CLOUD SECURITY ALLIANCE CONTRIBUTION TO THE EUROPEAN COMMISSION STRATEGY ON CLOUD COMPUTING

8 November 2011

FOREWORD

CSA would like to thank the European Commission for this opportunity to contribute to the European Commission's effort to make the European Union cloud "active" through the cloud strategy, and we would like to offer our contribution though both the already freely available best practices and research results, and with our expertise getting involved in the EU-funded projects.

With our best regards,

Daniele Catteddu Jerry Archer Dave Cullinane Nils Puhlmann

Alan Boehme Paul Kurtz Jim Reavis

The Cloud Security Alliance Board of Directors

ACKNOWLEDGMENTS

Main Authors

Jim Reavis, CSA Executive Director
Daniele Catteddu, CSA Managing Director EMA

Contributors

Kevin Fielder
Francoise Gilbert
Henry St. Andre
Raj Samani
John Howie
Cornelia Kutterer

CLOUD SECURITY ALLIANCE CONTRIBUTION TO THE EUROPEAN COMMISSION STRATEGY ON CLOUD COMPUTING

Cloud Security Alliance

The Cloud Security Alliance (CSA) is a not-for-profit, global organisation with a mission to promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders[1] (https://cloudsecurityalliance.org/membership/corporate-members/).

Contribution to European Commission Cloud Strategy

While cloud computing represents the advent of a global computing utility that transcends national boundaries, we believe a number of positive actions can promote EU interests and protect its citizens while leveraging cloud computing's benefits to its fullest. Through this paper, CSA would like to propose its contribution to the EC strategy for cloud computing by suggesting short- and medium-term actions that support a secure adoption of cloud computing across the EU.

The actions we propose refer to the particular areas of:

1. Interoperability and portability
2. Trust, security, and assurance
3. Security innovation in the cloud

Our proposals should be understood in the context of the CSA focus on security, assurance, and compliance.

1.0 Interoperability and Portability

To foster interoperability and portability we suggest, as a main strategic action, the use of public procurement to catalyse broader cloud adoption, and in such procurement to avoid vendor lock-in by following the guidance on openness in the European Interoperability Framework and utilizing available open standards.

[1] CSA has 16 employees, 26,000 individual members, 100 corporate members and 50 chapters worldwide. In the course of three years, we have released 12 research project reports, a cloud provider registry, and the only user certification related to the security knowledge of cloud computing. All of our research work products are the result of global collaboration and are provided at no cost and royalty-free to any organisation who wishes to use them (https://cloudsecurityalliance.org/about/). CSA currently has over 8,000 individual members and 10 chapters in the EU; our first official chapter worldwide was in Spain. CSA will establish a legal entity in the European Union in 2012. CSA EU chapters will continue to work collaboratively and independently to address cloud security issues within the EU and individual member states.

Based on our experience in supporting and collaborating with bodies such as the United States' federal government and NIST, we recognize that the public sector plays a crucial role in leading the adoption of cloud computing, especially in the presence of a geographically fragmented market with an inconsistent legal framework, relative market immaturity, lack of user awareness and information, resistance to change, and lack of explicit and structured requirements.

In CSA's opinion, the European public sector could catalyse cloud adoption by initiating a number of actions such as:

- Developing a standard framework and guidelines for service and data asset classification, which could be used to reflect the different levels of service criticality and the sensitivity of data processed by each service to help customers decide which services and data can be moved in which type of cloud (public, private, et cetera).
- Defining for each category of service and data assets which use cloud computing requirements for data security, privacy, portability and secure deletion that cloud providers should follow to support consumers who wish to use and eventually terminate their service.
- Designing models for cloud bursting (the dynamic deployment of a service that runs on internal organisational compute resources to a public cloud to address a spike in demand).
- Developing and publishing guidelines, checklists or "buyer's guides", as well as templates for Service Level Agreements (SLAs) and Request for Proposals (RFPs) for common, non-customized services.

In this paper, we point our attention to the definition, consolidation, and standardisation of policy syntax, baseline security, resilience, and privacy parameters and measures which are key tools for maintaining control over the process of cloud services portfolio management.

