Hardware-Enabled Security

Mike Bartock
NIST

January 24, 2023

AGENDA

- Hardware Platform Security Overview
- NIST Publications
  - NIST IR 8320 Hardware-enabled Security: Enabling A Layered Approach To Platform Security
  - NIST IR 8320A Hardware-Enabled Security: Container Platform Security Prototype
  - NIST IR 8320B Hardware-Enabled Security: Policy-Based Governance in Trusted Container Platforms
  - NIST IR 8320C Hardware-Enabled Security: Machine Identity Management and Protection
  - NIST SP 1800-19 Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments
  - NIST SP 1800-33 5G Cybersecurity
- Q&A

HARDWARE PLATFORM SECURITY OVERVIEW

- Increased software security leads attackers to pushing lower in the platform stack, forcing security administrators to address a variety of attacks that threaten the platform firmware and hardware:
  - Unauthorized access to and potential extraction of sensitive platform or user data
  - Modification of platform firmware
  - Supply chain interception through physical replacement of firmware or hardware
  - Access to data or execution of code outside of regulated geopolitical or other boundaries
  - Circumvention of software and/or firmware-based security mechanisms

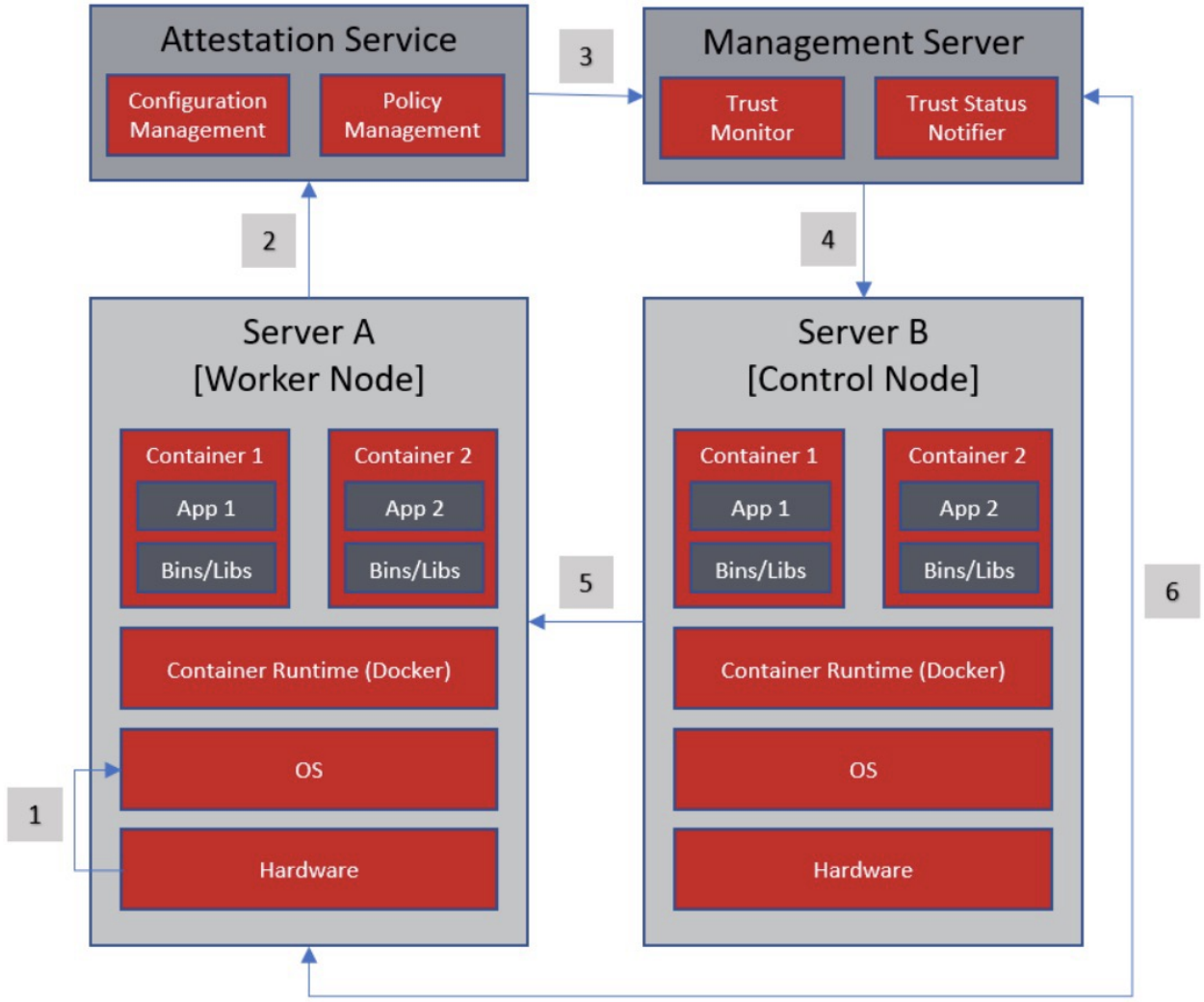
NIST IR 8320 PRINCIPLES

- Platform Integrity Verification
  - Cryptographic measurement of software and firmware
  - Firmware and configuration verification
  - Hardware Security Module (HSM)
