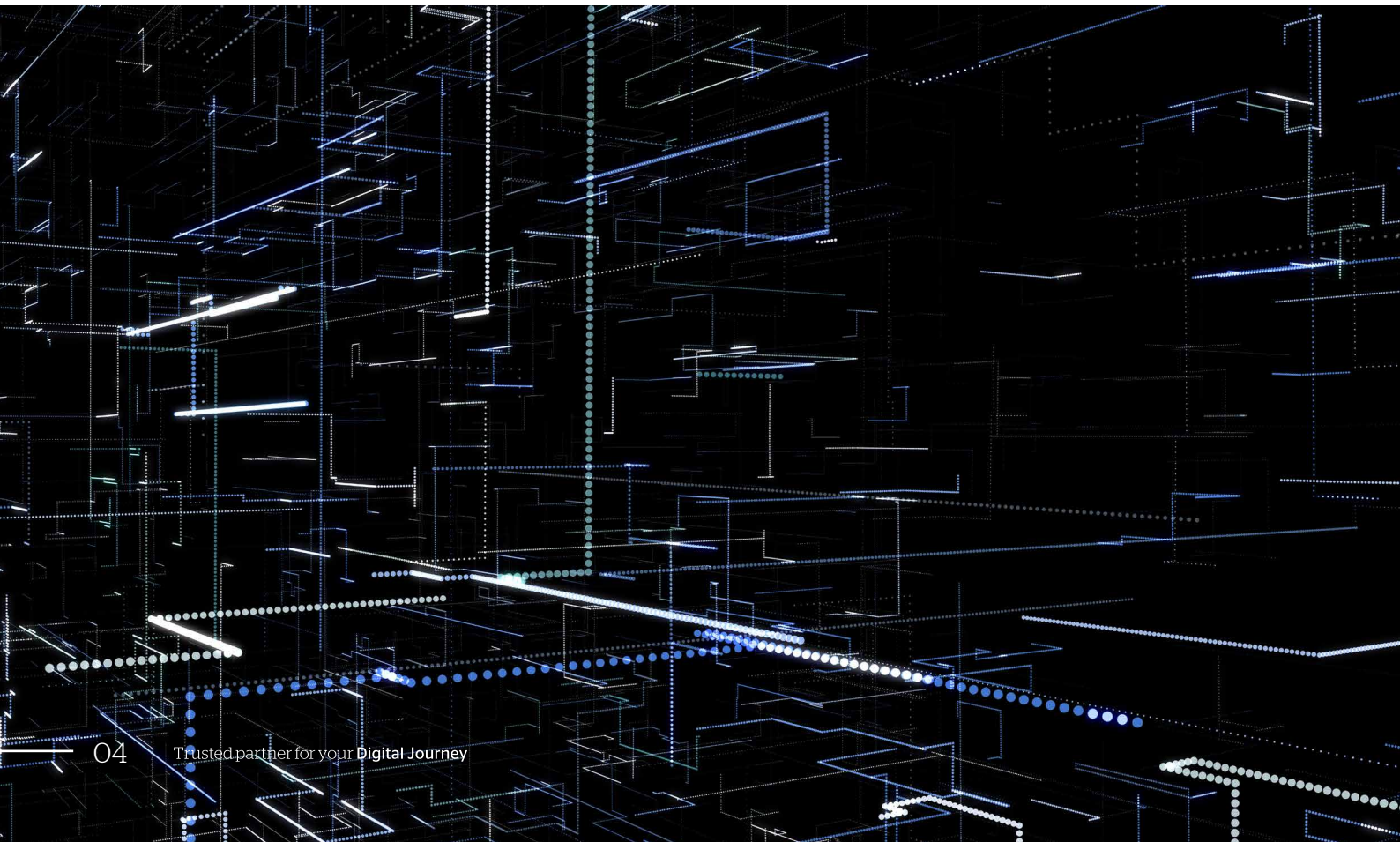
Recent world events have resulted in a step change in the cyber threat environment since tools more commonly associated with state actors (WannaCry) are now in the hands of anyone who is skilled in using IT. This means that the threat facing cloud services has morphed considerably. Now, there is significant risk not only from any compromise of the cloud infrastructure itself, but also from other services that may be running on that platform. Cyber attackers can jump between cloud service providers and their customers using 'supply chain' infiltration techniques. Whilst the attack vector itself may not be particularly sophisticated, being able to detect signs of such an attack across several systems connected by a hybrid cloud architecture does require up-to-date, relevant security measures.

