enclaive

Confidential Computing

Confidential Computing stellt einen bahnbrechenden Fortschritt in der Datensicherheit dar. Damit können Umgebungen – ob Container, Anwendung oder virtuelle Maschinen – **vollständig verschlüsselt ausgeführt** werden.

Das bedeutet, dass diese Umgebungen während des gesamten Betriebszyklus, vom Start bis zur Beendigung, verschlüsselt bleiben. Durch diese Laufzeitverschlüsselung werden Daten und Programmflüsse **kryptographisch vom Rest des Systems isoliert**.

Nur die CPU - und keine anderen Komponenten oder Prozesse - kann diese verschlüsselte Umgebung entschlüsseln, Anweisungen ausführen und Ergebnisse dann wiederverschlüsselt speichern.

virtual HSM

Verbessern Sie Ihre Infrastruktur: Nutzen Sie Krypto-Agilität, Elastizität und Cloud-fähige Sicherheit!

Aktualisieren Sie Ihre Infrastruktur ohne kostspielige Hardwareinvestitionen. Nutzen Sie die Vorteile von Krypto-Agilität, Elastizität und Cloud-Bereitschaft für Geheimnisse und Workload-Identitätsmanagement.

vHSM kombiniert die Leistungsfähigkeit von Vault und Nitride nahtlos und bietet eine Komplett-Sicherheitslösung.

Mit dem starken Credential-Schutz von Vault und der sicheren Workload-Identitäts- und Zugriffsverwaltung (WIAM) von Nitride gewährleistet vHSM ein **Höchstmaß an Sicherheit** für Ihre Geheimnisse, Schlüssel und Maschinenidentitäten.

Vertrauen Sie auf hardwaregestützte Identitäten, automatisierte **Workload-Authentifizierung und Zugriffskontrollverwaltung** – alles in einem einzigen, umfassenden Paket.

enclaive

Aktuelle Herausforderungen

Betriebskosten

HSMs können die Kosten für native Cloud-Entwicklungsprojekte aufgrund zusätzlicher Wartungs-, Überwachungs- und Supportanforderungen erhöhen. Native Cloud-Anwendungen sind kostenoptimiert und benötigen möglicherweise keine HSMs, die teuer sind. Berücksichtigen Sie ihre Kosteneffizienz, bevor Sie HSMs für native Cloud-Entwicklungsprojekte einführen.

Latenzprobleme

Native Cloud-Anwendungen verwenden häufig Microservices-Architekturen und zielen auf Interaktionen mit geringer Latenz ab. Physische HSMs können jedoch eine zusätzliche Latenz einführen, die für einige cloudnative Anwendungsfälle möglicherweise nicht akzeptabel ist.

Skalierbarkeit

HSMs haben möglicherweise keine flexible bedarfsgesteuerte Skalierbarkeit, die für moderne Cloud-basierte Anwendungen unerlässlich ist. Das Hinzufügen weiterer physischer HSMs entspricht nicht den dynamischen Anforderungen moderner Geschäftsanwendungen.

vHSMs bieten das gleiche Maß an Vertrauen und Sicherheit, das in Hardware verankert ist, mit dem Vorteil, dass Funktionen in Enklaven verlagert werden.

enclaive

Elastizität:

Skalieren Sie die Ressourcen einfach und schnellnach oben oder unten, um den sich ändernden Bedarf zu decken. Dadurch wird sichergestellt, dass sich das vHSM an unterschiedliche Anforderungen anpassen kann, ohne dass eine Überprovisionierung erforderlich ist.

Hardware Trust Anchor:

Wählen Sie einen Hardware-Anker wie CPU, TPM, HSM oder Cloud HSM, um die Integrität der vertraulichen Boot- und Attestierungstechnologie von enclaive zu gewährleisten.

