TRUSTED CLOUD: VMWARE HYBRID CLOUD INFRASTRUCTURE AS A SERVICE (IAAS) ENVIRONMENTS

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of securing cloud workloads in hybrid cloud environments through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Trusted Cloud project for VMware hybrid cloud Infrastructure as a Service (IaaS) environments, including challenge, proposed solution, and potential benefits. If you have questions or suggestions, please contact us at trusted-cloud-nccoe@nist.gov.

CHALLENGE

A *cloud workload* is an abstraction of the actual instance of a functional application that is virtualized or containerized to include compute, storage, and network resources. Cloud workloads are constantly being spun up, scaled out, moved around, and shut down. Organizations often find adopting cloud technologies is not a good business proposition because they encounter one or more of the following issues:

1. Cannot maintain consistent security and privacy protections for information—applications, data, and related metadata—across platforms.
2. Cannot dictate how different information is secured, such as providing stronger protection for more sensitive information.
3. Cannot retain visibility into how their information is protected to ensure consistent compliance with legal and business requirements.
4. Cannot maintain security regulatory compliance requirements for data across the hybrid cloud.

Many organizations, especially those in regulated sectors like finance and healthcare, face additional challenges because security and privacy laws vary around the world. Laws that protect information an organization can collect, process, transmit, or store may vary depending on whose information it is, what kind of information it is, and where it is located. Cloud technologies may silently move an organization's data from one jurisdiction to another, so an organization may want to restrict which on-premises private or hybrid/public cloud servers it uses based on their geolocations to avoid compliance issues.

PROPOSED SOLUTION

Organizations need to monitor, track, apply, and report their security and privacy policies on their cloud workloads in a consistent, repeatable, and automated way. Building on previous National Institute of Standards and Technology (NIST) work documented in NIST Interagency Report (IR) 7904, Trusted Geolocation in the Cloud: Proof of Concept Implementation, the NCCoE and its collaborators are developing a Trusted Cloud solution that will demonstrate how trusted compute pools leveraging hardware roots of trust, can provide the necessary security capabilities. These capabilities will provide assurance that cloud workloads are running on trusted hardware and in a trusted geolocation or logical boundary. They can also help improve protections for the data in the workloads and the data flows between workloads.

BENEFITS

The NCCoE's practice guide to Trusted Cloud can help organizations:

- understand how trusted cloud technologies can reduce risk and satisfy existing system security and privacy requirements, while meeting industry sector-specific regulatory compliance requirements
- become aware of the resources, skills, experience, and become aware of the resources, skills, and knowledge needed to implement and manage a trusted cloud environment
- provide a practical and effective way to design and implement trusted cloud technologies

LEARN MORE ABOUT NCCOE
Visit https://www.nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

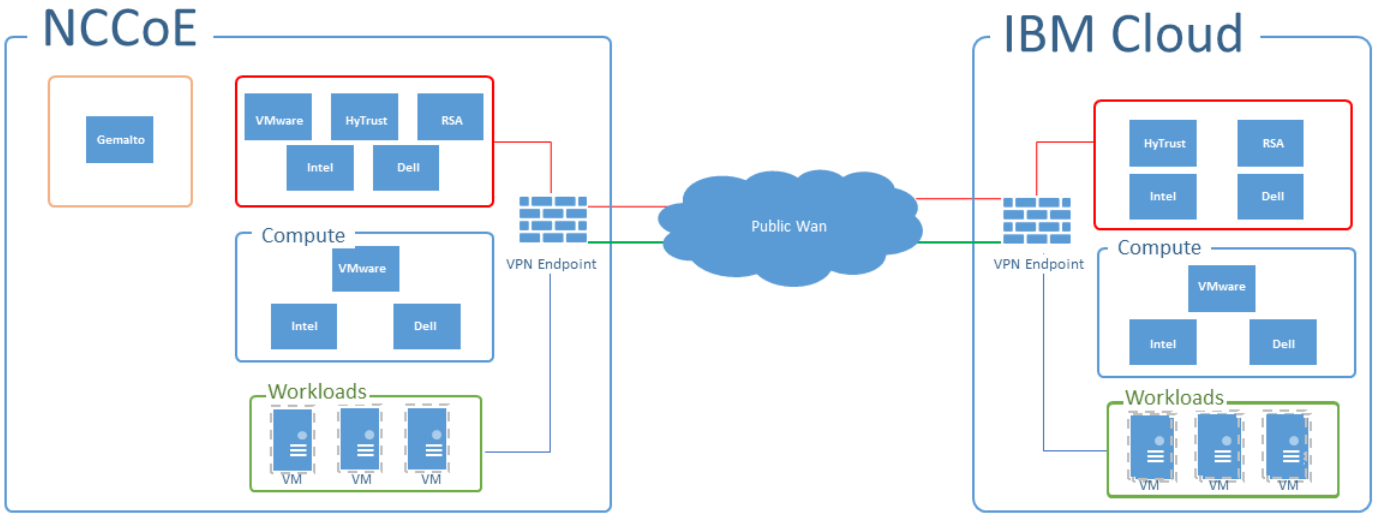
- gain the ability to determine each cloud workload's security posture at any time through continuous monitoring

HIGH-LEVEL ARCHITECTURE

The proposed solution leverages commercial off-the-shelf technology and cloud services to lift and shift a multi-tier application between an organization-controlled private cloud and a public cloud over the internet. At a high level, the architecture has three pieces: a private cloud hosted at the NCCoE, an instance of the public IBM Cloud Secure Virtualization (ICSV), and an Internet Protocol Security (IPsec) virtual private network (VPN) that connects the two clouds to form a hybrid cloud, with the public and private clouds in the same management domain. Workloads can be shifted or live-migrated between the clouds.

The proposed solution includes the following capabilities:

- single pane of glass for management and monitoring of cloud workloads—including software configurations and vulnerabilities
- data protection and encryption key management enforcement focused on trust-based and geolocation-based resource pools and secure migration of cloud workloads
- key management and keystore controlled by the organization—not the cloud service provider
- industry sector and/or organizational business compliance enforcement for regulated workloads between the clouds



TECHNOLOGY COLLABORATORS

The technology vendors participating in this project submitted their capabilities in response to an open call in the *Federal Register*. Companies with relevant security capabilities were invited to sign a Cooperative Research and Development Agreement with the National Institute of Standards and Technology (NIST), allowing them to participate in a consortium to build this example solution. Technology collaborators on this project are...

DELL EMC, gemalto a Thales company, HYTRUST HyTrust.com, IBM, intel, RSA, vmware

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or the NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the work underway to secure cloud workloads in hybrid cloud environments. For more details, download the project description by visiting https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud/hybrid or scan the QR code which takes you to the Trusted Cloud project page.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or are interested in contributing technology or expertise, please send an email to trusted-cloud-nccoe@nist.gov.