At the same time, General Data Protection Regulation (GDPR) puts obligations on all organisations; and the Directive on security of network and information systems (the NIS Directive) sets out requirements for Critical National Infrastructure organisations to ensure the security and resilience of their network and information systems.

Value of cyber trust

As cyber crime increases, people are becoming more wary of organisations who might fail to protect their data. To look more deeply at the value of cyber trust, Atos commissioned a survey of over 3,000 citizens who use UK businesses and public services. What the survey revealed is that customers are looking to organisations to do more to win and retain their trust, that they are willing to trade some aspects of their user experience for the sake of improved cyber security controls, and that increasingly they see cyber security as a differentiator when choosing which organisations to interact with online.

For more on the research, see The currency of cyber trust: your customers' attitudes towards cyber security at atos.net/cyber-research-uk



Your cyber security challenge

Just as having a powerful engine doesn't necessarily make for a fast car, having the right security controls isn't enough if your organisation isn't protected by a single security posture.

This is especially important for hybrid cloud environments in which combinations of software, platforms and infrastructure as-a-service offerings are endless.

Balancing security and business need

In a digital environment, sensitive data is produced by, collected from and shared everywhere. Your challenge as a business leader is to ensure there is enough security in place for the secure sharing of sensitive data within and between different cloud environments in line with the needs of your business.

To succeed, it's important to understand how your organisation will make use of cloud and identify every aspect of that way of working; for example, agreeing how cloud will change your technology landscape and the digital functionality that your employees and customers expect. These aren't just security or even technology issues; they are business decisions on how to achieve a balance so that cloud-based IT systems are secure and users get the benefits they were promised from digital.

Get functionality wrong and users will feel short-changed. Under-cook security and face legislative censure, reputational damage, severe financial penalties and loss of stakeholder confidence.

Overview: what do you need to protect?

Data and data-flows. Given the amount of external cloud based services now available and the persistent use of shadow IT (IT assets that are deployed locally without central authorisation), organisations must understand and control the data flowing between users and the cloud services they access. For example, did you know that your organisation may be contravening the Payment Card Industry Data Security Standard (PCI-DSS) and GDPR legislation if your employees are using webmail or a local file-sharing site whilst working at home to access sensitive personally identifiable information such as account numbers or payment card details?

Users and user activity. Fine-grained monitoring of user activity in accordance with policy will find signs of insider threats, malicious or otherwise. Many organisations now invest in Identity and Access Management (IDAM) solutions to safeguard identity information and automate how users access the resources they need. Privileged user analytics measure the threat from dormant user accounts, inappropriate permissions, unexpected escalation of user privileges and creation of new user accounts to identify potentially suspicious behaviour.

Applications. Organisations must demonstrate that data is stored, processed and analysed both within and between applications stored across hybrid cloud environments in accordance with company policy and prevailing legislation. Both the content of data and the context of how it is used are together relevant to understanding an organisation's specific cyber threat.

IT infrastructure. Gathering security logs from IT and physical equipment such as workstations, mobile devices, servers, print logs, Wi-Fi networks and building access controls systems is a useful start. Next, analysing this data to proactively look for patterns of interest is important. This is particularly demanding of resources when done manually, so investing in machine learning to profile what constitutes normal and potentially abnormal behaviour is worthwhile.

