VMware Cloud Foundation 9

Confidential Computing

VMware Cloud Foundation 9

Bob Plankers (bob.plankers@broadcom.com)
Product Management & Marketing, VCF

October 31, 2025

vmware by Broadcom

These slides correspond to the
“Confidential Computing in VCF 9”
video on the VCF YouTube Channel

https://www.youtube.com/@VMwareCloudFoundation

Disclaimer

Certain information in this presentation may outline Broadcom's general product direction.

This presentation shall not serve to (i) affect the rights and/or obligations of Broadcom or its licensees under any existing or future license agreement or services agreement relating to any Broadcom software product; or (ii) amend any product documentation or specifications for any Broadcom software product.

This presentation is based on current information and resource allocations and is subject to change or withdrawal by Broadcom at any time without notice.

The development, release and timing of any features or functionality described in this presentation remain at Broadcom's sole discretion.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future Broadcom product release referenced in this presentation, Broadcom may make such release available to new licensees in the form of a regularly scheduled major product release.

Such release may be made available to licensees of the product who are active subscribers to Broadcom maintenance and support, on a when and if-available basis.

The information in this presentation is not deemed to be incorporated into any contract.

Disclaimer

This document is intended to provide general guidance for organizations that are considering Broadcom solutions. The information contained in this document is for educational and informational purposes only.

This document is not intended to provide advice and is provided “AS IS.”

Broadcom makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

The Ability To Trust That…

1. Your data is where you think it is

2. Known people and systems have access

3. The system is verifiably secure

4. Problems are highlighted rapidly

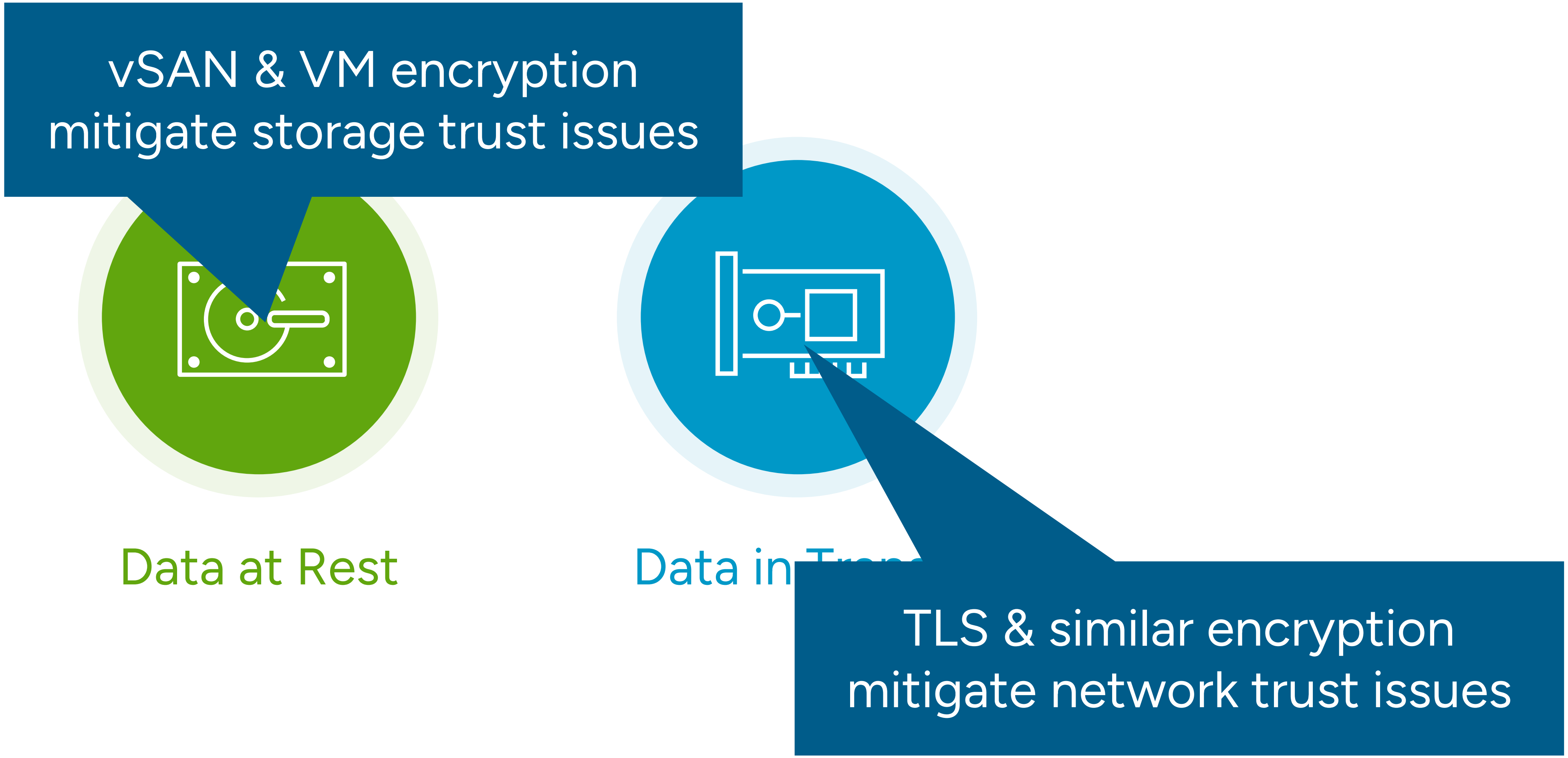
5. Resolutions are quick and non-disruptive

