NIST SPECIAL PUBLICATION 1800-19A

Trusted Cloud

Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments

Volume A:
Executive Summary

Donna Dodson
NIST

Daniel Carroll
Dell/EMC

Gina Scinta
Gemalto

Hemma Prafullchandra
HyTrust

Harmeet Singh
IBM

Raghuram Yeluri
Intel

Tim Shea
RSA

Carlos Phoenix
VMware

August 2018

PRELIMINARY DRAFT 1

This publication is available free of charge from: https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud/hybrid

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

- Cloud services can provide organizations the opportunity to increase their flexibility, availability, resiliency, and scalability, which they can use in turn to increase security, privacy, efficiency, responsiveness, innovation, and competitiveness.
- The core impediments to an organization's broader adoption of cloud technologies are the ability to protect its information and virtual assets in the cloud, and to have sufficient visibility so it can conduct oversight and ensure that it (and its cloud provider) are complying with applicable laws and business practices.
- The National Cybersecurity Center of Excellence (NCCoE) at NIST built a laboratory environment using commercial off-the-shelf technology and cloud services to safeguard the security and privacy of an organization's applications and data being run within or transferred between private and hybrid/public clouds.
- The full NIST Cybersecurity Practice Guide being developed for this project will demonstrate how organizations can implement trusted compute pools in order to enforce and monitor their security and privacy policies on their cloud workloads and meet compliance requirements as specified in NIST Special Publication 800-53 and the Cybersecurity Framework.

CHALLENGE

In cloud environments, 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, even for a single class of information.
2. Do not have the flexibility to be able to dictate how different information is protected, 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.

Many organizations, especially those in regulated sectors like finance and healthcare, face additional challenges because security and privacy laws vary around the world. For protecting information the organization collects, processes, transmits, or stores, laws 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. Because laws in some jurisdictions may conflict with an organization's own policies or local laws and regulations, an organization may decide it needs to restrict which on-premises private or hybrid/public cloud servers it uses based on their geolocations to avoid compliance issues.

SOLUTION

Organizations need to be able to monitor, track, apply, and enforce their security and privacy policies on their cloud workloads based on business requirements in a consistent, repeatable, and automated way. 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. Building on previous NIST work documented in NIST Interagency Report (IR) 7904, *Trusted Geolocation in the Cloud: Proof of Concept Implementation*, the NCCoE is 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 not only provide assurance that cloud workloads are running on trusted hardware and in a trusted geolocation or logical boundary, but also will improve the protections for the data in the workloads and data flows between workloads.

The example solution will leverage modern commercial off-the-shelf technology and cloud services to address a particular use case scenario: lifting and shifting a typical multi-tier application between an organization-controlled private cloud to a hybrid/public cloud over the Internet. The example solution will include the following capabilities:

- 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.
- Persistent data flow segmentation before and after the trust-based and geolocation-based/resource pools secure migration.
- Industry sector and/or organizational business compliance enforcement for regulated workloads between the on-premises private and hybrid/public clouds.

While the NCCoE will use a suite of commercial products to address this challenge, the practice guide will not endorse these particular products, nor will it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

Once available, the NCCoE’s full practice guide to Trusted Cloud can help your organization:

- Understand how trusted cloud technologies can reduce risk and satisfy existing system security and privacy requirements.
- Become aware of the resources, skills, experience, and knowledge needed to implement and manage a trusted cloud environment.
- Provide a practical and effective way to design and implement trusted cloud technologies, including restricting cloud workloads to on-premises private or hybrid/public cloud servers meeting specific characteristics.
- Gain the ability to determine each cloud workload’s security posture at any time through continuous monitoring, regardless of the cloud infrastructure or server.
- Modernize the legacy on-premises infrastructure by lifting and shifting existing workloads to the cloud environment while maintaining control and visibility of the workloads.
- Foster greater confidence in adoption of cloud technologies.

SHARE YOUR FEEDBACK

The comment period for the preliminary draft of this volume ends September 30, 2018. Comments may be submitted to trusted-cloud-nccoe@nist.gov with the Subject "Comments on Trusted Hybrid Cloud VolA-PD1." All comments are subject to release under the Freedom of Information Act (FOIA). There will be at least one additional comment period for this volume.

The other volumes of this guide will be released for review and comment on different schedules so that each volume is made available as soon as possible, rather than delaying the release of completed volumes until all other volumes are also completed. You will be able to view or download them at https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud/hybrid. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement to collaborate with NIST in a consortium to build this example solution.

DELLEMC gemalto HYTRUST IBM intel RSA vmware

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order 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 NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200