    - HSM - physical computing device that safeguards and manages cryptographic keys and provides cryptographic processing
    - TPM - special type of HSM that can generate cryptographic keys and protect small amounts of sensitive information, such as passwords, cryptographic keys, and cryptographic hash measurements
  - The Chain of Trust (CoT) - method for maintaining valid trust boundaries by applying a principle of transitive trust
  - Supply Chain Protection - help ascertain the authenticity and integrity of platform hardware, including its firmware and configuration

NIST IR 8320 PRINCIPLES (CONT'D)

- Data Protection and Confidential Computing
  - Protecting and securing data while in use
  - Trusted Execution Environment (TEE) is an area or enclave protected by a system processor
  - Memory Isolation - encrypt content running in platform memory
  - Application Isolation - protect the memory reserved for an individual application
  - VM Isolation - protect workloads in multi-tenant environments like public and hybrid clouds
- Remote Attestation Services
  - Collate server information and measurement details
  - Platform Attestation - collected host data is compared and verified against policies
    - Allowed-list policies, specifying which firmware versions and event measurements are acceptable
    - Asset tags - simple key value attributes associated with a platform
  - Remote TEE Attestation
    - generation of a verifiable cryptographic evidence by the TEE which is validated by a relying party,
  - Can be integrated with workload orchestrator