States In Which Data Exists

Data at Rest

Data in Transit

States In Which Data Exists



vSAN & VM encryption mitigate storage trust issues

Data at Rest

Data in Trans

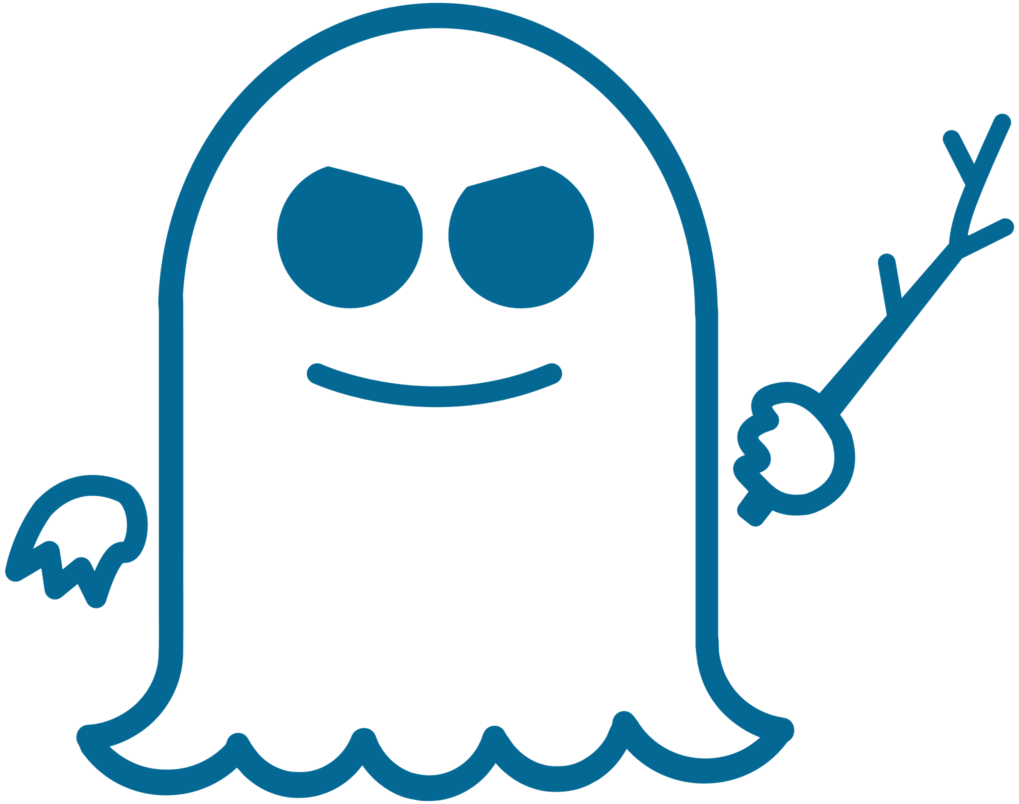
TLS & similar encryption mitigate network trust issues