Implementing cyber security controls for hybrid cloud

The National Cyber Security Centre (NCSC) has released guidance, called the 10 steps to cyber security, on the minimum approach that should be taken to protect any hosted infrastructure or service.

Atos' approach is to apply the 10 steps to cyber security for a hybrid cloud environment. Each step is associated with specific security controls. In a hybrid cloud environment, we focus on deploying the following controls into each workload environment:

- **Step 2.** Network security – control and inspection of traffic flow on the boundary as well as between workloads, or even individual hosts
- **Step 4.** Malware prevention – monitoring for anomalous activity on the workload through passive signature detection or advanced pattern detection methodologies
- **Step 9.** Home and mobile working - encryption – safeguarding access to corporate infrastructure by encrypting data either at rest or in transit for both structured and unstructured data
- **Step 6.** Secure configuration – ensuring that each workload is configured securely and remains secure through its lifecycle
- **Step 10.** Managing user privileges – identifying and managing users and their privileges to ensure that only the right people get the right level of access at the right time.

Regular test and rehearsal

The National Cyber Security Centre (NCSC) recommends regular testing of an organisation's security defences. Taking this further, Atos recommends that organisations undertake an end-to-end assessment of their ability to correctly diagnose, respond to and recover from attack. This approach, called 'red teaming' carried over from the military, subjects the organisation to a real-life attack and tests its ability to survive a serious compromise to its cyber resilience. This is best deployed across the whole organisation, involving cloud service providers, in-house IT, business and security stakeholders, together with all IT suppliers as a single coordinated exercise.

Consolidating the output to implement Prescriptive Security

By consolidating the output of all these steps into a single security lifecycle, it is then possible to implement Prescriptive Security by introducing advanced analytical techniques and automation.

Prescriptive Security combines data from the individual systems applying the security controls such as Identity and Access Management or a Security Information and Event Management (SIEM) system for aggregation into a single monitoring (step 8) capability. This is then combined with up-to-date threat intelligence and next-generation machine learning to detect the early signs of suspicious behaviour across this consolidated view and enable incident management (Step 9). Finally, artificial intelligence and service management tooling are used to automate the investigation and resolution of potential security events; where needed, this is combined with the judgement of an experienced person to ensure the necessary levels of decision support.

From here, we can layer process and policy to manage the remaining steps and controls such as user education and awareness (Step 3) and home and mobile networking (Step 7), with a view to providing effective risk management (Step 1).

Cyber Security Maturity Model
(based on NCSC Ten Steps to Cyber Security)

Which technologies are needed?

Atos and Google Cloud have a global partnership to deliver a secure hybrid cloud fully compliant with European and global regulation and in line with customer demand on critical data localisation. In hybrid cloud environments, there are three key consumption models: Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

If your consumption model is centred around SaaS, your challenge will be to **protect data and manage user access and privileges.**
If you consume multiple IaaS or PaaS platforms, in addition to securing legacy data-centre estate, your challenge will also be to **protect both the infrastructure and workload of the environment.**
In a complex hybrid cloud environment, you may need to address both these challenges.

Protecting data and managing user access and privileges

If your challenge is purely around controlling access and data to SaaS cloud services on the internet, such as Google Drive Office 365, Sailpoint and DropBox, you can achieve this using a Cloud Access Security Broker (CASB).