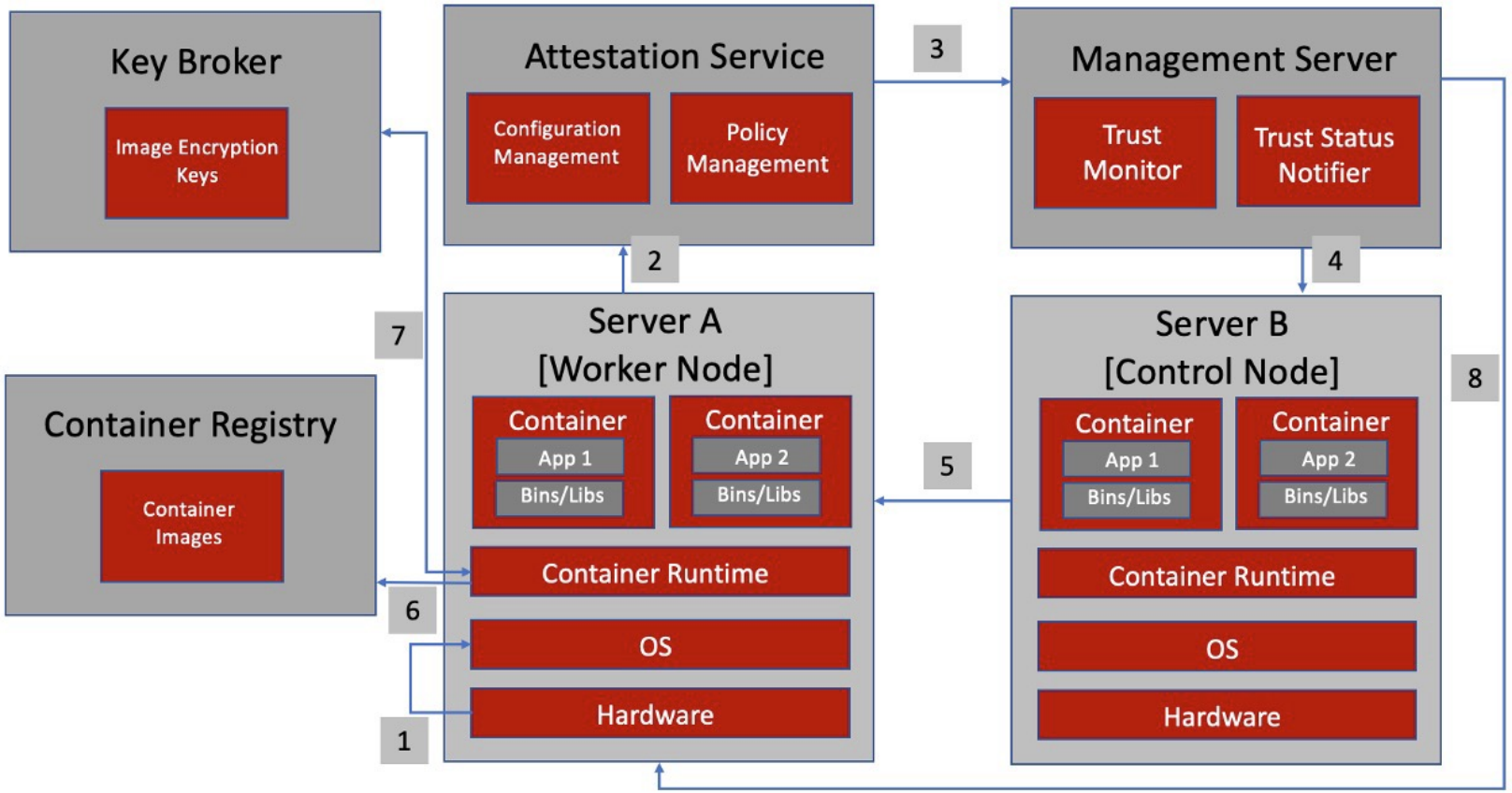
NIST IR 8320A: PROTOTYPE WORKLOAD PLACEMENT ARCHITECTURE



Principles Included:

- TPM
- Chain of Trust
- Asset Tagging
- Remote Attestation Services
- Integration with Orchestrator