We propose to the EC to start working on the following short-term priorities:

- Interoperability of security policy
- Security service level agreements
- Privacy level agreements
- Security as a service
- Promoting the use of open standards

In CSA's opinion, an approach (led by public procurement and based on standardisation) in the public administration domain of security policies formats, SLAs, security measures and security level agreements, privacy level agreements, as well as non-security and resilience-related requirements could represent a way to overcome the lack of solid technical standards for interoperability and portability.

The European market, mainly composed by micro, small, and medium enterprises, will greatly benefit from this approach, as they could use public procurement processes as a terms of reference in identifying appropriate cloud services and/or service providers for potential use.

This approach will also positively impact the Cloud Service Providers (CSPs), as it will lead to a clarification and definition of the requirements of potential customers within the public sector and Small and Medium Enterprises (SMEs). This will allow cloud service providers to further invest in the development of cloud offerings based on these explicit requirements.

1.1 Interoperable Security Policies and Measures

Organisations transpose their security and resilience requirements into their organisational and technical security policies, which are then translated in their information systems into security configurations and settings, such as privilege assignments, authentication/authorisation rules, firewall rules, logging scope and levels, data labelling, et cetera

When organisations migrate to the cloud, from cloud to cloud, or participate in a cloud community or federation, or when cloud bursting is required, it becomes crucial to be able to port these settings and configurations consistently and rapidly into the new environment. It is also crucial that policies and settings requested by the cloud users do not conflict with new hosting environments (e.g., a public cloud) or with the rules of the community-federation. (Moreover, cloud users may be given control over control policy execution, in some cases through continuous monitoring.)

Policy interoperability is of paramount importance also when establishing mutual aid and assistance plans for emergency situations (e.g., a partial or total failure of a large scale cloud, for instance, a private government cloud). Mutual aid agreements could represent an important tool for improving cloud resilience, but the interoperability of security policies and measures is a precondition.

In our opinion, interoperability of security policies and measures is also necessary for the implementation of consistent data governance and accountability across the different cloud layers and vertical supply chain.

Cloud computing, despite its simple pay-as-you-go philosophy, introduces a complex service supply chain, interconnected and interdependent systems, as well as the need for orchestration across many providers, which force CSPs to support automation to effectively and efficiently manage internal security policy as well user policies and settings. For automation, machine-readable policies based on standardised policy syntax are needed.

For these reasons, we suggest supporting the standardisation of security policy syntax and basic settings. Results can be achieved by leveraging:

- Resources internal to European and national institutions. For instance, through the constitution of an expert group composed of information security officers in national and European public administrations to collect requirements, policy syntax, and define the framework for policy interoperability.
- The research program framework. For instance, by developing projects on security policy management automation.

Once cloud standards are in place, we suggest providing guidance to potential cloud customers on aligning their internal policies with the agreed-upon cloud security policies where possible or applicable.

1.2 Security Service Level Agreements

Service level agreements are an important way for potential cloud users to evaluate the level of service offered by the cloud service provider.

Besides performance measures, modern SLAs must also take into account security and resilience parameters; they should be able to define the level of security and resilience a provider is willing to offer.

It is clear that it is not a trivial task to create SLAs, and more specifically security service level agreements (SecSLAs), which are able to:

- Reflect security and resilience parameters
- Offer quantitative and comparable measures for reporting parameters (for instance, how availability is defined? are availability metrics of 2 different providers comparable? do they refer to hourly, daily, monthly or annual availability? and so on).

Some good initial work has been already done in the identification of security and resilience parameters in RFPs and SLAs for cloud services: for instance, ENISA has published a report early this year about this subject (Security and Resilience in Governmental Clouds), NIST published draft recommendations, and there are established industry security frameworks such as the CSA Cloud Controls Matrix and the Common Assurance Maturity Model (CAMM).

We suggest that this existing work is leveraged to develop standardised templates for RFPs and SLAs, which can be offered as guidance to EU member states as baseline parameters. In particular, we recommend the proposal of different baselines according to the criticality of the service to be offered or procured and the sensitivity of the information trusted to these services.

1.3 Privacy Level Agreements

Privacy is one of the top concerns for potential cloud customers. Both CSPs and potential users struggle with different data protection inconsistencies within the EU, which creates barriers to a broad adoption of cloud computing within the EU.