States In Which Data Exists

Data at Rest

Data in Transit

Data in Use



Trust Issues: Hardware Edition

Vulnerabilities

CPUs, memory controllers, and other hardware components promise security, but shortcuts taken for speed gains **erode those boundaries**.

Evil Neighbors

In shared environments **you do not know who your neighbors are**, nor do you know the state of hardware vulnerability remediation.

Privileged Access

There is **always a certain level of trust you are forced to accept** in a hosted environment, primarily of the admins of the platform.

vmware® by Broadcom

In our zero-trust world, how do we mitigate these problems?

Think About It Like This...

Confidential Computing

Traditional Security

Hotel Safe:

- You lock your valuables in the safe
- Hotel staff has master key
- Must trust the hotel staff

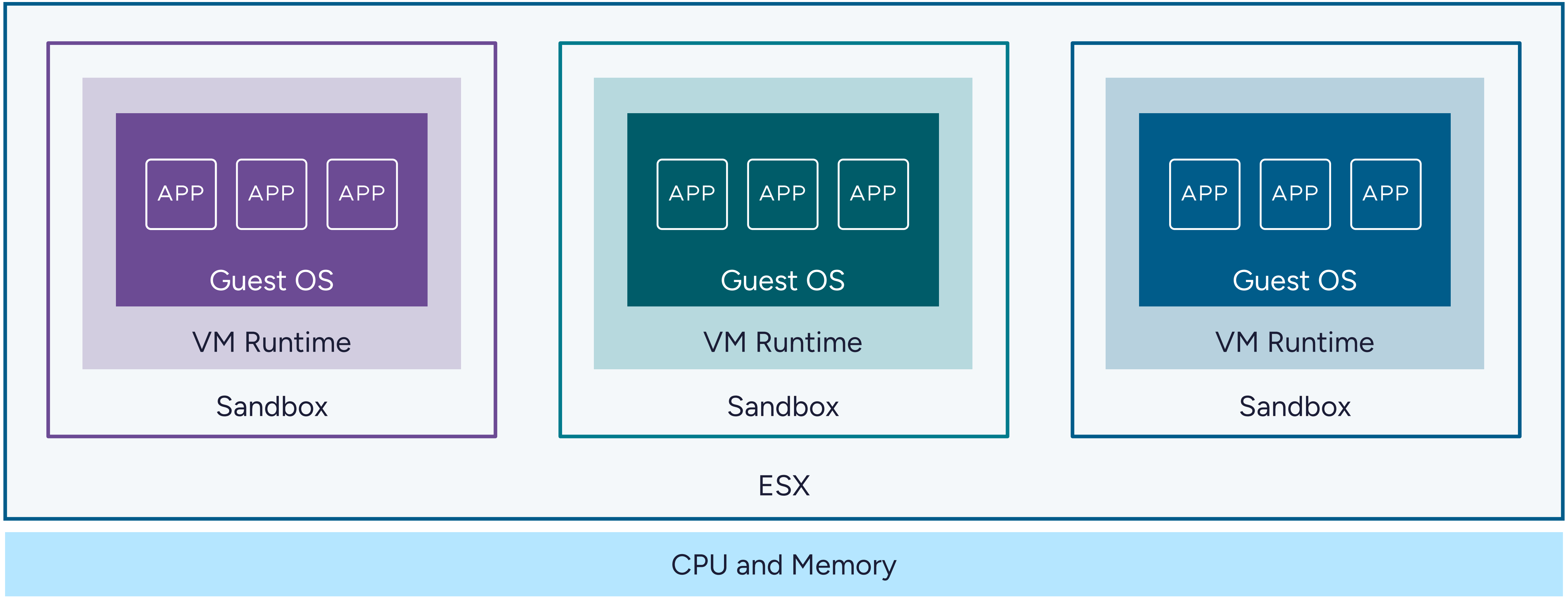
Confidential Computing

Storage Unit:

