

MAKING THE CLOUD THE SAFEST PLACE

---

SOLUTION BRIEF

# Quantum Enclaves

A pragmatic approach to security architectures for the post-quantum era



---

# Executive Summary

**Quantum computing is on the rise – and it will fundamentally change what we understand by digital security: encryption methods that are considered unbreakable today could soon be cracked within minutes.**

Companies are therefore facing the challenge of protecting their critical data, applications and services now – before the so-called Q-Day arrives.

Quantum Enclaves by enclave support this approach: as a post-quantum-ready security foundation, they enable sensitive workloads to be executed in isolated, certified enclaves, using cryptographic standards that are already resilient to future quantum attacks. All without code adjustments, change of infrastructure or operational complexity.

# Security With an Expiration Date

Quantum computers will render today's common cryptography obsolete and mark the end of most traditional methods – from RSA and ECC to Diffie-Hellman. Despite early initiatives, standards and pilot projects, post-quantum security (PQS) is still a young topic: according to a 2025 Utimaco study, only around 20% of companies have begun migration. 34% want to start in the next 1 to 3 years, while 25% have no plans yet.

In the wake of the quantum revolution, companies must prepare themselves for a range of new threat models:

- **Cryptography, authentication and PKI are being undermined:** Digital identities, signatures and certificates are no longer secure – with far-reaching consequences for online banking, e-government, supply chains and the entire internet.
- **„Harvest now, decrypt later“ becomes reality:** Many attackers have been storing encrypted data for years to decrypt it in the future using quantum computers. Huge amounts of highly sensitive data with a long lifespan are at risk – from health records to state secrets to intellectual property.
- **Quantum-resistant ransomware:** The next generation of ransomware attacks could use post-quantum cryptography to make encryption even more difficult to crack.
- **Sabotage of blockchains and cryptocurrencies:** Many cryptocurrencies are based on elliptic curve cryptography. A quantum computer could compromise wallets or destabilise entire blockchains.

**65%**

of organisations view 'harvest now, decrypt later' attacks as particularly worrying (Capgemini, 2025)

**~60%**

expect the so-called Q-Day – the day when classic cryptography is effectively broken – to arrive within the next 10 years

## Regulatory Pressure Increases

At the regulatory level, the European Commission issued a recommendation in 2024 that requires member states to develop viable strategies for post-quantum cryptography. Both NIS2 and DORA also call for verifiable protection of critical IT infrastructures. The GDPR requires the best possible protection of personal data. And official bodies such as the German BSI are proactively calling for PQ transformation. Companies therefore need to make this issue a priority.

In addition to regulatory demands, technical pressure is also growing: more than ever, it is important to reliably protect data and systems with a long lifespan – from ATMs and medical technology to industrial plants – from quantum attacks using future-proof cryptography.

# enclave Quantum Enclaves

When companies take their first practical steps towards PQS, they usually focus initially on cataloguing the cryptographic methods used and classifying particularly sensitive data sets. Then they launch their first pilot projects, which usually take a hybrid approach to the issue, combining traditional methods with post-quantum cryptography.

However, the topic of post-quantum encryption can also be tackled in a completely different way: modern approaches in the field of confidential computing protect data not only at rest or in transit, but also in use – the part that traditional methods cannot protect. Confidential computing does this by moving sensitive workloads to hardware-based, isolated ‘trusted execution environments’ (TEEs) – also known as enclaves – thus protecting data from unauthorised access in all three dimensions.

THE QUANTUM ENCLAVES COMPRISE THE FOLLOWING SOLUTIONS FROM THE ENCLAVE PORTFOLIO



With **Buckypaper**, enclave offers confidential virtual machines (cVMs) – VMs that run in a highly secure manner in hardware-based enclaves. This form of virtualisation offers a secure path to the cloud, protects against unwanted access and facilitates lift-and-shift migrations, as cVMs and enclaves can usually be integrated without code changes – or, if necessary, they can be configured exactly like the previous on-premises environment.



**Vault** enables cross-cloud key management based on the Hold-Your-Own-Key principle. Based on the vHSM, users retain control over their cryptographic keys at all times and ensure that only they can decrypt the enclaves. This makes Vault a literal key factor for digital sovereignty.



The **vHSM** (virtual High Security Module) is enclave’s innovative, cloud-native encryption module. It offers scalable, cost-efficient security for keys, identities and workloads – at the high level of physical hardware. It enables modern key and identity management, meets the highest compliance requirements and integrates seamlessly into any cloud environment. As a cloud-native solution, it is also always up to date in terms of encryption technology and regulatory requirements.



**Nitride** assigns unique identities and granular access privileges to workloads and users. Cryptographic attestation ensures that enclaves only boot with verified, trusted components. This gives you verifiable integrity for confidential workloads and makes it easy to meet compliance and audit requirements.



The **eMCP** (enclave Multi-Cloud Platform) is a secure, multi-tenant platform that allows confidential databases, virtual machines and containers to be set up, operated and scaled across different cloud providers. Users control their entire multi-cloud environment via a central dashboard – from resource and access management to central security and automation settings to monitoring and detailed analysis.

