enclaive NITRIDE

WHAT IS NITRIDE?

Your stepping stone into the Confidential Cloud

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

Using cloud services exposes organizations to various security, privacy, 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.

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

Nitride also ensures peace of mind, with features like workload-based access control, confidential environments, and supply chain integrity.

> Nitride enhances cloud security and efficiency, streamlining identity verification and access policy enforcement across diverse platforms.

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.

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.

CASE STUDY

MOVE TO THE CONFIDENTIAL CLOUD WITH CONFIDENCE

Transition to Confidential Cloud Computing:

Organizations are increasingly recognizing the need to implement robust security measures independently of cloud service providers (CSPs). This shift is driven by complexities in CSP contractual agreements and evolving cybersecurity regulations, which often limit the CSPs' liability in data breaches, posing challenges in ensuring customer trust and data protection.

The Challenge:

Standard CSP contracts can contain clauses that limit provider liability in data breaches. This, coupled with evolving cybersecurity regulations, makes it difficult for organizations to assure customers of robust data protection, potentially eroding trust.

The Nitride Solution:

The enclaive solution leverages confidential computing technologies, enabling organizations to create secure enclaves for cloud workloads. This ensures that sensitive data remains encrypted and protected, offering a more independent and resilient security framework in the cloud. Enclaive's Workload Identity and Access Management solution is pivotal for organizations adopting enclave-based security for their workloads.

Benefits of Using Nitride:

Workload Confidentiality and Integrity:

- Ensures data confidentiality and integrity, especially for sensitive workloads.

Granular Access Controls:

- Allows precise management of resource access within the enclave, enforcing the principle of least privilege and reducing unauthorized access risks.

Resilience Against Insider and Outsider Threats:

- Guards against both insider and outsider threats by limiting access to only necessary resources, even for legitimate users, adding an extra layer of protection against malicious activities.

Operational Efficiency:

- Streamlines identity and access management of enclaves, enhancing operational processes and contributing to overall efficiency.

WHY DO YOU NEED NITRIDE?

Nitride makes the difference between confidential and non-confidential infrastructure

Workload Identification

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

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 Integrity

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.

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 on enclaive Cloud

- This is a Software-as-a-Service (SaaS) model.
- It's ready-to-use and hosted on enclaive's cloud infrastructure.

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

LEARN MORE

About enclaive

enclaive 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 enclaive, businesses can confidently build, test, and deploy a wide range of cloud applications, all while maintaining complete control over their confidential information. enclaive'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/enclaive

linkedin.com/company/enclaive

https://enclaive.io

youtube.com/@confidentialcompute

CONTACT

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