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*
Computer Security Division
Information Technology Laboratory

Daniel Carroll
Dell/EMC
Hopkinton, Massachusetts

Gina Scinta
Gemalto
Austin, Texas

Hemma Prafullchandra*
HyTrust
Mountain View, California

Harmeet Singh
IBM
Armonk, New York

Raghuram Yeluri
Intel
Santa Clara, California

Tim Shea
RSA
Bedford, Massachusetts

Carlos Phoenix
VMware
Palo Alto, California

*Former employee; all work for this publication done while at employer.

October 2021

DRAFT

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

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

Organizations can take advantage of cloud services to increase their security, privacy, efficiency, responsiveness, innovation, and competitiveness. The core concerns about cloud technology adoption are protecting information and virtual assets in the cloud, and having sufficient visibility to conduct oversight and ensure compliance with applicable laws and business practices. This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates how organizations can address these concerns by implementing what are known as trusted compute pools. Through these pools, organizations can safeguard the security and privacy of their applications and data being run within a cloud or transferred between a private cloud and a hybrid or public cloud.

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 in a multi-tenancy environment.
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. Laws for protecting information the organization collects, processes, transmits, or stores 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.

This practice guide can help your organization:

- understand how trusted cloud technologies can reduce your risk and satisfy your existing system security and privacy requirements
- 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 your legacy on-premises infrastructure by moving existing workloads to the cloud while maintaining the same security and compliance outcomes

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. Building on previous NIST work documented in NIST Interagency Report (IR) 7904, *Trusted Geolocation in the Cloud: Proof of Concept Implementation*, the National Cybersecurity Center of Excellence (NCCoE) has developed a trusted cloud solution that demonstrates how trusted compute pools leveraging hardware roots of trust can provide the necessary security capabilities. These capabilities not only provide assurance that cloud workloads are running on trusted hardware and in a trusted geolocation or logical boundary, but also improve the protections for the data in the workloads and data flows between workloads.

The example solution uses technologies and security capabilities (shown below) from our project collaborators. The technologies used in the solution support security and privacy standards and guidelines including the NIST Cybersecurity Framework, among others.

Collaborator	Security Capability or Component
DELL EMC	Server, storage, and networking hardware
gemalto a Thales company	Hardware security module (HSM) for storing keys
HYTRUST An Entrust Company	Asset tag and policy enforcement, workload and storage encryption, and data scanning
IBM	Public cloud environment with IBM-provisioned servers
intel	Intel processors in the Dell EMC servers
RSA	Multifactor authentication, network traffic monitoring, and dashboard and reporting
vmware	Compute, storage, and network virtualization capabilities

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does 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.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-19A: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-19B: Approach, Architecture, and Security Characteristics,* which describes what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-19C: How-To Guides*, which provide specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud. 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.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at trusted-cloud-nccoe@nist.gov.

COLLABORATORS

Collaborators 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). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

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.