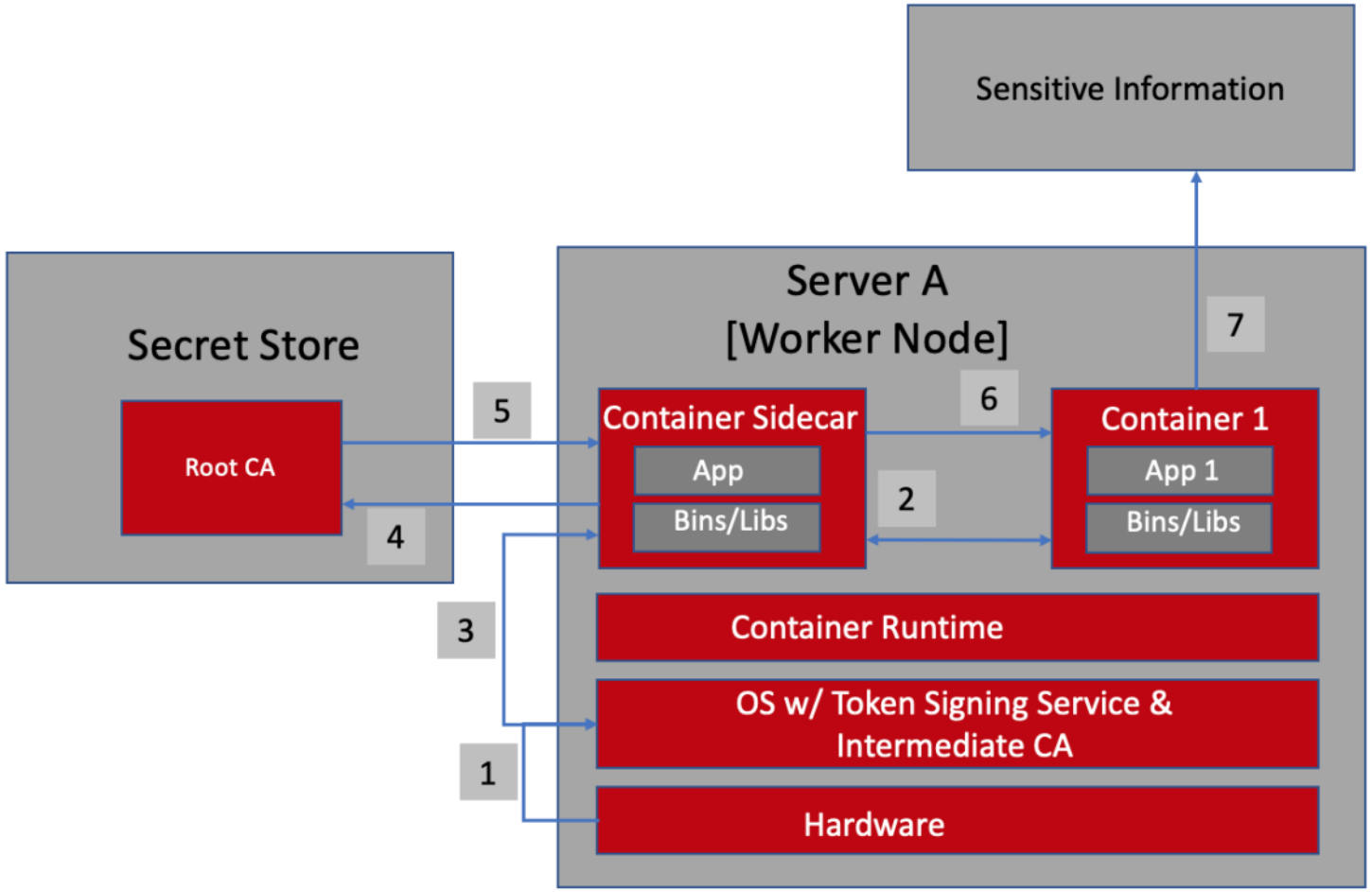
NIST IR 8320B: PROTOTYPE WORKLOAD PLACEMENT ARCHITECTURE



Principles Included:

- TPM
- Chain of Trust
- Asset Tagging
- Remote Attestation Services
- Workload Encryption
- Integration with Orchestrator