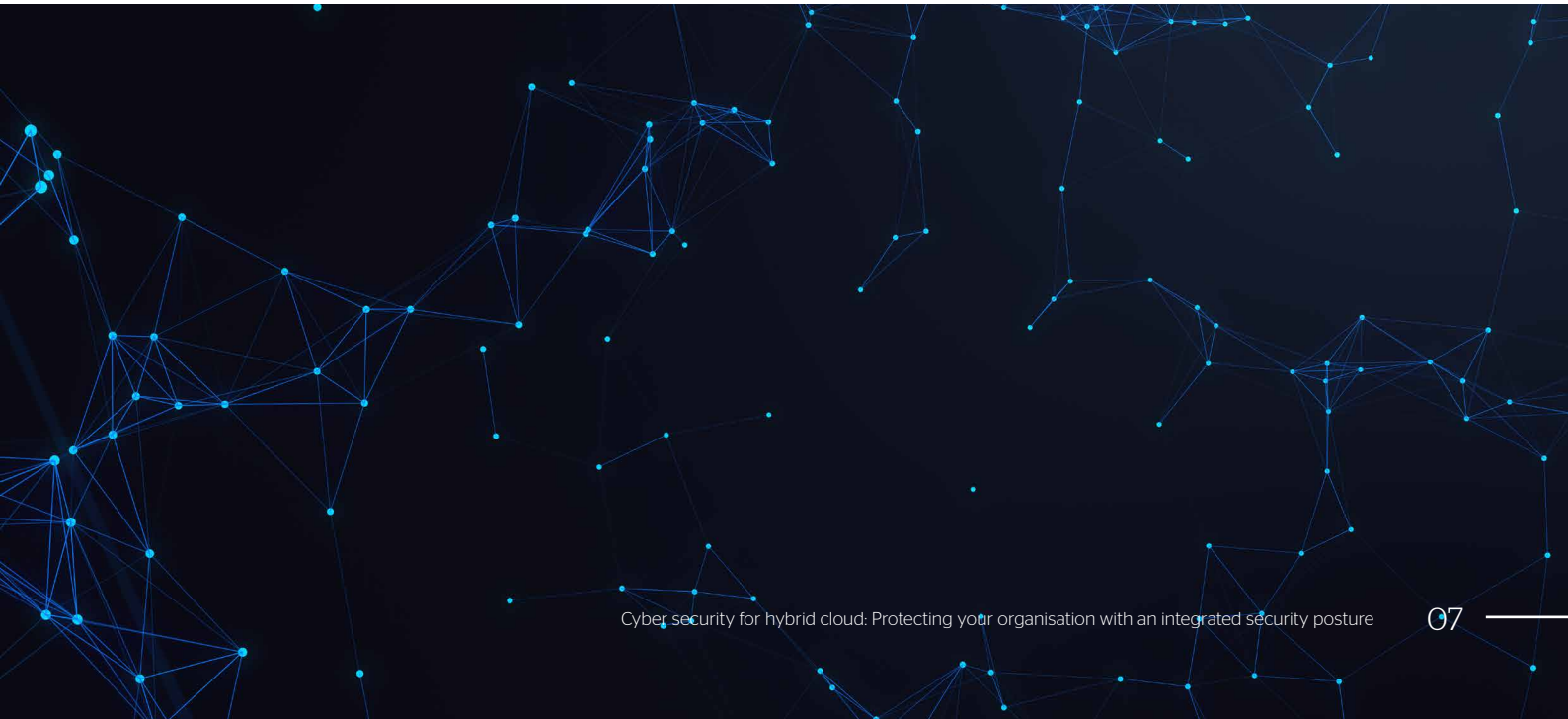
CASB platforms are brokers that sit between your users and the services they are accessing. These solutions enable you to implement fine-grained Identity and Access Management (IDAM) and Privilege Access Management (PAM) policies through the Application Programme Interface (API) interactions with third-party cloud services, effectively controlling who can access what and which actions they can perform. They can also be used to enforce data migration controls through Data Loss Prevention (DLP) services, as well as providing insight into which cloud services are in use through your entire organisation (grey IT).

Most CASB platforms will also enable you to reduce some of these controls to other implementations if required, enabling integration with existing deployed services such as DLP and IDAM.

Some platforms will also give you visibility of user activity over time, enabling a certain level of user behaviour analysis, effectively establishing a baseline and alerting on what can then be identified as anomalous behaviour.

In most cases, CASB technology can itself be provisioned as SaaS from the cloud, resulting in little or no impact on the IT estate or the services it protects.