We suggest the introduction of baselines for compliance to data protection legislation and best practices by defining a standard format for Privacy Level Agreements (PLAs) and standards, through which a cloud service provider declares the level of privacy (data protection and data security) that it sustains for the relevant data processing.

We believe that privacy level agreement templates can be a powerful self-regulatory harmonisation tool and could obtain results that are difficult to obtain using traditional legislative means. Moreover, we see the PLA as:

- A clear and effective way to communicate to (potential) cloud customers the level of data protection compliance of a CSP (see paragraph on “Transparency and Assurance”).
- A tool to assess the level of compliance of a CSP with regards to data protection legislative requirements and best practices.
- A way to offer contractual protection against possible financial damages due to lack of compliance.

1.4 Security as a Service Standardisation

Cloud customers are both excited and nervous at the prospects of cloud computing. They are excited by the opportunities to reduce capital expenditure, as well the opportunity to divest infrastructure management and focus on core competencies. Most of all, they are excited by the agility offered by the on-demand provisioning of computing resources and the ability to align information technology with business strategies and needs more readily. However, research suggests that customers are concerned about the security risks of cloud computing and the loss of direct control over the security of systems for which they are accountable.

Vendors have attempted to satisfy this demand for security by offering security services in a cloud platform, but because these services take many forms, they have caused market confusion and complicated the selection process. This has led to limited adoption of cloud-based security services thus far. However, cloud-based security services are predicted to triple in many segments by 2013.

In CSA research, this specific market niche is defined Security as a Service (SecaaS), and it refers to the provision of security applications and services via the cloud, either to cloud-based infrastructure and software, or from the cloud to the customers' on-premise systems.

CSA recommends that the EC to take measures aiming to support and facilitate the development of the SecaaS market, bringing clarity in definition, characterisation, and in developing standards for cloud-based security services in order for consumers to understand the unique nature of cloud-delivered security offerings so they can evaluate the offerings and understand if they will meet their needs.

We also believe that creating a common vocabulary for SecaaS, describing service categories offered in "as a service" mode (and their core functionalities), and keeping records of providers offerings will be important transparency measures.

Based on survey results collected by CSA from prominent consumers of cloud services, the following security service categories are of most interest to experienced industry consumers and security professionals:

- Identity and Access Management (IAM)
- Data Loss Prevention (DLP)
- Web security
- Email security
- Security assessments
- Intrusion management
- Security Information and Event Management (SIEM)
- Encryption
- Business continuity and disaster recovery
- Network security

The continued CSA research into Security as a Service is focusing on the above categories, and for standardisation and consistency, it is recommended that the EC uses this as the initial basis for their SecaaS-related work and guidance. This should be confirmed through a survey of European industry consumers, paying special attention to the needs of SMEs.

2.0 Trust, Security, and Assurance

2.1 Assessment Framework

Both service providers and their clients lack a consistent and standard means to evaluate offers on the basis of their security, even though security is seen as a prime concern by most organisations. As a result, customers cannot compare offerings on security, and service providers are duplicating the effort of providing information many times over. This is not only wasteful but may also reduce the overall security of the organisations. The overhead of auditing is also increased, as it is harder to provide agreed-upon and understood evidence of compliance due to the lack of standardised terms and processes.

CSA is conscious that there is a need to provide a framework that allows cloud service providers to transparently and efficiently demonstrate their information assurance maturity, good data protection and governance through assessment, and independent audit. Organisations need an economically feasible framework to demonstrate to their customers, regulators and stakeholders their commitment to privacy and security in a regular, quantitative manner.

CSA supports an integrated approach for the assessment of cloud service providers as well as all their external suppliers. This single approach should provide cross-mapping between existing standards (ISO 2700x, COBIT, PCI- DSS, ENISA Cloud IAF, CSA CCM and ISF SOGP) to enhance acceptance by organisations using different standards, thus driving a common approach. The assessment mechanism should provide businesses and governments with full visibility of risks. In our opinion, such a level of visibility and transparency can be achieved only through a solution which will establish:

- A common language to define key terms and controls according to commonly understood industry frameworks to manage risks to information.
- Objective measure through quantitative controls.
- Objective criteria to compare qualitative controls.
- Mechanisms to promptly integrate new requirements expressed in the new directives (the review of the privacy legislation is an example) and regulated markets (e.g. healthcare and public administration).

