enclaive

Transitioning Roadmap for Data Center Providers to a Confidential Cloud

Leveraging Confidential Computing and Buckypaper Virtualization

www.enclaive.io

Content Structure

You will read about:

1. Introduction 3
2. Background on Confidential Computing 4
3. enclaive’ Buckypaper Virtualization 7
4. Roadmap Phases 20
5. Conclusion 23

Abstract

The migration of data centers to the cloud offers significant advantages in terms of scalability, cost-effectiveness, and agility. **However, security concerns surrounding sensitive data processing in shared cloud environments remain a major hurdle.**

Confidential computing technology emerges as a game-changer, enabling organizations to leverage the cloud's benefits while ensuring data privacy and integrity.

This whitepaper explores the challenges of traditional cloud migration, introduces confidential computing concepts, and outlines a strategic approach for transitioning data centers to a confidential cloud environment supporting Buckypaper virtualization.

1. Introduction

The advent of cloud computing has revolutionized how data is stored, processed, and managed. However, as cloud adoption grows, so do concerns about data security and privacy. Traditional data center providers must evolve to meet these demands, ensuring that sensitive data remains secure throughout its lifecycle.

Many organizations, particularly those dealing with sensitive data, hesitate to migrate to the cloud due to security concerns. Traditional cloud models raise the following anxieties:

Multi-tenancy

Sharing resources with other cloud users in a multi-tenant environment poses a risk of data leakage or interference enclaive

Data Visibility

Cloud providers have inherent administrative access to the underlying infrastructure, raising concerns about potential data breaches or unauthorized access

Regulatory Compliance

Strict regulations in various industries (e.g., healthcare, finance) mandate specific data security protocols. Traditional cloud environments might not offer the necessary level of control to comply.

Liability

The growing landscape of cyberattacks, specifically those by dedicated special units of governments, puts a burden on a shared responsibility model. While customers typically are in charge of managing the security of what is “in” the cloud, data centers are urged to manage the security “of” the cloud.

2. Background on Confidential Computing

Confidential computing is a breakthrough technology that protects data in use by performing computations in a hardware-based Trusted Execution Environment (TEE).

2.1. Confidential Computing: A Paradigm Shift

Confidential computing offers a revolutionary approach to data security in the cloud.

This technology utilizes Trusted Execution Environments (TEEs) or secure enclaves, which are isolated hardware compartments within the main processor.

These enclaves protect data "in use" by encrypting it during processing, rendering it inaccessible to the cloud provider, other tenants, or even the operating system itself.

2.2 Benefits of Confidential Cloud

Transitioning data centers to a confidential cloud environment unlocks a multitude of benefits:

Enhanced Data Security

Confidential computing significantly reduces the attack surface, ensuring data privacy and integrity even in a shared cloud environment.

Regulatory Compliance

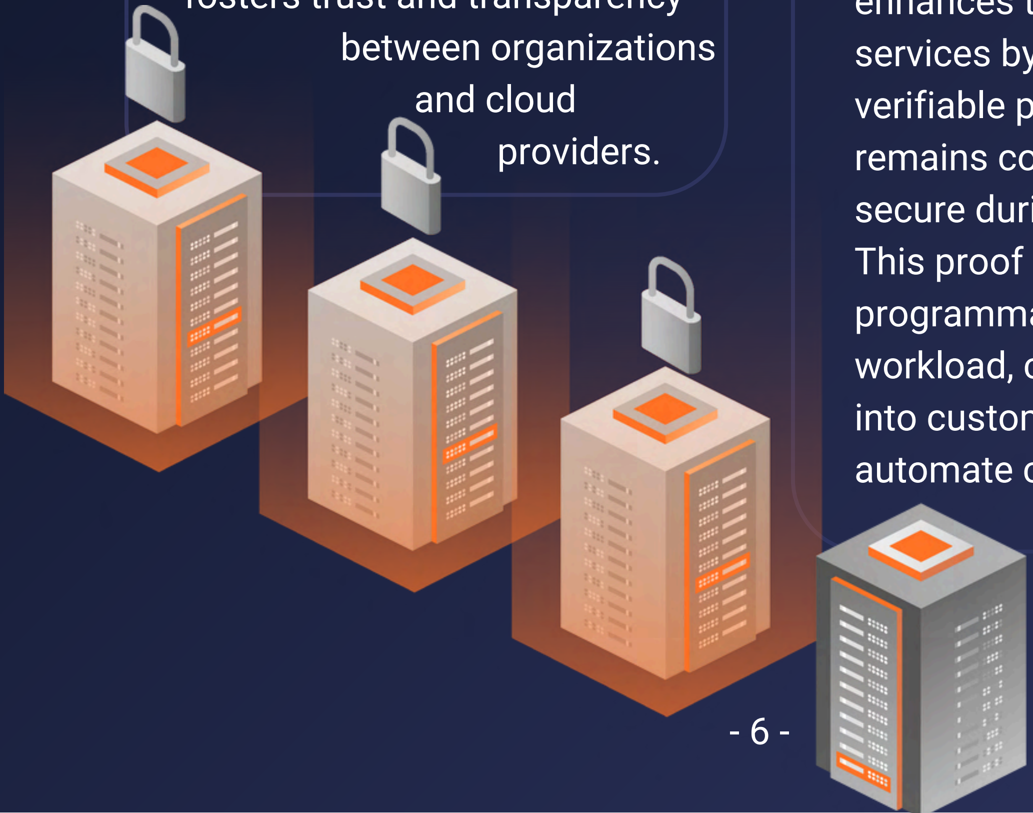
Organizations can leverage confidential cloud solutions to meet stringent regulatory requirements without compromising on cloud benefits.