Finally, the security log feeds from deployed security controls, workload elements and underlying provisioned hypervisor/public cloud platform can be sent back to a single monitoring platform. This allows for a holistic and dynamic view of the hybrid security estate to enable you to monitor and respond to threats both inside and out.



Which technologies are needed?

Atos and McAfee: securing hybrid cloud environments, seamlessly

Given the investment that organisations have already made in security, it is important that, where possible, this is either moved to the cloud or replicated as part of a hybrid solution. This means organisations benefit from cloud ways of working without reinventing new ways of safeguarding sensitive data.

While IT must be able to identify, control and protect data in the cloud, this doesn't always mean implementing strict yes/no policy rules. Instead, more nuanced decision-making should be applied which adheres to the current risk landscape, incorporating technologies such as data loss prevention, anomaly detection, collaboration control and device/user granular policies.

Visibility of exactly what data is held in the cloud and which applications employees are using to access this data is essential. McAfee's Skyhigh Security Cloud, as a Cloud Access Security Broker (CASB), provides this across all cloud services (SaaS, IaaS or PaaS) and provides organisations with the right information to enforce policy.

Despite the increasing prevalence of cloud-first IT programmes, most cloud applications used by companies fall into the shadow IT category, potentially putting sensitive data at risk. Companies can alleviate these risks by using a CASB to gain visibility and control of shadow IT whilst maintaining employee productivity. This goes beyond informing Security teams on how much traffic is routed via a certain cloud service, to being able to provide a risk score associated with the behaviour of each service so the organisation can make intelligent policy-making decisions. Armed with this information, clients can see what data is being shared with third parties via the cloud, and then take the required action based on this insight; for example, an employee is sharing information with someone via a cloud service with a Gmail address: is this a threat?

A perfect cloud partnership

Moving to a hybrid cloud environment shouldn't be hampered by process or security concerns. With the right technology and partner to support the transition, the end result is not only a more efficient working environment, but a more secure one too.

Atos' expertise in McAfee's CASB technology enables companies to make hybrid cloud management and security a more seamless experience. Atos has the skills, knowledge and capability not only to understand a company's individual infrastructure and deliver cloud-based services tailored to that organisation, but also to provide up-to-date insights on bleeding-edge cloud technology.

Protecting the infrastructure and workload environment

The controls involved in protecting the workload environment are more traditional security controls, focused on securing the boundary, the server and the data. In a single vendor cloud environment, many of these controls can be provisioned and utilised from the vendor platform without having to deploy additional third-party technology. In a hybrid cloud environment, the challenge is to deploy multiple security controls across multiple cloud vendors whilst ensuring a single point of management and policy control.

To meet this challenge, vendors offer next-generation technologies that can be installed across multiple virtual cloud environments as well as physical deployments whilst still being controlled from a single management platform. When augmented by cloud orchestration tools and Security DevOps techniques, this means that security controls can be deployed and configured automatically so that highly changeable or containerised workload environments can be serviced.

Using this next-generation tooling and the principles of the NCSC 10 steps to cyber security, Atos' approach is to:

- Protect data flowing both north and south (between environments) and east and west (between workloads held within environments)
- Implement micro segmentation to tightly control host-to-host data flow within workloads
- Provide whole life encryption (virtual/database/in motion and at rest), linking back to an external key management system allowing for single point of key management across multiple environments
- Install signature or derived activity-based anti-malware controls on servers
- Deploy network and host data loss prevention to ensure secure data management in accordance with policy, industry regulations and government legislation.

From here, Atos can then overlay Identity and Access Management (IDAM) and Privilege Access Management (PAM) solutions, deployed centrally to provide unified user access and privilege control across multiple cloud platforms and legacy estate. Again, these services can themselves be consumed as cloud services.

How does this work within the security lifecycle

To maximise the economic advantages of a hybrid cloud environment, both server and application estate should quickly scale up and down. In addition, servers and applications are likely to be provisioned within fast timescales, typically within a few minutes of users requesting new servers or applications.