It is fundamental that the assessment approach scales down to the needs of micro, small and medium enterprises, which are often characterized by modest requirements, such as the use of simple risk analysis and assessment mechanisms and lack of information security awareness.

For the sake of transparency, CSA has delivered the following relevant project work products, which will continue to be updated to address industry needs:

- Cloud Controls Matrix (CCM), which is a control framework and fundamental security principles in assessing the overall security risk of a cloud provider. The CCM is fully mapped to the existing standards and industry accepted frameworks previously mentioned.
- Consensus Assessment Initiative (CAI), which is an industry-accepted way, based on the control matrix, to document what security controls exist in IaaS, PaaS, and SaaS offerings. The Consensus Assessment Initiative Questionnaire is a list of over 160 questions which can be used during provider assessment and procurement, and can be included in service level agreement (SLA) language.
- Common Assurance Maturity Model (CAMM) works to build objective measure of quantitative controls and objective criteria to compare qualitative controls. (Note: The CAMM project is currently in development)
- CloudAudit provides a common interface and namespace that allows cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments and allow authorized consumers of their services to do likewise via an open, extensible, and secure interface and methodology.
- Cloud Trust Protocol defines a question-and-answer method leveraging NIST SCAP for querying provider security control settings. Combined with CloudAudit, these two specifications enable automated and continuous controls monitoring, allowing for an understanding of governance, risk and compliance issues in real-time.

2.2 Transparency Registry

CSA believes that, in order to achieve the best level of transparency in the cloud market, there should be a system in place to share and compare assessment results. This system could take the form of a registry managed and maintained by a European or national public institution (e.g. ENISA, national regulatory authority for telecommunication market, data protection authorities, or new specific authority for information society services) or from an independent trusted party or a public private partnership. Assessment results should be sent to the collecting organisation on a voluntary basis.

In CSA's opinion, an effort to bring transparency in the market brings the greatest benefits if the participation to the schema is voluntary; it should be in the interest of the cloud service providers to show the good work they have done to make existing cloud services more secure than non-cloud services. Moreover, the voluntary participation creates a more "friendly" environment that generates trust and cooperation, allowing service providers to share information relevant to home users, SMEs, public opinion, and national and European institutions.

CSA sees the imposition, via legislative measures, of an information sharing mechanism as a last resort, and we hope it won't be necessary. Therefore, we recommend the EC to support the creation of such a transparency registry.

For the sake of transparency, CSA has worked and is developing the following relevant project:

- The CSA STAR (Security, Trust and Assurance Registry), which is a voluntary repository of the results of self-assessments (Consensus Assessment Initiative Questionnaire) of any business providing cloud services. CSA believes that industry accountability and self-regulation should be in place as soon as possible as we work with governments and industry to develop appropriate regulation for a nascent market. This registry is open and free to use, and can be extended to include registry entries for EU-specific requirements. We also believe an open registry will encourage competition between providers to deliver the most secure services.

2.3 Security Breach Notification

CSA supports any measures that could bring more transparency in the market, and we are convinced that the introduction of an incident reporting mechanism, similar to the ones recently introduced by Article 13a (3) of Directive 2009/140/EC and Article 4 of the revised Directive 2002/58/EC (as amended by Directive 2009/136/EC) could be an appropriate solution.

Even in this case, completed and on-going work at ENISA (on a legislative framework) regarding supporting Member States in the implementation of Article 13a and Article 4 in their national legal framework and operations can be an initial base, especially when it comes to the definition of the scope of the reporting, the severity of the incident to be reported (to avoid excessive reporting), the reporting mechanisms, et cetera. The work done by Unit A3 in DG INFSO within the EP3R project, European Public Private Partnership for Resilience, must also be considered.

In order to exploit all the positive externalities of an incident reporting/breach notification schema, there should be high trust relationships between the various actors of the cloud community. The quality and level of detail of the information provided by cloud service providers in case of an incident will be proportional to the level of trust between market operators and public institutions.

The higher the trust, the more favourable will be the sharing of information such as incident root causes, threats identified and isolated, measures taken to manage the incident, et cetera. For this very reason we recommend the EC to support the creation a voluntary incident reporting schema.

