enclaive

Buckypaper

enclaive Buckypaper

Highly secure confidential virtual machines with resilient post-quantum encryption

Virtual machines are a cornerstone of modern IT infrastructures. However, without proper security measures, sensitive workloads remain exposed to unwanted access—from cybercriminals or even cloud providers. Confidential Computing encrypts virtual machines within isolated CPU-level enclaves, ensuring data protection across all three dimensions — at rest, in transit, and in use. With **Buckypaper**, enclaive takes this concept even further: by integrating post-quantum encryption, it not only protects against today's attacks but also against future threats posed by quantum computers.

Challenges

Organizations face a difficult trade-off: traditional on-premises infrastructures are expensive and inflexible, while cloud migration often appears complex and unsafe. And those who have already moved to the cloud now face an ever-expanding threat landscape—one that will soon evolve dramatically with the advent of quantum computing.

High Costs

On-premises infrastructures require major investments and ongoing maintenance—from hardware and staffing to security patching.

Inefficiency & Limited Scalability

On-premises setups must reserve capacity for peak loads, leaving resources underutilized most of the time. Scaling is costly and time-consuming.

Complex Migration

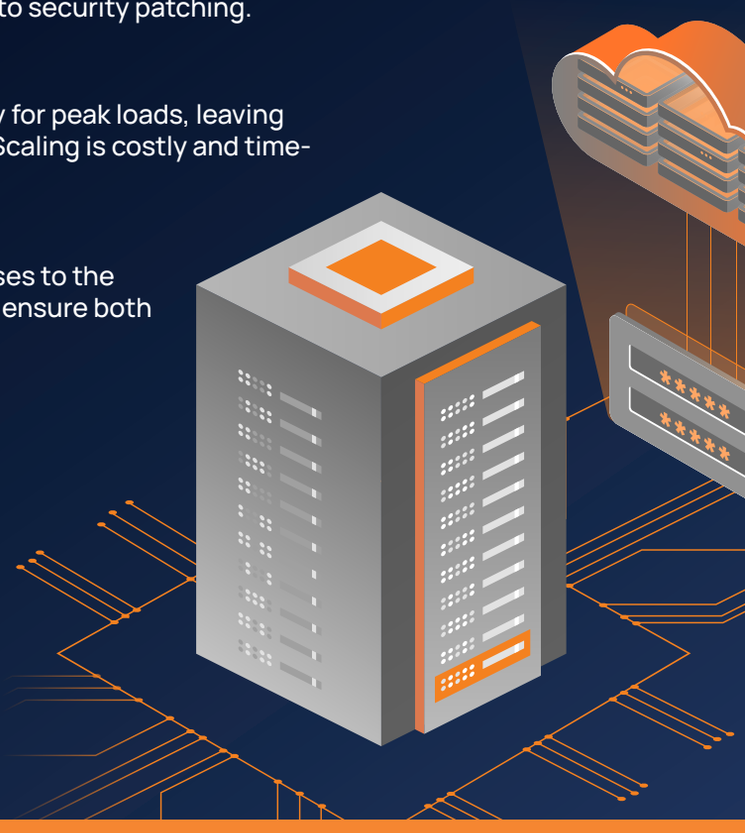
Moving workloads and data from on-premises to the cloud demands significant effort and must ensure both efficiency and data integrity.

Confidentiality Risks

In conventional cloud environments, administrators and operators can theoretically access sensitive workloads.

Cloud Security in the Quantum Era

Encryption, authentication, and PKI are becoming vulnerable to quantum attacks. "Store now, decrypt later" tactics already threaten massive data theft and future breaches.



Our Solution

With Buckypaper, enclaive provides a solution that encrypts workloads within isolated, hardware-based enclaves. Data is protected not only at rest and in transit, but also during processing. This creates trusted, future-proof environments for your workloads—enabling secure use of shared infrastructure in the public cloud of your choice.

Hardware-Based Security

Sensitive applications run within a secure enclave, completely isolated from the host system. Even administrators or cloud providers with root privileges cannot gain access.

Workload Isolation

Critical workloads are reliably separated from other VMs. Multi-tenant environments remain protected, even if neighboring workloads are compromised.

Post-Quantum Encryption

Our enclaves use state-of-the-art post-quantum cryptography, delivering maximum protection and robust defense against quantum-enabled attacks.

Compliance by Design

End-to-end encryption and operation in certified EU data centers (ISO 27001, BSI Grundschutz, C5) simplify compliance with legal and industry-specific requirements.

Optimized Performance

Our encryption only adds about 3% computational overhead, providing full performance with no compromises in data security.

Why Choose Buckypaper

- **Long-Term Security:** Post-quantum encryption protects your data permanently—even against attacks that may only become feasible years from now.
- **Maximum Confidentiality:** Data and workloads remain encrypted at all times, regardless of the cloud provider or underlying infrastructure.
- **Flexible Infrastructure:** Freely choose between US hyperscalers or European cloud providers to meet your exact compliance requirements.
- **Reduced Operational Effort:** Automated updates and security patching minimize administrative workload and eliminate potential human error.
- **Seamless Migration and Integration:** Our virtual machines deploy without any code changes, allowing effortless workload migration to the cloud and secure integration into your existing architecture.

Learn more:
enclaive.io/buckypaper-confidential-virtual-machines

Mail: contact@enclaive.io
Tel.: +49 302 33 29 29 73
Chausseestr. 40, Berlin, Germany