Based on these confidential computing solutions from enclave, the Quantum Enclaves transform applications into isolated, post-quantum encrypted and attested security areas without any code modification. This ensures that data is processed securely in the cloud and that secrets are reliably prevented from ever becoming visible in plain text – neither to administrators, attackers, compromised operating systems nor curious cloud providers.

With Quantum Enclaves, companies are already setting the course for long-term digital sovereignty and retaining control over their keys and data at all times. This is a crucial competitive advantage, particularly in light of potential activities by state actors with powerful quantum technology.

---

**This approach not only provides companies with a high level of security for today, but also lays important groundwork for the security architectures of tomorrow: investing now creates a solid foundation on which post-quantum cryptography can be seamlessly integrated and continuously adapted to new encryption methods.**

# Protecting You Today and Tomorrow

Quantum Enclaves by enclave offer companies three key advantages:

01

## Future-proof Security Architecture

With Quantum Enclaves, companies benefit from a highly secure environment in which they can reliably protect and operate applications and data – both today and in the post-quantum era. The solution provides a pragmatic and operational response to the uncertainty surrounding the point at which classical cryptography will fail.

02

## Setting the Course for Compliance and Governance

Auditable attestation and guaranteed isolation enable companies not only to meet regulatory requirements, but also to prove compliance conclusively to auditors – including data sovereignty, cloud independence and controllable security domains.

03

## Quantum Readiness as a Growth Driver

The additional security also offers tangible economic benefits – from lower liability risks and lower incident handling costs to shorter audit cycles and reliable protection of business-critical secrets. This enables companies to not only strengthen their security strategy, but also actively use it as a driver of innovation.

## Use Cases

The use of Quantum Enclaves is particularly recommended for workloads with high risk levels, for example:

- **Finance and payment services:** In the financial sector, strict compliance requirements – increasingly also for post-quantum cryptography – apply to confidential data such as credit reports and securities, transaction histories and risk analyses. Quantum Enclaves protect this long-lived financial data, ensure the secure exchange of information across institutional boundaries, and thus create a trustworthy basis for digital assets and payment infrastructures.
- **Government and critical infrastructure:** Public registers, classified information, and critical infrastructure (KRITIS) must be particularly well protected for the long term. Post-quantum enclaves secure them against current and future decryption attacks, safeguard administrative processes and ensure the availability of digital services. They strengthen both internal and national security by making government and military networks, government operations and critical infrastructure long-term resilient against espionage and manipulation.

- **Healthcare:** Medical data is highly sensitive and often relevant for an entire lifetime. Quantum Enclaves protect this data in a future-proof manner – and ensure that information can be exchanged securely between organisations, institutions and authorities in safe data spaces. This improves patient care, research and decisions on healthcare policy, while also meeting the high regulatory requirements of the GDPR, and – in Germany – the BSI and gematik.
- **Industrial IoT:** In industrial environments, post-quantum enclaves secure connected devices, machine configurations and trade secrets in any environment, even in third-party data centres. Neither compromised hosts nor side-channel attacks or unauthorised provider access jeopardise the integrity or confidentiality of the data. Confidential computing effectively prevents cyber sabotage and enables companies to implement robust micro-segmentation, tamper-proof remote maintenance and protected digital twins.
- **AI & Machine Learning:** AI models and training data are among the most valuable intellectual property of many companies. Quantum Enclaves protect model artefacts, feature stores and entire inference pipelines from data theft. They also enable confidential training (federated learning, secure aggregation) and secure interaction with internal models. In addition, enclaive offers Garnet, a GenAI firewall that filters and pseudonymises sensitive information within the enclave before it interacts with external AI models.

---

## Conclusion

Quantum Enclaves encapsulate applications in a hardened execution environment that is cryptographically attested and fully encrypted. The processes run as if in a digital safe that remains hidden even from the operator.

Based on standardised interfaces, this solution can be seamlessly integrated into Kubernetes clusters, multi-cloud deployments or on-premises architectures. Companies retain full sovereignty and control over keys and location – even when using public cloud resources.

**enclaive therefore acts as a bridge: from today's infrastructures to a fully post-quantum-secure IT landscape. Existing protection remains in place and continues to grow with future standards.**

---

NEXT STEPS

# Start your post-quantum journey now!

The migration to the post-quantum era is not a sprint, but a transformation. However, it begins with a single, crucial step: protecting the most important data first.

enclave provides a quick and low-risk introduction:

Joint quantum readiness workshop

Identification of critical workloads

PoC deployment of selected applications in quantum enclaves

Compliance mapping and operational integration into DevSecOps processes

If you start this journey with us today, you will benefit twice over: you will immediately gain greater security – and lay a solid foundation that will endure in the post-quantum future.

---

CONTACT

[sales@enclave.io](mailto:sales@enclave.io)

MORE INFORMATIONEN

[enclave.io](https://enclave.io)

 **enclave**