

enclave Buckypaper

Hochsichere Confidential Virtual Machines mit resilienter Post-Quanten-Verschlüsselung

Virtuelle Maschinen sind ein zentraler Baustein moderner IT-Infrastrukturen. Doch ohne passende Sicherheitsmaßnahmen sind sensible Workloads hier unerwünschten Zugriffen durch Cyberkriminelle oder Cloud-Provider ausgesetzt. Mit Confidential Computing lassen sich virtuelle Maschinen in isolierten Enklaven auf CPU-Ebene verschlüsseln, um Daten durchgehend in allen drei Dimensionen (**at rest, in transit, in use**) zu schützen. Mit **Buckypaper** geht enclave noch einen Schritt weiter: Mittels Post-Quanten-Verschlüsselung werden nicht nur heutige Angriffe abgewehrt, sondern auch zukünftige Bedrohungen durch Quantencomputer.

Herausforderungen

Unternehmen stehen vor einem Dilemma: Klassische On-Premises-Strukturen sind teuer und unflexibel, die Migration in die Cloud erscheint vielen immer noch als komplex und unsicher – und wer den Weg in die Cloud gegangen ist, sieht sich einer weitläufigen Bedrohungslandschaft gegenüber, die durch Quantencomputer eine neue Dynamik entwickelt.



Hoher Kostenaufwand

On-Premises-Infrastrukturen erfordern hohe Investitionen und verursachen laufend Wartungsaufwand – von Hardware über Personal bis Security-Patches.



Ineffizienz & begrenzte Skalierung

Bei On-Premises müssen Ressourcen für Spitzenlasten vorgehalten werden, die dann oft ungenutzt bleiben. Flexibles Skalieren ist hier teuer und zeitaufwändig.



Komplexe Migration

Der Wechsel von On-Premises in die Cloud ist aufwendig. Daten und Anwendungen sind dabei ebenso sicher wie effizient zu übertragen.



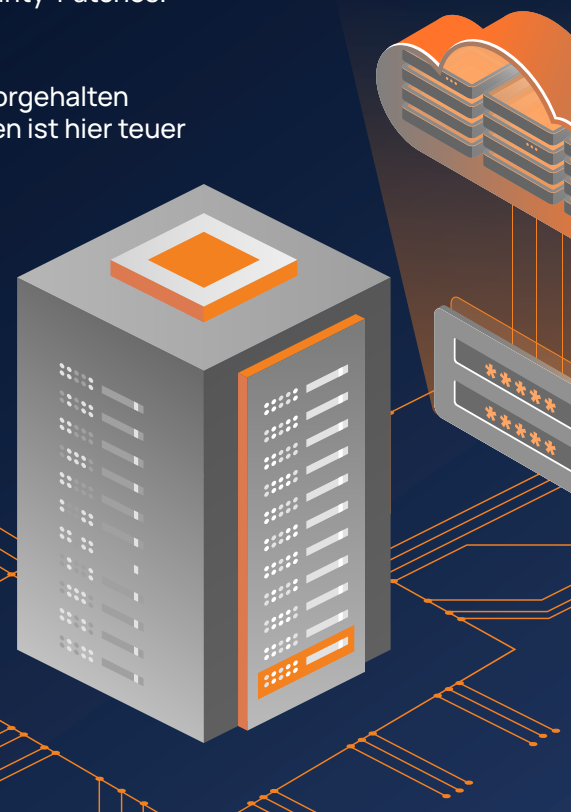
Vertraulichkeit

In klassischen Cloud-Umgebungen haben Administratoren und Betreiber theoretisch Zugriff auf sensible Workloads.



Cloud-Sicherheit im Quantenzeitalter

Verschlüsselung, Authentifizierung und PKI werden durch Quantencomputer bald angreifbar. Und bereits jetzt droht durch „Store now, decrypt later“-Angriffe immenser Schaden durch Datendiebstahl.



Unsere Lösung

Mit **Buckypaper** bietet enclaive eine Lösung, die Workloads in isolierten, hardwarebasierten Enklaven verschlüsselt. Daten sind so nicht nur im Ruhezustand und bei der Übertragung, sondern auch während der Verarbeitung geschützt. Damit erhalten Unternehmen vertrauenswürdige, zukunftssichere Umgebungen für ihre Workloads und können auch Shared Infrastructure bedenkenlos nutzen – in der Public Cloud ihrer Wahl.

Hardwarebasierte Sicherheit

Sensible Anwendungen laufen abgeschottet in einer sicheren Enklave. Selbst Administratoren oder Cloud-Provider mit Root-Rechten haben keinen Zugriff.

Workload-Isolation

Kritische Anwendungen werden zuverlässig von anderen VMs getrennt. Multi-Tenant-Umgebungen bleiben sicher, selbst wenn benachbarte Workloads kompromittiert sind.

Post-Quanten-Verschlüsselung

Unsere Enklaven bieten dank moderner Post-Quanten-Kryptografie maximalen Schutz für Ihre Daten und eine wirksame Verteidigung gegen Quantencomputer.

Compliance by Design

Die durchgängige Verschlüsselung von Daten und der Betrieb in zertifizierten EU-Rechenzentren (ISO27001, BSI-Grundschutz, C5) erleichtert die Einhaltung gesetzlicher und branchenspezifischer Vorgaben.

Optimierte Performance

Die Verschlüsselung in unseren Confidential VMs verursacht eine zusätzliche Rechenleistung von nur etwa 3 %. Die Folge: Volle Performance ohne Kompromisse bei der Datensicherheit.

Warum Sie auf Buckypaper setzen sollten

- ▶ **Langfristige Sicherheit:** Post-Quanten-Verschlüsselung schützt Ihre Daten dauerhaft – auch gegen Angriffe, die erst in Jahren möglich werden.
- ▶ **Maximale Vertraulichkeit:** Daten und Workloads bleiben jederzeit geschützt, unabhängig vom Cloud-Anbieter oder der zugrunde liegenden Infrastruktur.
- ▶ **Flexible Infrastruktur:** Wählen Sie frei zwischen US Hyperscalern oder europäischen Cloud-Anbietern – und erfüllen so passgenau ihre Compliance-Anforderungen.
- ▶ **Weniger Aufwand:** Automatisierte Updates und Security-Patches reduzieren den Betriebsaufwand und eliminieren Fehlerquellen.
- ▶ **Einfache Migration und Integration:** Unsere virtuellen Maschinen lassen sich ohne Codeänderungen einrichten. So migrieren Sie Ihre Workloads mühelos in die Cloud und sichern ihre bestehende Cloud-Architektur.