Skalierbarkeit:

Horizontale Skalierbarkeit beinhaltet das Hinzufügen weiterer vHSM-Instanzen zu einem System, um eine erhöhte Last zu bewältigen und vertrauenswürdige Domänen über mehrere, gegenseitig isolierte vertrauenswürdige Domänen/Organisationen zu erfassen. Vertikale Skalierbarkeit beinhaltet die Erhöhung der Kapazität und Leistung einer einzelnen Maschine, typischerweise zur Bewältigung von Hochleistungsanforderungen.

einfaches Einfügen:

Fügen Sie Funktionen schnell hinzu, aktualisieren oder entfernen Sie sie mit enclavierter Virtualisierung.

enclaive

Vorteile

Wirtschaftlichkeit

Elastizität hilft Unternehmen, ihre Ausgaben zu optimieren. Sie zahlen für die Ressourcen, die Sie verwenden, und Sie müssen nicht ständig Spitzenlasten bereitstellen. Dies kann zu Kosteneinsparungen führen, da Sie Ressourcen, die in Niedertarifzeiten nicht ausgelastet sind, nicht pflegen und bezahlen.

Krypto-Agilität

Verwalten Sie PKCS-, EC- und PQ-fähige Kryptografie flexibel und anpassungsfähig an sich ändernde NIST/BSI/NATO-Kryptografiestandards und kryptografische Durchbrüche.

Automatische Skalierung

Die Skalierbarkeit ermöglicht die automatische Bereitstellung und Aufhebung der Bereitstellung von Ressourcen basierend auf dem Echtzeitbedarf. Wenn das vHSM einen erhöhten Datenverkehr oder eine erhöhte Arbeitslast erfährt, kann es automatisch weitere Rechenressourcen (wie Virtual Machines) hinzufügen, um die Last zu bewältigen. Wenn der Bedarf sinkt, werdendie Ressourcen reduziert, um Kosten zu sparen.

Automatische Behebung

Wenn ein vHSM ausfällt, kann das vHSM es schnell durch einen neuen Cluster ersetzen und die Serviceverfügbarkeit über mehrere Server, Rechenzentren oder Cloud-Serviceanbieter hinweg aufrechterhalten. Verschlüsselter Speicher wird redundant repliziert und auf jede vHSM-Instanz versiegelt.

Schnellere Markteinführung

Fügen Sie ganz einfach neue Services oder Funktionen hinzu, ohne langfristige Investitionen zu tätigen. Sie können neue vHSM-Updates schnell testen und bereitstellen und so einfach anpassen, wie eine VM zu ersetzen.

enclaive

Implementierungsoptionen

vHSM Standalone

- Stellen Sie alle vertraulichen computerfähigen Systeme in Ihrer IT-Umgebung bereit.
- Implementieren Sie in IaaS-Umgebungen, die offen sind, um Confidential Computing zu unterstützen.

vHSM in der Cloud

- vHSM kann auf den derzeit von enclaive unterstützten Clouds eingesetzt werden:
- Die Hyperscaler (Azure, AWS, GCP)
- Ausgewählte regionale Anbieter

SaaS in der enclaive Cloud

- Hierbei handelt es sich um ein SaaS-Modell (Software-as-a-Service).
- Es ist einsatzbereit und wird in der Cloud-Infrastruktur von enclaive gehostet.

enclaive

Mehr erfahren

Über enclaive

Mit enclaive können Unternehmen ihre sensiblen Daten und Anwendungen **in nicht vertrauenswürdigen Cloud-Umgebungen sicher schützen**, indem sie den Einsatz von Confidential Computing nutzen.

Das umfassende Multi-Cloud-Betriebssystem ermöglicht die **Zero-Trust-Sicherheit**, indem es verwendete Daten verschlüsselt und Anwendungen sowohl von der Infrastruktur als auch von Lösungsanbietern abschirmt. Mit enclaive können Unternehmen eine Vielzahl von Cloud-Anwendungen souverän erstellen, testen und implementieren und gleichzeitig die vollständige **Kontrolle über ihre vertraulichen Informationen behalten**.

Das Ziel von enclaive ist es, eine universelle, cloud-unabhängige Technologie für die Enklave anspruchsvoller Multi-Cloud-Anwendungen bereitzustellen, die mit Sicherheit und Leichtigkeit implementiert werden kann.

Kontaktinformationen

github.com/enclaive

linkedin.com/company/enclaive

https://enclaive.io

youtube.com/@confidentialcompute

KONTAKT

contact@enclaive.io
+49 30233292973
Chausseestr. 40, 10115 Berlin, Germany
enclaive.io