

Nitride

Your stepping stone into the Confidential Cloud

Leveraging confidential compute, Nitride ensures only attested workloads can access specific resources and data within a cloud infrastructure.

Your cloud knows more about your workload than you

Using cloud services exposes organizations to various **security, and privacy risks, and compliance risks.**

Cloud computing leaks any workload and opens the gateway to bad actors, cyber attacks and industrial espionage. BYOK, data-at-rest or in-transit encryption do not **protect from leaking sensitive data while in use.**



About Confidential Computing



Confidential computing represents a breakthrough advancement in data security. It enables environments - whether container, application or VM - to **run in a fully encrypted form.**

This means that throughout the entire operational cycle, from startup to termination, these environments remain encrypted. Data and program flows are **cryptographically isolated from the rest of the system** thanks to this runtime encryption.

Only the CPU - and no other components or processes - can decrypt this encrypted environment, execute instructions, and then store results in encrypted form again.

Current Challenges



Workload Residency

Organizations must adhere to data residency requirements, ensuring data stays within specific geographical boundaries. Relying on the cloud provider's security measures may not be sufficient to meet these regulatory demands.



Loss of control

Organizations have limited control over how their data is processed and who accesses it within the cloud environment. This lack of transparency can make it difficult to detect and respond to security incidents.



Workload Governance

Organizations may struggle to enforce their own data governance policies, data retention schedules, and compliance requirements when relying solely on the cloud provider's measures. This can result in non-compliance with industry regulations and internal policies.



Limited visibility

Organizations have limited visibility into how their data is processed and who accesses it within the cloud environment. This lack of visibility can make it difficult to detect and respond to security incidents.

Current Challenges



Zero-Trust

When data is processed, it is reliant on the cloud provider's access controls. This dependence can be risky, as breaches or misconfigurations within the provider's infrastructure lead to unauthorized access.



Cloud Service Provider Vulnerabilities

While cloud service providers implement robust security measures, vulnerabilities can still exist in their infrastructure. Cloud IAM services are appealing targets to attack. A single exploit can grant immediate access to millions of accounts.

Nitride makes the difference between confidential and non-confidential infrastructure

Workload-based Access Control:

Implement robust access control and management policies to ensure only authorized users and attested workloads access data, processes, and services.

Supply Chain Immutability:

Protocol of the hardware and software supply chain, including firmware, program code, image repositories, and packages. Validate supply chains and implement automated mechanisms for monitoring the trustworthiness of workloads.

Workload Identification:

Leveraging confidential compute, cloud workloads have a unique cryptographic identity.

Confidential Environments:

Confidential workloads can be securely run in private, hybrid, or multi-cloud environments, with fine-grained privileges enforced for accessing the workload by organizations, groups, users, and services.

Benefits

▶▶ Secure Cloud Migration

Transition your IT infrastructure to the cloud securely by leveraging the power of confidential computing. This approach ensures that only authorized workloads, applications, and services have access to specific resources, thereby reducing the risk of unauthorized access, data breaches, and insider threats.

▶▶ Automated Access Management

Streamlining access control automates resource provisioning and de-provisioning while ensuring appropriate permissions and dynamic access rights updates.

▶▶ Audit and Reporting

Specific regulations regarding data processing and storage, such as GDPR, HIPAA, NIS2 can be complex. Decrease the complexities for reporting and auditing, with workload identification in conjunction with hardware-graded boot measurement.

▶▶ Reduced Attack Surface

Limiting access to resources managed by the cloud service provider reduces the attack surface, making it harder for malicious actors to exploit vulnerabilities or launch cyberattacks.





Deployment Options

Nitride standalone*

- Flexible deployment option.
- Can be deployed on any hypervisor.
- Can be installed on bare metal infrastructure.
- Allows the user to choose their operating system.

Nitride integrated with vHSM*

- This is a cloud-ready offering.
- It seamlessly integrates with vHSM (Virtual Hardware Security Module).
- Utilizes encryption functionality from either AMD or Intel.

SaaS in der enclave Cloud

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

*Prerequisite for Nitride is a Key Management solution, like enclave Vault

Learn more

About enclave

enclave enables businesses to securely **protect their sensitive data and applications in untrusted cloud environments** by leveraging the use of Confidential Computing.

Its comprehensive, multi-cloud operating system allows for **Zero Trust security** by encrypting data in use and shielding applications from both the infrastructure and solution providers.

With enclave, businesses can confidently build, test, and deploy a wide range of cloud applications, all while **maintaining complete control over their confidential information**. enclave's goal is to provide a universal, cloud-independent technology for enclaving sophisticated multi-cloud applications, that can be deployed with confidence and ease.

Contact details



github.com/enclave



[linkedin.com/company/enclave](https://www.linkedin.com/company/enclave)



<https://enclave.io>



[youtube.com/@confidentialcompute](https://www.youtube.com/@confidentialcompute)

CONTACT

contact@enclave.io

+49 30233292973

Chausseestr. 40, 10115 Berlin, Germany
enclave.io

**Making the Cloud the
safest place for
digital businesses**