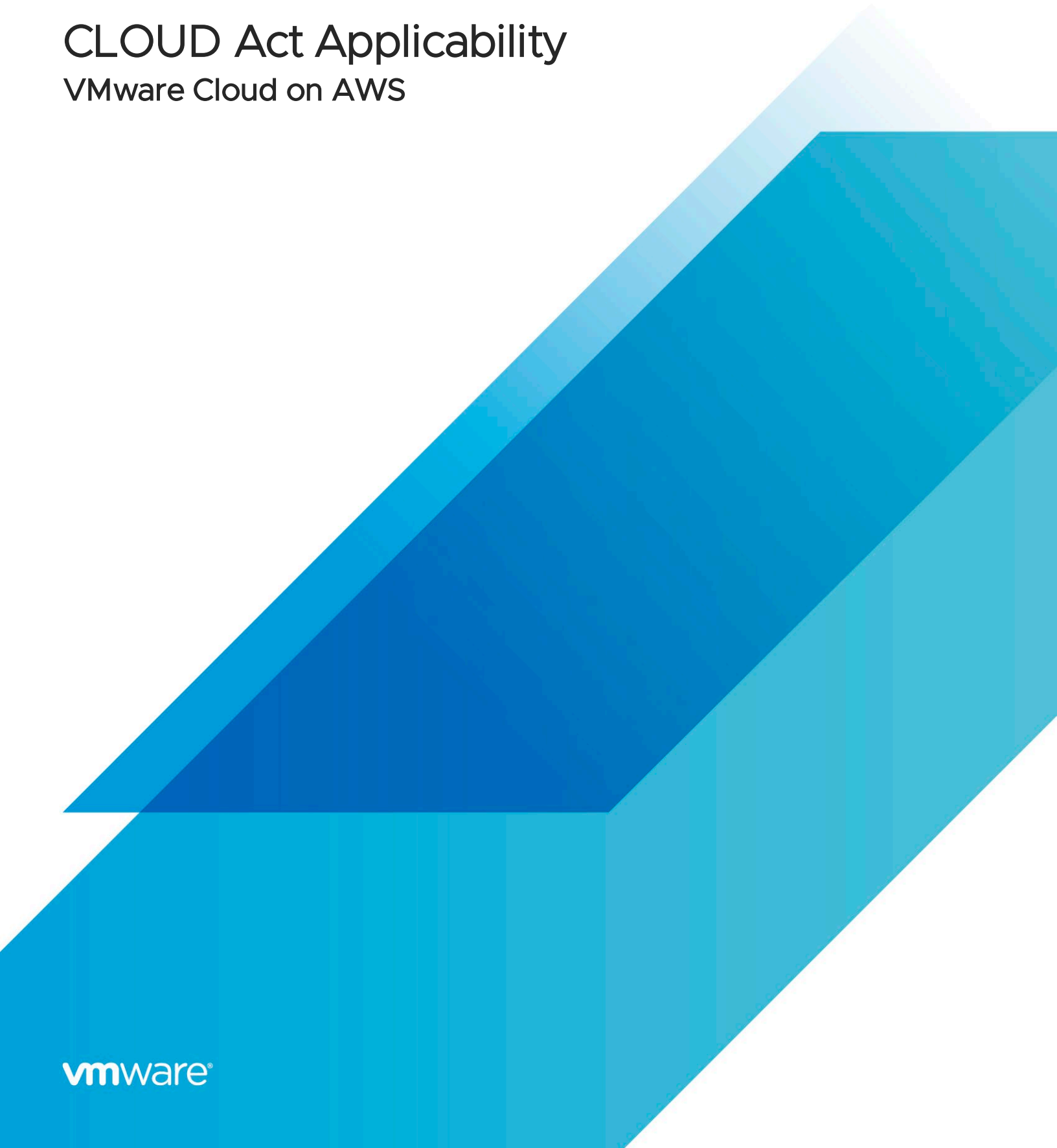
WHITE PAPER–MAY 2023

CLOUD Act Applicability

VMware Cloud on AWS

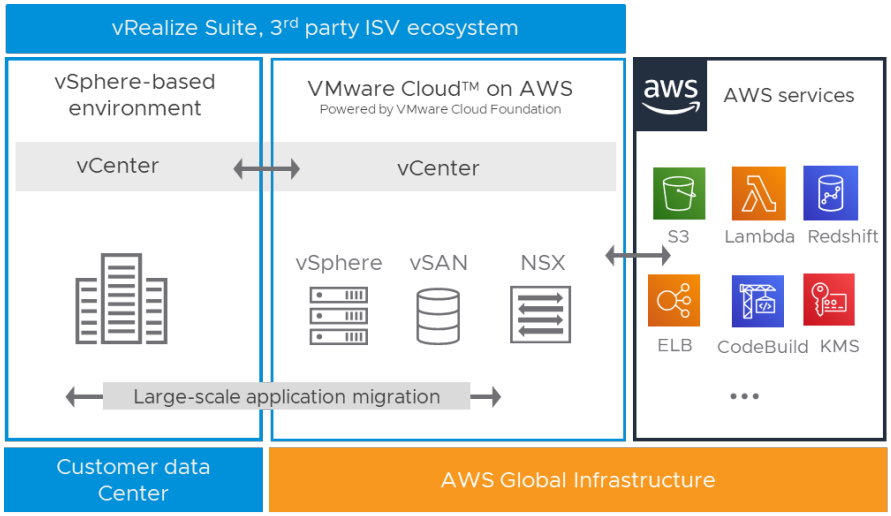


vmware

VMware Cloud on AWS

VMware Cloud on AWS is a jointly engineered service that brings VMware's enterprise-class Software-Defined Data Center software to the AWS Cloud's dedicated, elastic, bare-metal infrastructure, delivered as an on-demand service with optimized access to AWS services, enabling IT teams to rapidly migrate and modernize VMware vSphere applications in AWS Cloud by leveraging the best of both worlds.

VMware Cloud on AWS is available in 21 regions globally including 8 regions in Europe, Middle East and Africa (EMEA), 7 regions in Asia and 6 regions in Americas and is audited against a wide range of global compliance frameworks including SOC 2, ISO 27001, PCI, HIPAA, C5 (Germany), Cyber Essentials Plus (U.K), MTCS (Singapore), ISMAP (Japan), OSPAR (Singapore), and IRAP/CSG (Australia). For more information, please visit *Trust Center (vmware.com)* . In this whitepaper, we aim to address some of the common questions from customers and partners regarding the applicability CLOUD Act for VMware Cloud on AWS.



The CLOUD Act

- The United States enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act in March 2018 to improve procedures and mechanisms for foreign and U.S. government, courts and law enforcement investigators in obtaining access to electronic information held by service providers. In brief, it updated the lawful mechanism for such entities to request data kept outside their borders to investigate serious crimes. It also created a possibility for foreign countries to sign bilateral agreements with the United States (Cloud Act Agreements) to enable law enforcement requests directly to service providers rather that via the traditional mutual legal assistance treaty process. The CLOUD Act safeguards customer content, including the rights of providers and customers to challenge requests that conflict with national laws or interests.

What's new in the CLOUD Act

- The CLOUD Act is an update to the United States Stored Communications Act (SCA), clarifying the extra-territorial scope of law enforcement requests made under the SCA. It also enables service providers to challenge and respond to requests from government/law enforcement agencies where demands conflict with foreign laws.

  It is important to note that under the Cloud Act, law enforcement requests for data are limited to investigations related to serious crimes; the Act does not provide the U.S. government unrestricted access to customer data. VMware supports customers during any such requests and as set forth in VMware's standard contractual terms

vmware

(VMware General Terms, accessible on *VMware ONE Contract Center)*. VMware will provide customers with notice and a copy of the requests unless legally prohibited from doing so. For a summary of how VMware handles government access requests, please visit *Trust Center (vmware.com)*

The CLOUD Act provides that the United States may enter into CLOUD Act agreements only with rights-respecting countries that abide by the rule of law. Before the United States can enter into an executive agreement anticipated by the CLOUD Act, the CLOUD Act requires that the U.S. Attorney General certify to the U.S. Congress that the partner country has in its laws, and implements, in practice, robust substantive and procedural protections for privacy and civil liberties. So far, the United States has enter into Cloud Act Agreements with the United Kingdom and Australia.

Does CLOUD Act supersede country's national laws?