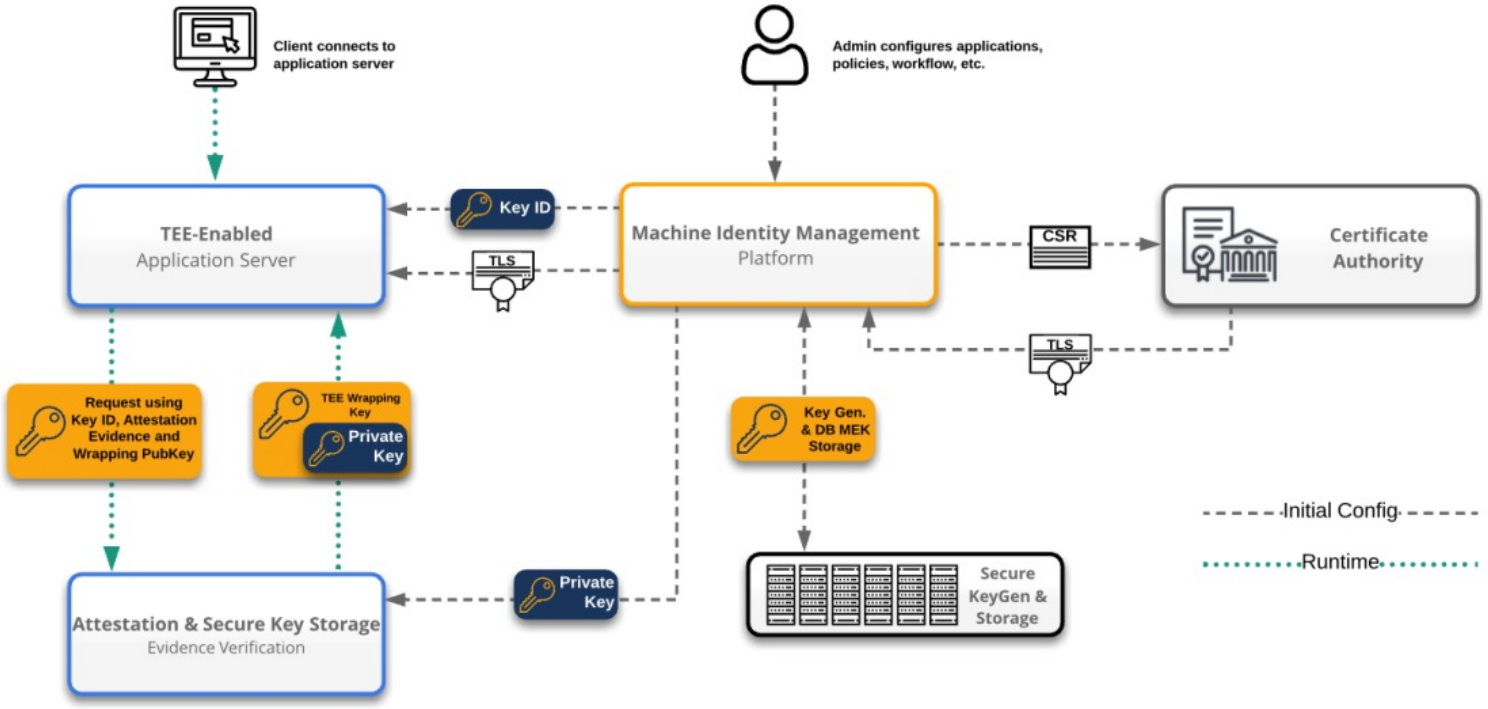
NIST IR 8320B: PROTOTYPE APPLICATION IDENTITY ARCHITECTURE



Principles Included:

- TPM
- Chain of Trust
- Asset Tagging
- Remote Attestation Services
- Workload Encryption
- Integration with Orchestrator