Increased Trust

By mitigating data visibility concerns, confidential cloud fosters trust and transparency between organizations and cloud providers.

Trust and Transparency

Confidential computing enhances trust in cloud services by providing verifiable proof that data remains confidential and secure during processing. This proof allows to programmatically audit workload, can be integrated into customer SIAMs, and automate compliance efforts.



2.3 Technical Perks

Off-the-shelf hardware

Prior security hardening technologies prerequisited a crypto coprocessor like a TPM or HSM. Confidential Computing runs on standard CPUs that have an in-built crypto coprocessor on the SOC. Key technologies include Intel SGX, AMD SEV, and ARM CCA.

Negligible Performance Overhead

The fact that the security processor runs at 3GHz to 5GHz, the encryption engine on the CPU introduces 1-3% of additional CPU cycles to encrypt/decrypt the memory.

No change to code

Prior approaches to compute on encrypted data like fully homomorphic encryption or multi-party computation protocols required to recompile the program, making it unavoidable to access the source code. Confidential Computing comes as it is. You can run any program - even legacy 32-bit programs - without the need to make any modifications.

3. enclaive’ Buckypaper Virtualization

Entrypoint for Data Center Providers towards **confidential Virtual Machines**

	“Classical” Virtualization	“Buckypaper” Virtualization	Realization
Data-in-transit encryption	✓	✓	Secure Communication (e.g. SSH, TLS)
Data-at-rest encryption	✓	✓	Disk encryption (e.g. bitlocker, LUKS)
Data-in-use encryption		✓	Memory encryption (e.g. Intel TDX, ARM SEV)
Attestation		✓	enclaive’s vHSM/Nitride
Secret Provisioning		✓	enclaive’s vHSM/Vault

Tab.1: Technology comparison - classical vs. Buckypaper VMs

3.1 "Classical" Virtualization

Virtualization is the process of creating a virtual version of something, such as an operating system, a server, a storage device, or network resources.

This technology allows multiple virtual instances to run on a single physical hardware system, effectively partitioning it into several independent environments. Virtualization is typically managed by software known as a hypervisor, which sits between the hardware and the virtual machines (VMs), allowing multiple operating systems to run concurrently on a host computer.

Virtualization maximizes the use of physical resources by allowing multiple VMs to run on a single physical server, leading to better resource utilization. **It allows to scale resources up or down according to demand without needing additional physical hardware. The elasticity reduces hardware costs.**

Decreased need for physical servers reduces capital expenditure on hardware. Fewer physical servers result in reduced power and cooling requirements, leading to significant energy savings.