At the Summit 2011 (16/17 November, Orlando, USA), CSA will present the project CloudSIRT (Computer Security Incident Response Team, https://cloudsecurityalliance.org/research/initiatives/cloudsirt/), which enhances the capability of the cloud community to prepare for and respond to vulnerabilities, threats, and incidents in order to preserve trust in cloud computing.

CloudSIRT is a community of cloud providers willing to share, between themselves, information on security incidents, vulnerabilities and threats. Most of the leading cloud service providers are members of CloudSIRT.

CSA will be happy to share with EC institutions, as well as national government, the results of the CloudSIRT project and advice so the EC can take advantage of this already-established trusted relationship in order to realise a European Information Sharing and Analysis (or Observatory) Centre for Cloud Computing.

2.4 CloudSIRT and Real-Time Security Monitoring

CSA research in areas such as SecaaS and CloudSIRT are already providing details and guidance around 1) real-time monitoring (for instance in the area of Security Information and Event Management (SIEM)) and, 2) a European Information Sharing and Analysis Centre for Cloud. Any EC research into this area would be supported by the CSA.

The creation of an impartial and trusted EC-wide cloud-related SIRT, or the addition of explicit cloud expertise and reporting to an existing EC SIRT, would be recommended as a single point for vendors and customers to get data on the latest risks and incidents.

Real- time reporting solutions could potentially and voluntarily send non-sensitive data to the SIRT to ensure it provided the most up-to-date information and thus, the greatest value.

2.5 Continuous Controls Monitoring and Auditing

We have already mentioned the need for a reference control framework that provides guidance around how to assess the service performance with regards to security and assurance and compliance, along with checking both the fulfilment of the requirements expressed in SLA, security SLA, PLAs, and the application of the security policy. We have also suggested some solutions.

Besides appropriate assessment criteria and relevant control objectives, timely and controlled access to the necessary supporting data is required to satisfy the requirements of Governance, Risk Management and Compliance (GRC).

The importance of timely access to information is highlighted by the work done by the USA with FedRAMP, particularly in the area of continuous monitoring (see https://info.apps.gov/sites/default/files/Chapter-2-Continuous-Monitoring.pdf).

We recommend that the EC supports the research into and development of frameworks and automated systems for continuous controls monitoring and auditing.

For the sake of transparency, the CSA is currently working on the GRC Stack toolkit, which is a project relevant in the area of continuous monitoring. We have already mentioned in this paper the four components of the GRC Stack, which are CloudAudit, Cloud Controls Matrix, Consensus Assessment Initiative, and Cloud Trust Protocol.

2.6 Identity Model

Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today. While an enterprise may be able to leverage several cloud computing services without a good identity and access management strategy, in the long run, extending an organisation's identity services into the cloud is a necessary prerequisite for strategic use of on-demand computing services. Supporting today's aggressive adoption of an admittedly immature cloud ecosystem requires an honest assessment of an organisation's readiness to conduct cloud-based Identity and Access Management (IAM), as well as understanding the capabilities of the organisation's cloud computing providers.

CSA recommends that the EC supports cloud providers and standard development organisations (SDOs), e.g. OASIS, developing secure and interoperable identity, access and compliance management configurations, and practices.

CSA is currently working on a research project called Trusted Cloud Initiative (TCI) Reference Architecture, which is meant to be both a methodology and a set of tools that enable security architects, enterprise architects, and risk management professionals to leverage a common set of solutions that fulfil their common needs to be able to assess where their internal IT and their cloud providers are in terms of security capabilities, and to plan a roadmap to meet the security needs of their business.

2.7 Consumer Education

CSA is firmly convinced that one of the reasons for the delay in cloud adoption in Europe is due to a lack of awareness and understanding around this new service-provisioning model. We suggest that the EC launch an educational campaign to clarify and explain:

- What cloud computing is and what various terms mean; greater general awareness and understanding of the terminology will enable potential customers to better understand the potential benefits and use cases.
- The positive economic impact of cloud computing from the European single market, especially with regards to eGov services and SMEs.
- The evaluation of security risks of cloud computing adoption against security risks on premise and how to address them.
- The complexity of legal framework and methods of cloud adoption that meet the EU legal requirements.