- No. the CLOUD Act does not supersede or amend another country's local laws. The CLOUD Act allows service providers and customers to challenge requests that conflict with another country's national laws provided that the customer is allowed to be informed under the underlying warrant. The CLOUD Act does not create any new form of warrant: the Stored Communications Act requires law enforcement agencies to obtain a warrant for content requests. Under U.S. constitutional law, law enforcement agencies must meet high standards to obtain a warrant. They would require substantial evidence to prove that a probable crime has occurred and that the content requested relates to it. This requirement was already in place in the Stored Communications Act, which was already in place before the CLOUD Act.

Can U.S. Government directly access customer data?

- No, the CLOUD Act does not provide U.S. Government or Law enforcement agencies unrestricted access to customer data. As indicated above, the request can be made to service providers like VMware Cloud only in connection with serious crimes and only if there is an associated warrant issued by a U.S. court in line with the CLOUD Act. VMware does not provide any direct access to customer SDDCs or any customer data. VMware will evaluate the demand for disclosure to determine whether it is legally valid and binding and will challenge any unlawful request for disclosure (For a summary of how VMware handles government access requests, please visit *Trust Center (vmware.com).*

How does the CLOUD Act impact VMware Cloud on AWS?

- CLOUD Act does not require the VMC on AWS service to be delivered differently from the way the service is currently delivered. VMware Cloud on AWS stores customer data inside a geographic region chosen by the customer when they deploy a Software Defined Datacenter (SDDC). Customer data will not be relocated, replicated, archived, or copied without the explicit request or Actions of the customer administrator. For a list of available regions see ,*VMC on AWS available regions*. We have established policies and practices designed to protect the data we process on behalf of our customers, including any PII or metadata. For more information see *VMware Privacy Datasheet*.

How does CLOUD Act impact customers and partners who consume the service?

- As described in the *VMC on AWS Shared Responsibility Model*, VMware is responsible for securing the software and systems that make up the VMware Cloud on AWS service and customers are responsible for managing the customer data and the virtual machines (including in guest security and encryption) and access governance over the customer data.

Do customers/partners need any additional contractual amendments under CLOUD Act?

- Customers/Partners do not need to amend the existing contracts with VMware.

How does CLOUD Act affect the PII data stored or transferred between U.S. and other countries?

- The CLOUD Act is not specific to PII data. It is only one of many legislative tools to request specific data to investigate a serious crime and must be supported by an appropriate warrant from U.S. courts. U.S. governments or law enforcement agencies cannot directly access or alter the PII data uploaded by customers.

Are only U.S. companies subjected to CLOUD Act?

- No, Cloud Act applies to all electronic communication service providers or remote computing service providers subject to U.S. jurisdiction.

Can customers still use VMware Cloud on AWS with CLOUD Act in place?

- VMware is committed to providing high standards in data security, disaster recovery and privacy for all customers without any geographic restrictions. VMware has had customers across E.U. and Asia prior to CLOUD Act and is growing more customers across the world without any concerns around CLOUD Act or any other legal frameworks.

Conclusion

CLOUD Act only comes into play for investigations related to serious crimes and must be supported by appropriate warrants issued by an independent court in accordance with criminal investigation proceedings. Even in court orders, the CLOUD Act does not supersede the country's national laws, providing customers with adequate safeguards and protection over their data.

Even before CLOUD Act the U.S had various surveillance acts such as the Foreign Intelligence Services Act (FISA) and Five-Eyes which prescribes procedures for requesting judicial authorization for electronic surveillance and physical search of persons engaged in espionage or international terrorism against the United States on behalf of a foreign power.

Organizations worldwide are using VMware solutions to reduce their infrastructure footprint, efficiently handle business spikes, and progress their digital transformation journey. We work with customers across U.S., E.U. and Asia Pacific across all industry verticals and are committed to help our customer achieve their digital transformation goals and meet their compliance needs. If you have further questions regarding CLOUD Act or VMware service, do contact your VMware account team.

Contributors

- Moin Nawaz Syed – Product Line Manager, VMware Cloud Solutions
- Patrick O'Brien – Group Product Line Manager, VMware Cloud Solutions
- Matt Dreyer – Sr. Director, VMware Cloud Solutions
- Ali Emadi – Senior Corporate Counsel

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.