This raises a number of challenges from a security viewpoint:

- **When a server or application is provisioned,** it must be automatically configured into the security systems such as event log management, vulnerability scanning, automated incident systems and compliance reporting. If this is not done using automated service provisioning tooling there may be 'blind spots'. Due to the speed of change, manual steps will not suffice. Automated verification is needed so that the servers are successfully provisioned into the security tooling before being used. This must include the successful application of patches, system lockdown and removals on non-required deployment accounts and tools. Mechanisms must also be in place to defend servers from attack whilst in the provisioning phase as they may be insecure for a short time.
- **Equally, when a server or application is de-provisioned,** it must be automatically removed from the security systems described above. This prevents the altering and/or reporting against devices that no longer exist in an environment which in turn delivers cost-efficiency in service licensing. Here, accuracy is critical to ensure correct monitoring of relevant infrastructure and up-to-date records for compliance purposes.

It is critical that security services are fully included in infrastructure automation systems to ensure timely successful instantiation of service when a server is provisioned, prompt servers are removed from systems when de-provisioned.

Finally, in a modern hybrid cloud environment, Atos would recommend that services be supported using a Security DevOps arrangement to ensure that the business benefits of cloud can be realised. This means that security is managed throughout the IT estate, with security controls tailored to suit digital ways of working and provide the visibility and automation capability relevant to the hybrid cloud environment in use.

Securing data cost-effectively

Different kinds of data have different levels of sensitivity in terms of commercial value, personally identifiable information, intellectual property, regulatory compliance requirements, or government or organisational protective marking scheme requirements.

Appropriate security levels at optimum cost

One advantage of hybrid cloud is being able to select and combine differently-priced public, private and on-premise cloud services to ensure that each piece of data is managed at the appropriate level of security and therefore at optimal cost. This entails balancing data sensitivity, risk appetite and cost.

Until recently, levels of security baked into commercial cloud offerings were pre-determined by the provider and usually listed in inflexible option packages. Today, more bespoke additional security layers (including your chosen encryption) make it possible to customise security controls to the cloud environment. The key question then becomes, what goes where.

Integrating security controls required for each type of cloud

Previous concepts of allowing data to flow only upwards in security terms, with 'read-only' access downwards, are not sophisticated enough for a hybrid cloud. More dynamic security controls are needed, not just to secure data within each cloud environment, but to manage the relationships between different cloud services.

Organisations need to know their data, where it's located and its level of sensitivity so that they can decide which 'flavour' of cloud is appropriate for each data set (always remembering that if data of different levels of sensitivity is mixed, then the entirety must be treated at the highest level of security). This data classification process is also fundamental to meeting the requirements of GDPR.

In a hybrid cloud, it is also essential to manage the relationship between each constituent cloud environment (plus any legacy infrastructure). Security controls applied to each environment are likely to vary (often significantly). What's more, data needs to transfer between environments with the associated upgrading or downgrading of sensitivity levels. This requires the frictionless flow of data between each cloud services to that sensitive data doesn't find its way to an inadequately protected environment and highly secured environments don't fill up with data that could be stored more cost-effectively elsewhere.

Checklist for organisations

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

- ☐ How well do you understand the cyber threat facing your organisation, 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 and NIS, 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?
- ☐ 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?
- ☐ How ready is your organisation's Leadership Board, security and commercial teams to manage the consequences of a high-profile cyber attack?

Why Atos?

Atos is **Europe's number one security provider** operating 14 24/7 Security Operations Centres (SOC) worldwide, providing cyber security services to national and global clients across all sectors. Atos is a trusted partner and digital services leader delivering end-to-end security advice, support and solutions. This means:

Relevant security, tailored to your security risk. Given the wealth of technical material on the cyber threat, threat actors and their motivations, understanding what this really means for your organisation can be a challenge. Atos can work with your senior team to diagnose the threat you face and the associated business risk, advise on investment choices and embody a culture of cyber maturity into your people and ways of working.