3.2. Buckypaper Virtualization

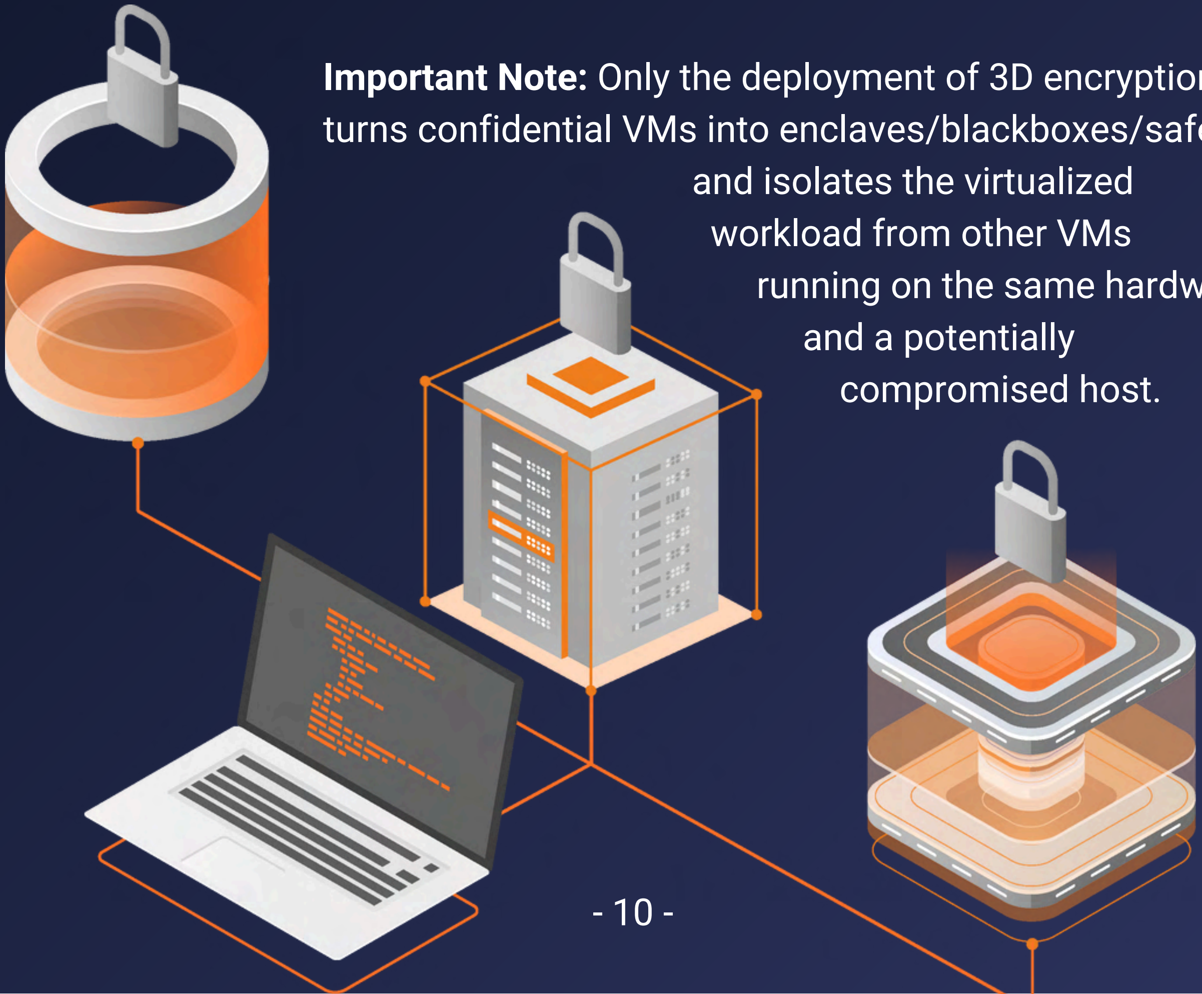
Leveraging confidential computing, **Buckypaper enables the virtualization of confidential VMs (cVMs)**. Confidential VMs are fully compatible Virtual Machines with the twist that they are 3D encrypted:

Data in transit: any communication to and from the Buckypaper VM is confidential and integrity-protected

Data at rest: any persistent storage to a block volume (or any other storage device/network) is confidential and integrity-protected

Data in use: any program execution in memory is throughout the runtime confidential and integrity protected

Important Note: Only the deployment of 3D encryption turns confidential VMs into enclaves/blackboxes/safes and isolates the virtualized workload from other VMs running on the same hardware and a potentially compromised host.