- Your own padlock on storage unit
- Only you have the key
- **No need to trust facility staff**

Defense-in-Depth Inside ESX

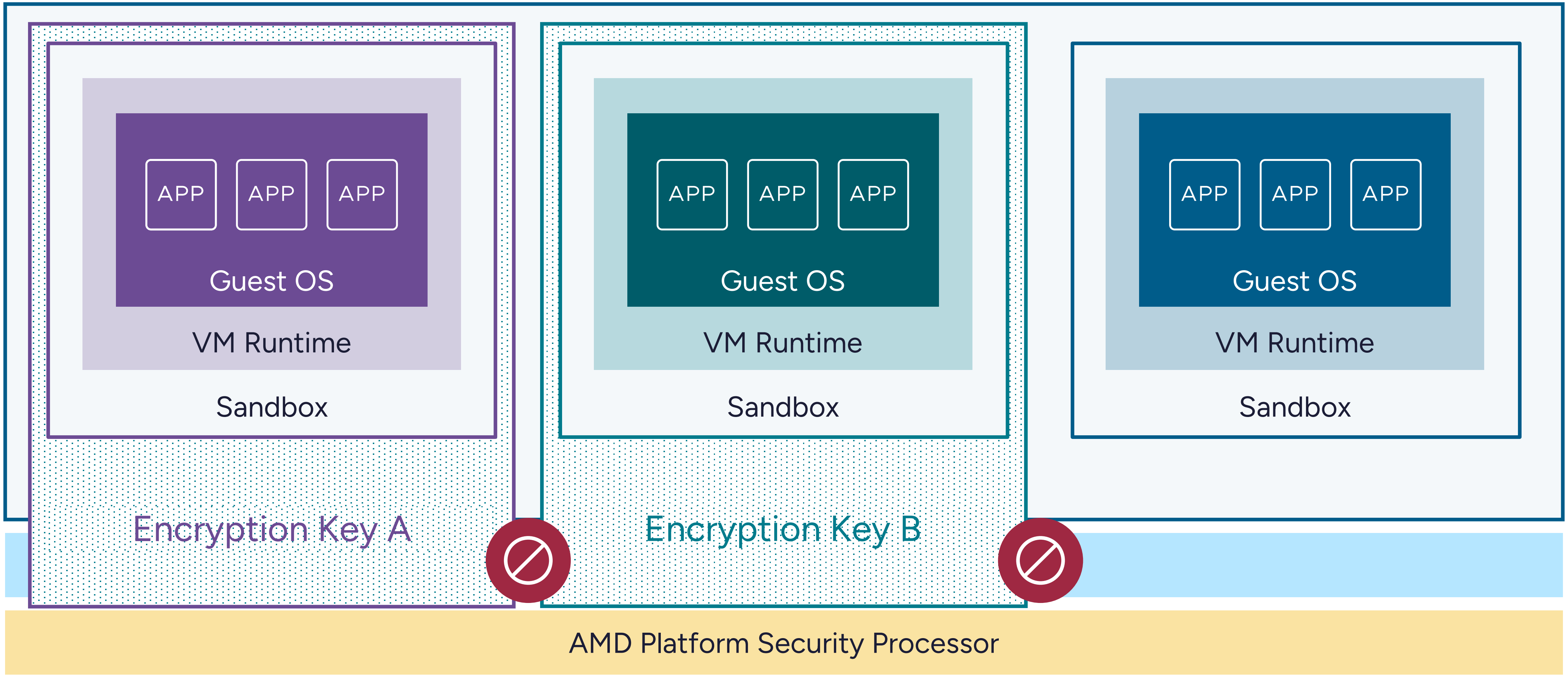
Confidential Computing



vmware by Broadcom

Trusted Execution Environments Help Avoid Trust

Confidential Computing



Advanced Workload Security Protections

Confidential Computing

Hypervisor is not granted access by default

Advanced Workload Security Protections

Confidential Computing

Hypervisor is not granted access by default

Hypervisor can still manage scheduling, memory allocation, device assignments, and power state.

VM can choose to share memory pages and/or paravirtualized devices with the hypervisor

Advanced Workload Security Protections

Confidential Computing

Hypervisor is not granted access by default