Resilient services based on evergreen technology. We design, build and run security as a service to keep up with the latest technologies so you don't have to. This delivers enterprise-grade security leveraging existing investments in areas such as service management based on ServiceNow to deliver value for money.

Improved confidence. A partnership with Atos means effective support in good times and bad. You will have visibility of what really is happening in your network, insight into how this affects your sensitive data and practical help in the event of compromise.

What's next?

If you'd like to talk about your cyber security challenge or how Atos can help, contact us at **ukwebenquiries@atos.net**

Lexicon

Application programme interface (API) – Routines and tools for building software applications, which specify how components should interact.

Cloud access security broker (CASB) – A CASB platform is a software tool or service that acts as a broker, sitting between your users and the services they are accessing. The CASB allows an organisation to extend the reach of their security policies beyond their own infrastructure.

Data at rest – Inactive data stored on a device or network, sometimes thought to be less 'at risk' than data in motion.

Data in transit – Data which is in motion, or being transferred between two entities.

Data loss prevention (DLP) - A method for preventing a data breach by monitoring, detecting and blocking sensitive data in use, and making sure end users don't transfer sensitive data outside of the network.

Edge computing – A method of improving cloud computing systems by processing data near the source, i.e. at the edge of the network. An example of this could be data produced by a wind turbine or a traffic light system.

Encryption - A process to convert data into code that conceals the data's original meaning to prevent it from being accessed, understood or used.

Evergreen technology – IT which is comprised of components which are updated frequently.

General Data Protection Regulation (GDPR) – EU data protection and privacy legislation implemented on 25 May 2018.

Infrastructure as a Service (IaaS) – Outsourcing infrastructure requirements, such as a server or storage requirements, and accessing virtualised computing resources over the internet.

Machine learning – A form of artificial intelligence that allows the cognitive learning of computing equipment, without being explicitly programmed.

Micro segmentation – Splitting up of a unified system, such a as a network, into smaller isolated segments to tightly control host-to-host data flow within workloads.

NCSC -The UK's National Cyber Security Centre, part of GCHQ, established to enable the UK to manage the cyber threat.

NIS Directive – The EU directive on security of network and information systems, which sets out requirements for critical national infrastructure organisations to ensure the security and resilience of their network and information systems.

Passive signature detection – Recognising bad patterns or threats, and acting in a passive manner, for example simply monitoring and notifying.

Platform as a Service (PaaS) – A category of cloud computing, where hardware and software, typically those needed for application development, are outsourced and accessed over the internet. This provides a platform for customers to develop, run and manage applications.

Predictive Security: Capability that analyses network traffic to identify potential threats.

Prescriptive Security: Capability that uses machine learning and artificial intelligence to identify a potential issue, and then acts to prevent the threat developing.

Red teaming – A term carried over from the military, when an organisation is subject to a real-life attack and tests its ability to survive a serious compromise to its cyber resilience.

Security DevOps – Including security checks and procedures throughout the software development process.

Security Incident Event Management (SIEM) - Tool or function that collates and analyses log data coming from a variety of sources to help manage security threats.

Shadow IT – IT assets that are deployed locally without central authorisation or knowledge.

Software as a Service (SaaS) – A software licencing and subscription model, where a 3rd party hosts the software centrally and provides it over the internet, in exchange for a monthly cost.

Structured data – Data in a standardised, organised format to provide information or classify contents.

Supply chain infiltration techniques - Cyber attackers can jump between cloud service providers and/ or their customers, damaging an organisation by targeting less secure elements in the network.

Swarm intelligence – A form of artificial intelligence which is similar to the behaviour of swarms of social insects. Swarm refers to loosely structured, decentralised self-organised systems.

Unstructured data – Data which is not organised in a pre-defined manner, usually text heavy but can be in many formats.

About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 73 countries and annual revenue of around € 13 billion. The European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, The Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

Find out more about us
atos.net

Let's start a discussion together

CT_J749_180504_RY_B_CYBERSECURI