As with any new technology, and especially one that offers the opportunity for such a paradigm shift as cloud computing, education is paramount to ensuring potential users understand the technology from a benefits and risk perspective.

2.8 Legal Framework

The rapid pace of technology has consistently proven to present challenges to the interpretation, application, and enforcement of laws and regulations. This is especially true in the case of cloud computing, where the cloud provider becomes a third party in the relationship between an organisation and its data. As already mentioned in this paper, cloud computing introduces new complexities, especially due to need to orchestrate and manage contractual and technical relationships between different cloud service models, IAAS, PAAS, and SAAS (a typical sample scenario is described by a final user, either company or home user, having a contractual relationship with a company, which buys services from a SaaS provider, which, in turn, buys services from a IaaS provider). Those complexities include location, distribution and ownership of the data, multiple jurisdictions, and ownership of software, processes and systems. Moreover, the need to balance the right to privacy and anonymity of cloud customers with the need to implement end to end accountability should be considered.

2.8.1 Applicable Law and Jurisdictions

As with any regulations or guidance across the EC, considerations must be given to differing regulations of member states. Also key to the success of any guidance relating to cloud computing is the recognition of the global nature of most cloud service providers and how EU data protection rules can be accommodated given this business model.

CSA welcomes a clarification on the applicable law and competent jurisdiction. In our opinion, a general framework should be established to clarify cases of multiple (and conflicting) applicable laws and jurisdictions. Such a framework should clarify, as a general rule, which law should be applied (the one more favourable to cloud customer? the one of the country of origin of the user? the one where the data processing is mainly executed? et cetera) and which are the exceptions.

The CSA has multiple European chapters along with a recently appointed directorate with direct responsibility for the EC region. As such, the on-going CSA research and guidance will have an increased focus on issues relating specifically to the EC jurisdiction and rules, along with more general cloud security guidance.

2.8.2 Government Access to Data

CSA is conscious of the fact that government access to data in the cloud (e.g., the USA Patriot Act, and similar acts in other countries), grants to government agencies extensive or unlimited access to information held in servers and networks for the purpose of investigations related to national security. These laws may hamper cloud adoption (as noted also by ENISA in the report: “Security and Resilience in Government Clouds”); therefore, we suggest to establish a bilateral agreement between EC and the US federal government to set up clear rules of engagement and limitations to the right of a government to confiscate servers sitting in its national territory or owned by companies with headquarters situated in their country. This bilateral agreement could be then extended to other countries as well.

2.8.3 e-Discovery

The conflict between US regulations regarding the collection of evidence in connection with litigation also creates significant hurdles. US laws regarding the collection of evidence in civil litigation may be used to require litigants to bring into evidence personal and other data that are held in servers located out of the United States, such as in the EU or other countries. On the other hand, these other countries where the evidence is located may have blocking statutes that prohibit or significantly restrict the transfer of data out of their territory for purpose of litigation. They may also have data protection laws that prohibit the transfer of personal information out of the country unless stringent conditions are met.

We suggest, in essence, to bring forward the Article 29 opinion on pre-trial discovery for cross border civil litigation (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf) as a first step in addressing the prohibition against the transfer of personal data out of the EU in connection with litigation conducted in the United States. Also relevant are the current negotiations for an EU-US umbrella agreement on data protection.

CSA supports recommendations that improve the collaboration between lawyers and technology professionals and recommends methods or standards for educating lawyers on cloud computing and on how the different cloud models can impact legal and e-discovery laws and regulations.

3.0 Security Innovation in the Cloud

In addition to the previously mentioned set of recommendations, CSA feels that technical innovation also holds much promise to solve many of today’s problems related to interoperability and portability, as well as trust, security and assurance. For example, new encryption and key management approaches such as format preserving encryption, tokenisation, and homomorphic encryption hold promise to manage data in a way that supports existing laws and policies, without giving cloud providers “back door” access to sensitive information. CSA is developing an Innovation Initiative to articulate principles for entrepreneurship and innovation in cloud computing that increase security in the global compute utility in a way that respects the sovereignty and requirements of individual member states and the common European Union. We believe the EU can also encourage development of cloud management technologies that enforce desired policies at data centres around the world.