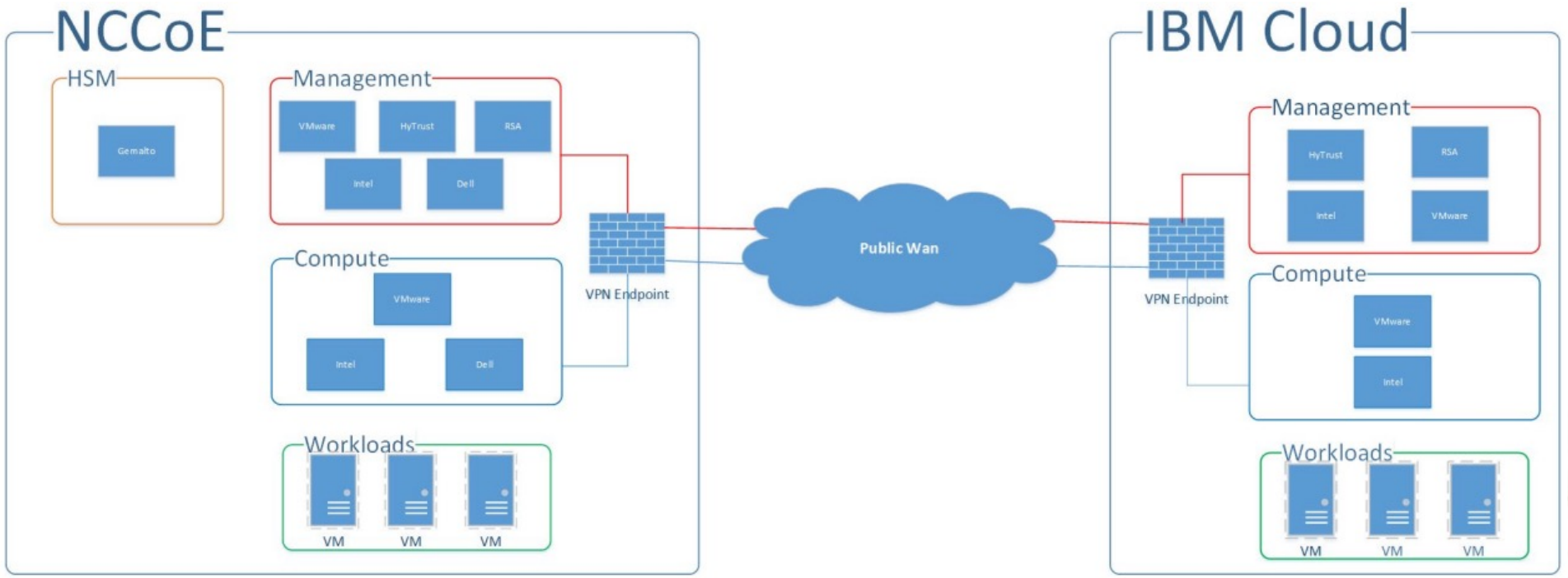
NIST IR 8320C: PROTOTYPE CONFIDENTIAL COMPUTING ARCHITECTURE



Principles Included:

- TEE
- Memory Isolation
- Remote TEE Attestation
- Integration with Orchestrator

NIST SP 1800-19 TRUSTED CLOUD REFERENCE ARCHITECTURE



Principles Included:

- TPM
- Chain of Trust
- Asset Tagging
- Remote Attestation Services
- Workload Encryption
- Integration with Orchestrator