Additional integrity protections

Advanced Workload Security Protections

Confidential Computing

Hypervisor is not granted access by default

Additional integrity protections

Even if the hypervisor cannot read memory it could still do other things, which this prevents.

Includes protections against devices accessing workload memory.

Advanced Workload Security Protections

Confidential Computing

Hypervisor is not granted access by default

Additional integrity protections

Strong attestation capabilities

Advanced Workload Security Protections

Confidential Computing

Cryptographic proof that the code you think is running is actually what is running.

Also cryptographic proof that the platform you expect is the one you're on.

Hyper
grante
default

protections

Strong attestation capabilities

Mitigating Various Attacks, By Technology

Confidential Computing

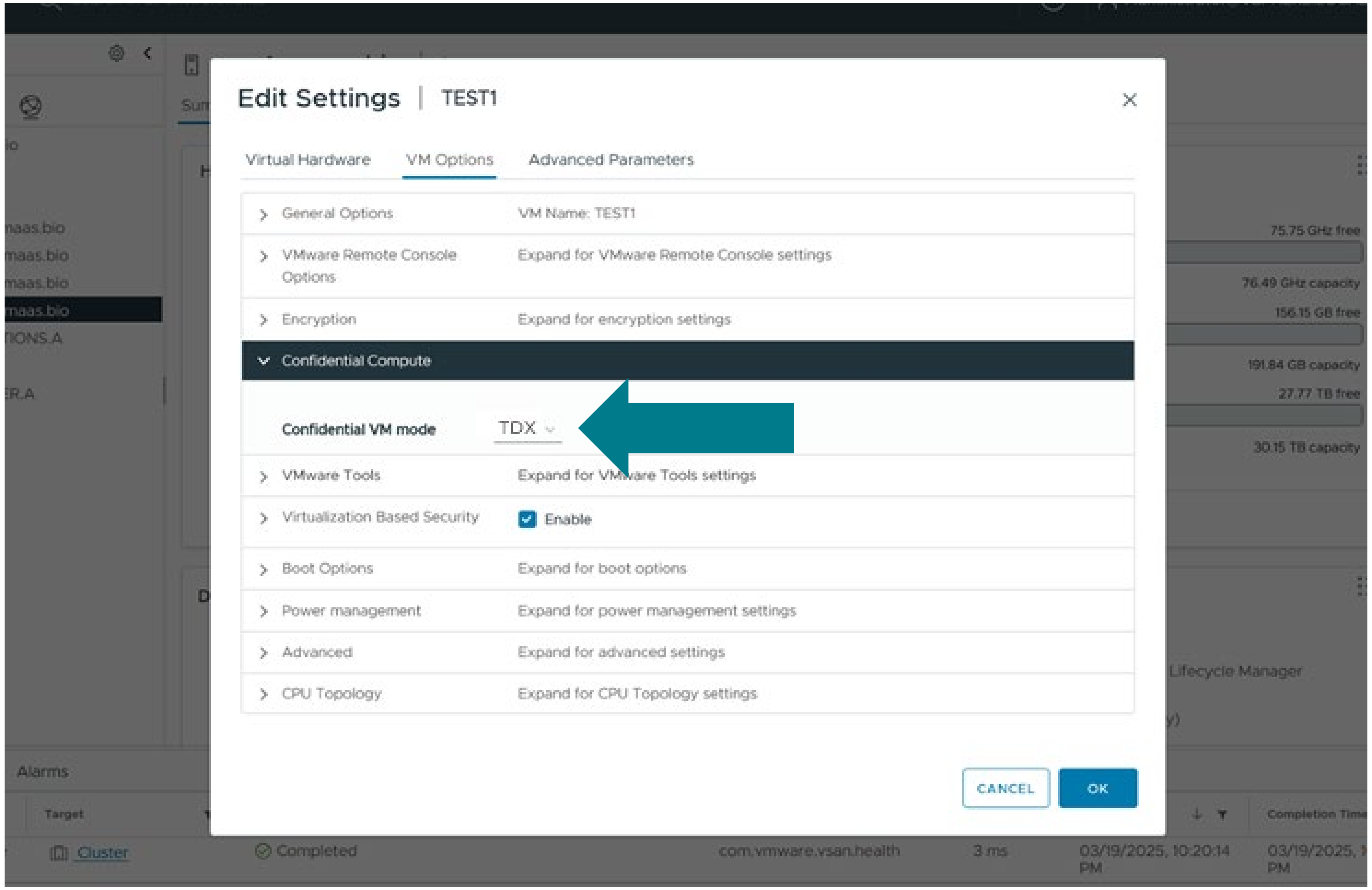
Attack Vector	Description	SGX	TDX	SEV	SEV-ES	SEV-SNP
VM Introspection	Read VM memory, set breakpoints, debug	Yes*	Yes	Yes	Yes	Yes
VM CPU Register State	Read VM register state after VMEXIT	Yes*	Yes	No	Yes	Yes
Memory Protections	Replace/remap VM memory	Yes, v2	Yes	No	No	Yes
DMA Protection	Device attempts to read memory	Yes*	Yes	Yes	Yes	Yes
DMA Integrity	Device attempts to write/corrupt memory	Yes*	Yes	No	No	Yes
Offline DRAM Analysis	DRAM retains data after power off	Yes	Yes	Yes	Yes	Yes
Active DRAM Corruption	“Rowhammer,” manipulation of DDR bus	No	No	No	No	No
Remote Attestation	Compromised platform	Yes	Yes	No	No	Yes
Secure Migration Support	Migration to another host with protections	No	TBD	No	No	Yes**