3.2. Buckypaper Virtualization

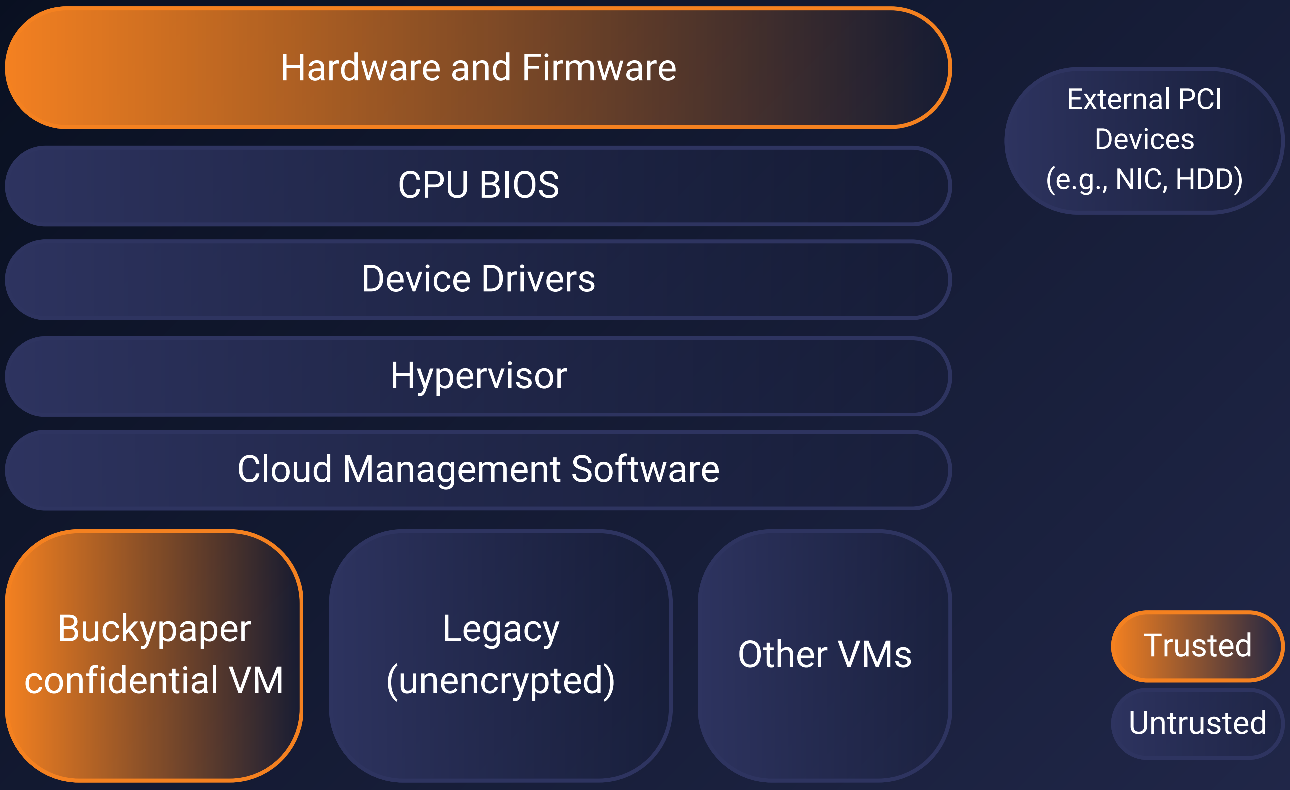
Comparing the trust model of "classical" with "Buckypaper" VMs reveals the following benefits:

The folklore understanding of "trust your host" is reduced to "trust your hardware"

Buckypaper VMs shield against compromised neighbour (unencrypted/encrypted) VMs and **protect against all forms of attacks that bypass the security perimeter** of the hypervisor ("vertical" isolation)

Buckpaper VMs shield against a vulnerable and/or compromised hypervisor and host ("horizontal" isolation). This feature releases the burden on data center providers (thus decreasing resources and costs) to implement a comprehensive methodology, making sure the host is well protected.

Implicitly, **Buckypaper VMs provide security irrespective of the data center's choice of hypervisor and cloud management software.** This feature makes it easier for data center providers to deploy buckypaper virtualization, as it does not interfere with the choice of the cloud management stack.



Hardware and Firmware

CPU BIOS

Device Drivers

Hypervisor

Cloud Management Software

Buckypaper confidential VM

Legacy (unencrypted)

Other VMs

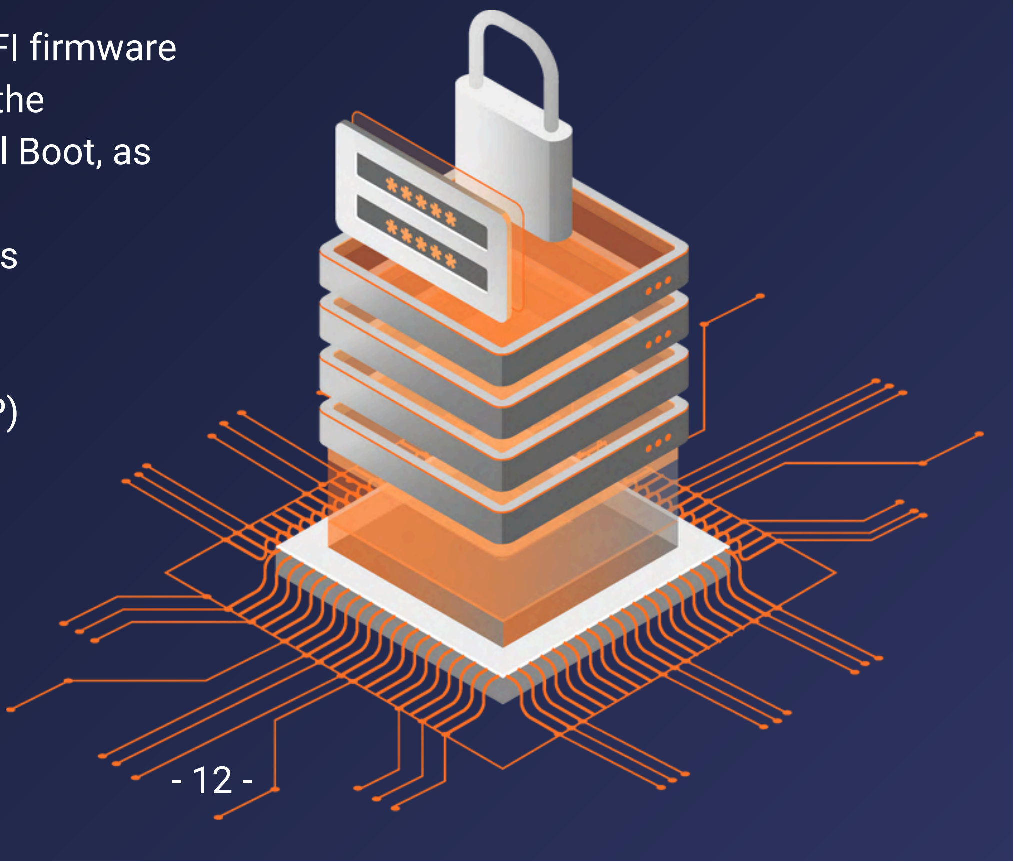
External PCI Devices (e.g., NIC, HDD)