NIST SP 1800-33 5G CYBERSECURITY

Notional Architecture

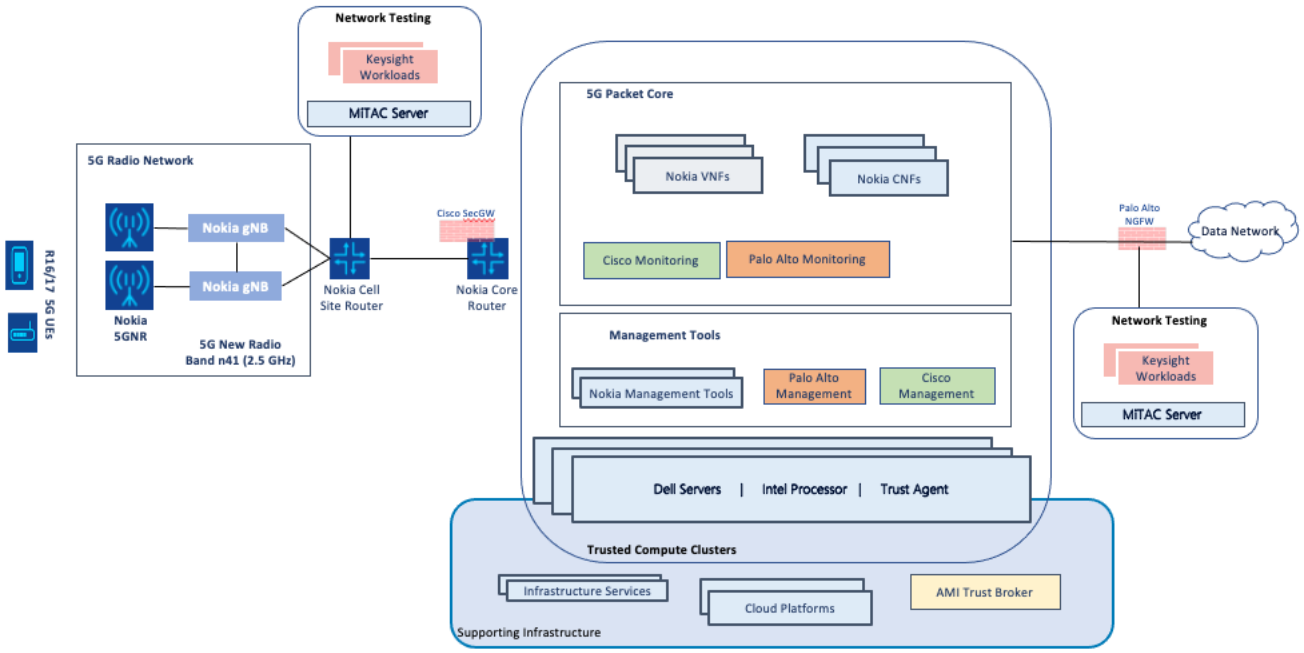


Table 3-2 Security Capabilities

Security Capability	Subreference	Description
Infrastructure Security Categories		
Hardware Roots of Trust Packet Core, ISC-1		
Hardware-Based Platform Measurement	ISC-1.1	Measure platform integrity for each server in the infrastructure using hardware-based controls.
Hardware-Based Labeling	ISC-1.2	Assign specific labels for each server in the infrastructure using hardware-based controls.
Remote Platform Attestation	ISC-1.3	Attest each server's trust measurements and asset tags against policies, and allow services like workload orchestrators access to these findings so the results can be used as factors in workload placement/migration.
Network Function Orchestration Enforcement	ISC-1.4	Deploy and migrate NFs to servers that match platform measurements and labels.
Network Function Image Encryption	ISC-1.5	Encrypt each NF's image, and release the decryption keys only to servers that meet trust policies.
Infrastructure Recommended Practice, ISC-3		
Infrastructure Security Monitoring	ISC-3.1	Provide the visibility across the infrastructure needed to continuously monitor communications patterns, see threats within the extended network, and detect and respond to threats using methods such as behavioral modeling and supervised and unsupervised machine learning.
Network Segmentation	ISC-3.2	Ensure that the infrastructure design and implementation support keeping the different types of network traffic separate from each other.

REFERENCES

- https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud
- NIST IR 8320: Hardware-Enabled Security:Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases
  - https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8320-draft.pdf
- NIST IR 8320A Hardware-Enabled Security: Container Platform Security Prototype
  - https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8320A.pdf
- NIST IR 8320B Hardware-Enabled Security: Policy-based Governance In Trusted Container Platforms
  - https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8320B.pdf
- Draft NIST IR 8320C Hardware-Enabled Security: Machine Identity Management And Protection
  - https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8320C.ipd.pdf
- NIST SP 1800-19 Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-19.pdf
- NIST SP 1800-33B 5G Cybersecurity Preliminary Draft
  - https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf
- Contact hwsec@nist.gov

Questions?