* Intel SGX does not protect entire VMs; instead, it allows the creation of smaller secure enclaves

** Hardware support from partner; Cloud Foundation support on roadmap

Reduce Trust of Your Underlying Hardware

Confidential Computing in VMware Cloud Foundation



Edit Settings | TEST1

Virtual Hardware | VM Options | Advanced Parameters

- General Options: VM Name: TEST1
- VMware Remote Console Options: Expand for VMware Remote Console settings
- Encryption: Expand for encryption settings
- Confidential Compute
  - Confidential VM mode: TDX
- VMware Tools: Expand for VMware Tools settings
- Virtualization Based Security: ☑ Enable
- Boot Options: Expand for boot options
- Power management: Expand for power management settings
- Advanced: Expand for advanced settings
- CPU Topology: Expand for CPU Topology settings

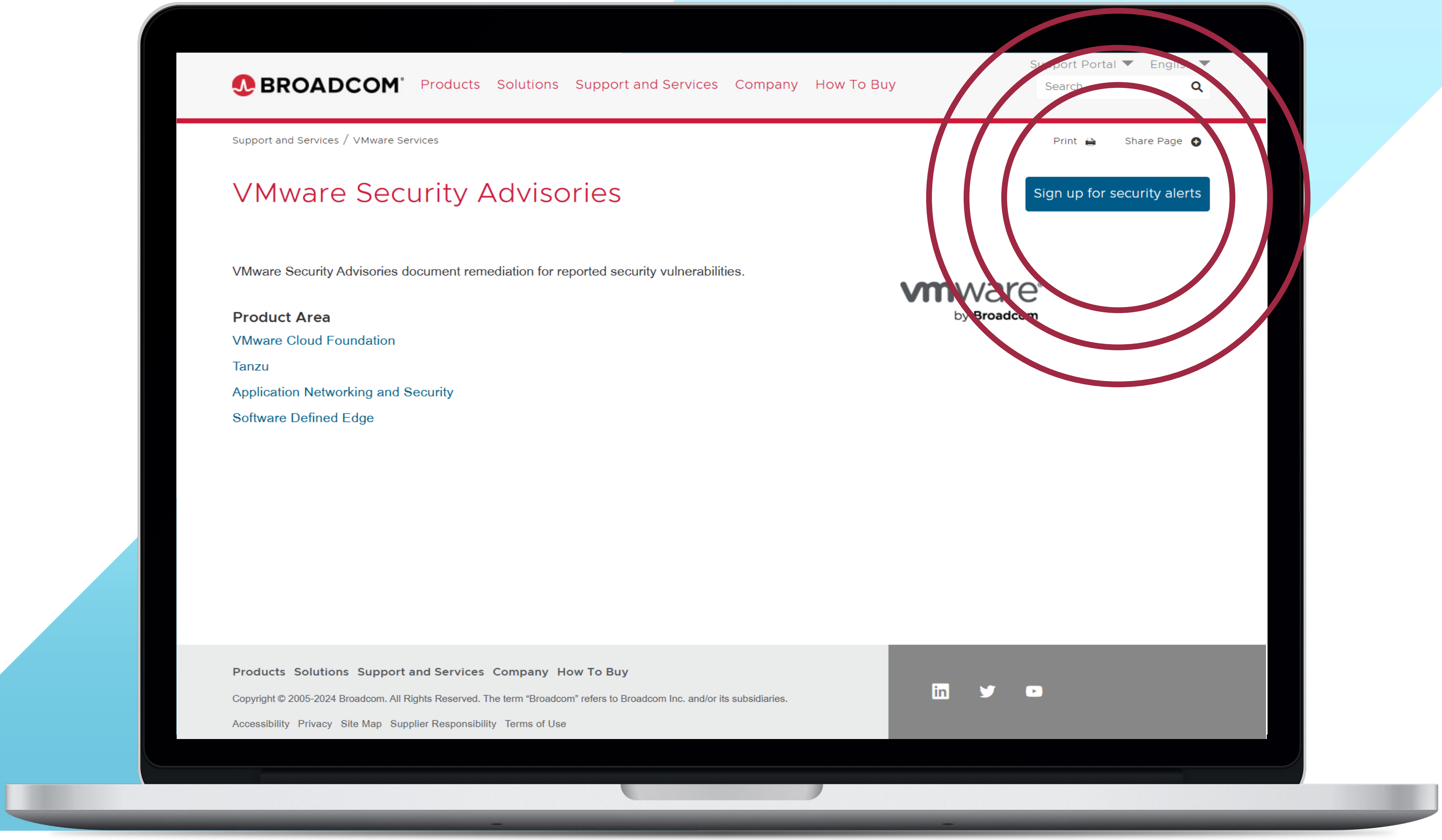
Confidential Computing started with vSphere 7

VCF 9 enables AMD SEV-SNP and Intel TDX protections

Enable Confidential Containers with AMD SEV-ES today

Rich roadmap going forward, deep security made easier

vmware® by Broadcom



Support and Services / VMware Services

VMware Security Advisories

Sign up for security alerts

VMware Security Advisories document remediation for reported security vulnerabilities.

Product Area

- VMware Cloud Foundation
- Tanzu
- Application Networking and Security
- Software Defined Edge

Security Hardening & Compliance Resources

https://brcm.tech/vcf-security

https://github.com/vmware/vcf-security-and-compliance-guidelines/

VMware Cloud Foundation 9

Thank You