Trusted

Untrusted

3.3 How does buckypaper virtualization work?

We have developed a UEFI firmware (FW-CB) that possesses the capability for Confidential Boot, as well as a Linux kernel that performs persistent hard disk encryption through the Secure Processor (SP) (kernel with Disc Encryption Layer).



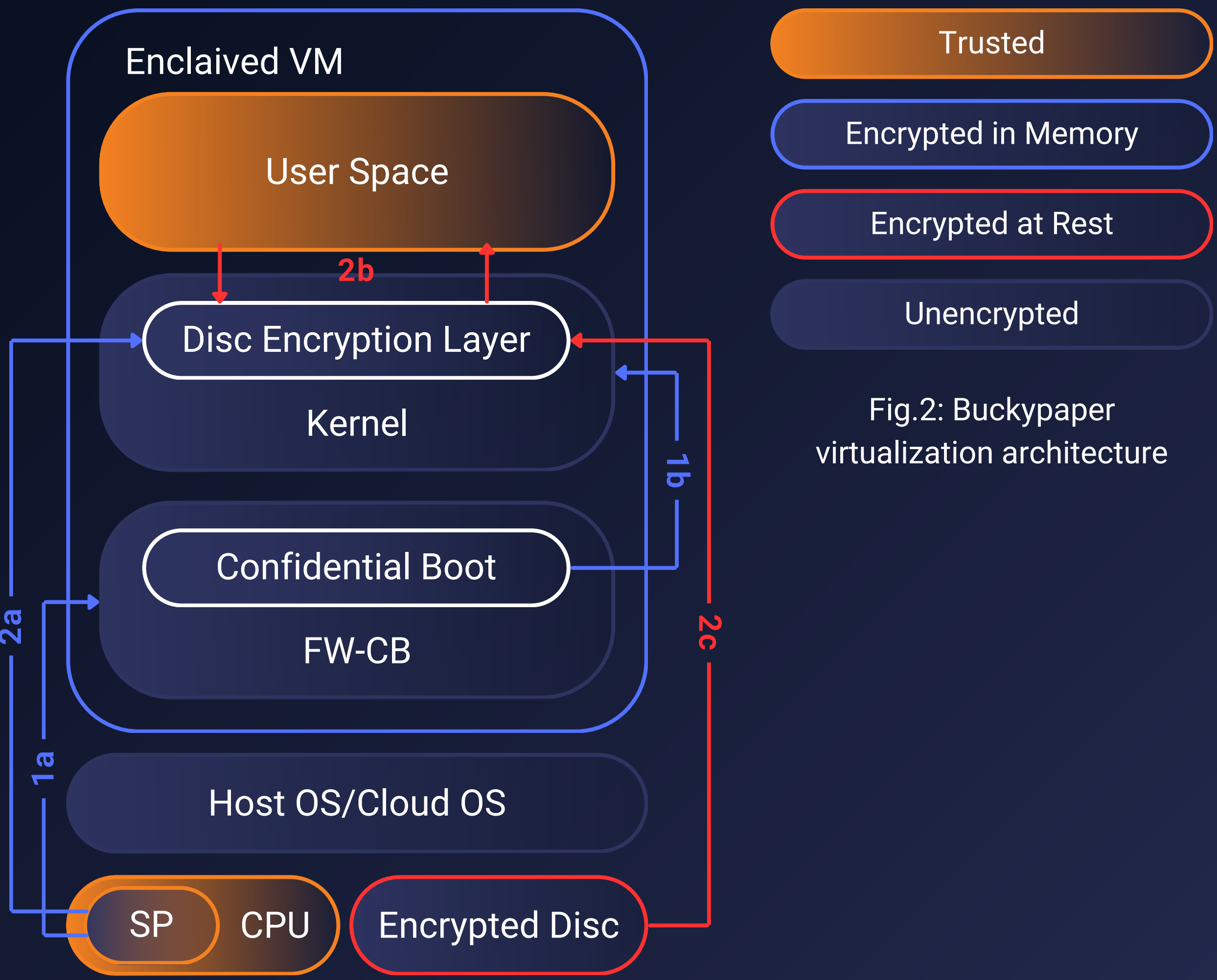


Fig.2: Buckypaper virtualization architecture

The execution of the Buckypaper takes place according to the following steps:

1a The SP allocates a special, "enclaved" memory area that the CPU knows is encrypted and can only be executed with the help of the SP. The SP generates a one-time AES key for encrypting this memory area, which is not accessible outside the CPU. The virtual machine is executed in this enclave. As a first step, FW-CB is loaded into the enclave, with the SP attesting to the firmware and thus ensuring the integrity of the following Confidential Boot process.

1b As a second step, the modified kernel is loaded into the enclaved memory area after the authenticity of the kernel binary has been verified by FW-CB.

2a Due to the successful attestation with the vHSM (see Section 3.4.3), the enclave is parameterized with secrets, config parameters, or additional packages. This includes, for example, platform-bound "Sealing Key" to decrypt the disk encryption key, environment variables to set admin passwords, or instructions to run applications/containers.

2b With the help of this Sealing Key, the persistent storage is decrypted. In this way, the “user space” application can be loaded into the enclave, decrypted by the Disk Encryption Layer, and executed in the enclaved environment. This includes not only the application code but also the Vault's secrets. Modifications to the application code are detected during decryption by the AES-GCM method, which is secure against Chosen Ciphertext Attack.

2c New secrets or changes to the user space are persistently encrypted with the help of the Sealing Key.

Additional Notes

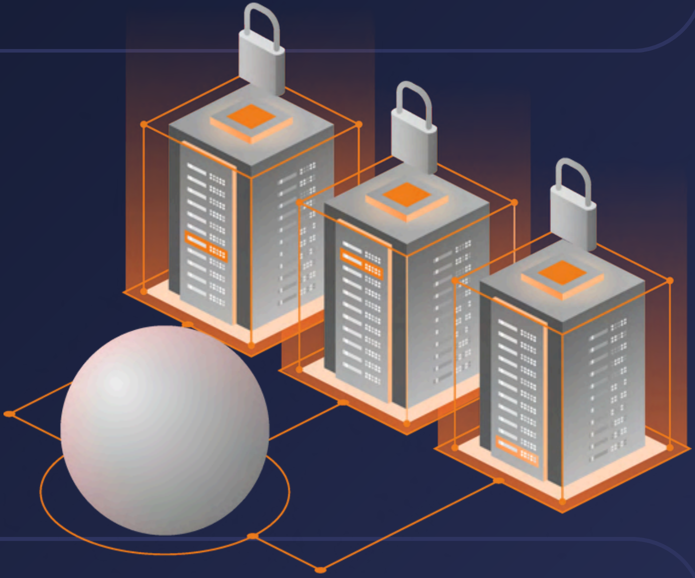
The term "Confidential Boot" refers to the process of booting a system in a way that protects the integrity of the boot process and ensures that only trusted code is executed.

Additional Notes

A "Secure Processor" (SP) is a hardware component that is designed to provide a secure environment for sensitive operations, such as cryptographic key generation and storage. It refers to TDX, SEV, or CCA.

A "virtualized Hardware Security Module" (vHSM) is a software implementation of a hardware security module that can provide the same level of security as a hardware HSM. enclaive's vHSM itself leverages a Buckypaper VM to run a comprehensive, cloud-agnostic key, identity, and access management.

A "Sealing Key" is a cryptographic key that is used to encrypt and decrypt data that is stored in a secure enclave.



The "Disk Encryption Layer" is a software component that is used to encrypt and decrypt data that is stored on a hard disk.

The "AES-GCM" method is a cryptographic algorithm that is used to encrypt and decrypt data. It is secure against Chosen Ciphertext Attack, which means that an attacker cannot decrypt a ciphertext without knowing the corresponding plaintext.

3.4 Technical Requirements

3.4.1 Hardware Requirements

Buckypaper Virtualization builds upon confidential compute enabled hardware:

Technology	CPU	Codename
AMD Secure Encrypted Virtualization (SEV)	EPYC 2 (SEV ES) EPYC 3 (SEV SNP) or later	Rome Milan
Intel Trusted Domain Extension (TDX)	Xeon Series 5 or related	Saphire Rapids Emerald
ARM Confidential Compute Architecture (CCA)	ARM Cortex A9	n/a

3.4.2 Software Requirements

Guest and host operating systems including the hypervisor need to be enriched to support the new security capabilities of CPUs (i.e. SEV, TDX, CCA). Typically the host kernel, hypervisor, guest UEFI, and guest kernel need patches to implement the support.

3.4.2.1. KVM / QEMU / LibVirt / Proxmox / Opentack

The necessary patches to support the security processor are currently discussed in the Linux kernel working group and are going to be upstreamed to mainline Linux kernel 6.11.

Patches address the host kernel/ kvm, qemu, UEFI and guest kernel. Linux distributions like SUSE Enterprise, Red Hat Enterprise or Ubuntu canonical have (partially) implemented the patches.

enclaive provides all patches for SEV and TDX for major Linux distributions and ready-to-use VM images (.iso, .ovf)

3.4.2.2 VMWare

In vSphere 7.0 Update 1 and later, you can activate Secure Encrypted Virtualization-Encrypted State (SEV-ES) on supported AMD CPUs and guest operating systems. Currently, SEV-ES supports AMD EPYC 2 CPUs (code named "Rome") and later CPUs, and only versions of Linux kernels that include specific support for SEV-ES.

VMWare plans to release updates in Q4/24 to support Secure Encrypted Virtualization-Secure Nested Pages (SEV SNP) and Intel Trusted Domain Extension (TDX).

3.4.3 enclaive's Virtual HSM (vHSM)

The virtual HSM (vHSM) is a hardware-graded full-fledged key management solution tailored towards confidential VMs. It consists of two applications, **Vault** and **Nitride**.

3.4.3.1 Vault

Vault is enclaive's Key, Identity, and Access Management solution. It is used to store secrets (including database passwords, disk encryption keys, and TLS certificates) and manage access. Buckypaper leverages Vault to provision secure secrets into the VM.

Key Features:

- **Identity Access Management** (username/password, TLS cert, passkey, ...)
- **Key Management** (Key Value store, SSH certs, kubeconfig, PKI-CA)
- **Access Control** (simple policy language)
- **Multi-tenancy**
- Transition to PQ-cryptography

3.4.3.2 Nitride

Nitride is enclaive’s Workload Identity Management solution. It is used to attest Buckypaper VMs and issue access tokens to Vault. Buckypaper leverages Nitride to attest its confidentiality and ask for permission to access Vault and retrieve keys it is only entitled to.

Key Features:

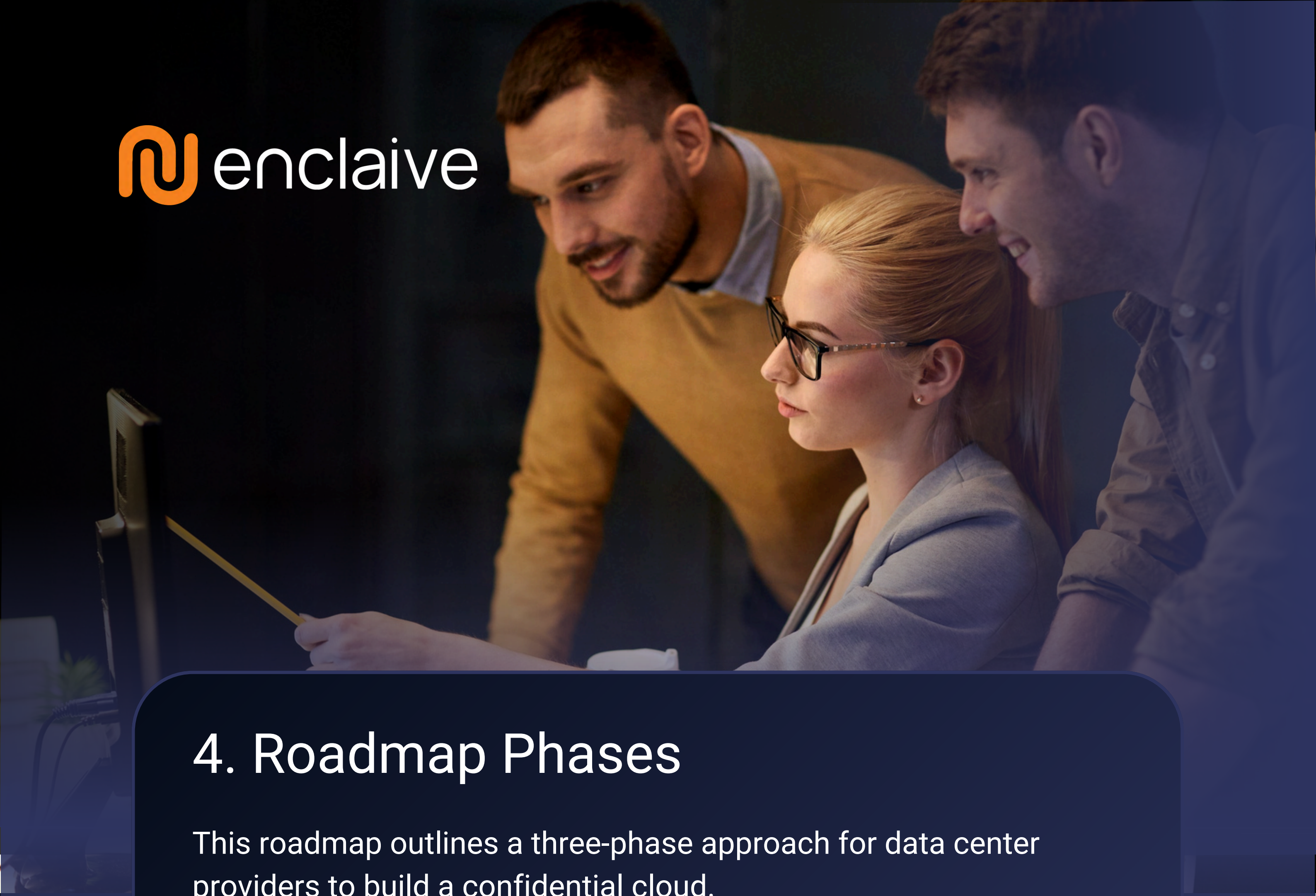
- **Identity Access Management** (username/password, TLS cert, passkey, …)
- **Attestation management and verification** (with support of SEV, TDX)
- **Attestation report export**
- Transition to **PQ-cryptography**

3.4.3.3 enclaivelet

The enclaivelet is an attestation shim (agent) running in the cVM. Its purpose is to allow Nitride to retrieve from the security processor the attestation report and to connect to Vault for secret provisioning.

Key Features:

- Shim to support SEV, TDX, and CCA attestation retrieval and key provisioning
- Available as binary, container, and sidecar



4. Roadmap Phases

This roadmap outlines a three-phase approach for data center providers to build a confidential cloud.

We remark that the estimated time covers a setup where no infrastructure is present. In practice, the efforts are significantly lower as data center providers typically possess the right hardware and already have the cloud management stack that needs to be patched.

Phase 1

Foundation Building

- **Technology Assessment:** Evaluate leading confidential computing technologies like Intel TDX, AMD SEV, and ARM CCA. Consider factors like performance overhead, ease of integration, and industry adoption.

Phase 1

Foundation Building

- **Infrastructure Upgrade:** Identify and procure hardware that supports the chosen confidential computing technology. This might involve upgrading CPUs, motherboards, and firmware.
- **Security Policy Development:** Define clear policies for access control, key management, and logging within the confidential cloud environment.
- **Team Training:** Train staff on confidential computing principles, security best practices, and operational procedures specific to the chosen technology.

Phase 2

Environment Development

- **Hypervisor Selection:** Choose a hypervisor compatible with confidential computing technologies. Explore options like KVM, vSphere, or confidential cloud-specific hypervisors.
- **Virtualization Strategy:** Develop a virtualization strategy of how to maintain CC-enabled VM images and manage customer cVMs.
- **Optional: Containerization Strategy:** Develop a containerization strategy utilizing technologies like enclaive's Dyneemes to leverage TEEs for secure processing within confidential containers (Kubernetes + kata containers).
- **Security Testing:** Conduct rigorous penetration testing and vulnerability assessments of the confidential cloud environment to identify and address potential weaknesses.

Phase 3

Service Deployment and Growth

- **Confidential Cloud Service Development:** Develop and offer confidential cloud services tailored to specific industry needs. This could include secure data analytics, confidential machine learning, or namespaces-as-a-service.

- **Partner Ecosystem Building:** Collaborate with software vendors and system integrators to create a robust ecosystem of confidential cloud-compatible applications and services.

- **Compliance Certification:** Pursue relevant industry compliance certifications like C5 or VS-NfD to demonstrate the security posture of the confidential cloud environment. enclaive supports data center providers in this process and has much of the documentation in place.

- **Marketing and Sales:** Launch marketing campaigns highlighting the benefits of confidential cloud to attract new security-conscious customers.

Benefits

By following this roadmap, data center providers can unlock the following benefits:

- **Increased Market Share:** Attract new customers hesitant to migrate sensitive data to the cloud due to security concerns.

- **Enhanced Brand Reputation:** Position your data center as a leader in secure cloud computing solutions.

- **Differentiation from Competitors:** Offer unique value proposition compared to non-confidential cloud services.

5. Conclusion

The shift towards confidential computing is inevitable. **Datacenter providers who act proactively and build a robust confidential cloud offering will be well-positioned to capture a significant share of the growing secure cloud market.**

This roadmap provides a blueprint for successful implementation, ensuring data security and customer trust are at the forefront of your cloud strategy.

Contact details

github.com/enclaive	contact@enclaive.io
linkedin.com/company/enclaive	+49 302 33 29 29 73
youtube.com/@confidentialcompute	Chausseestr. 40, Berlin, Germany

www.enclaive.io