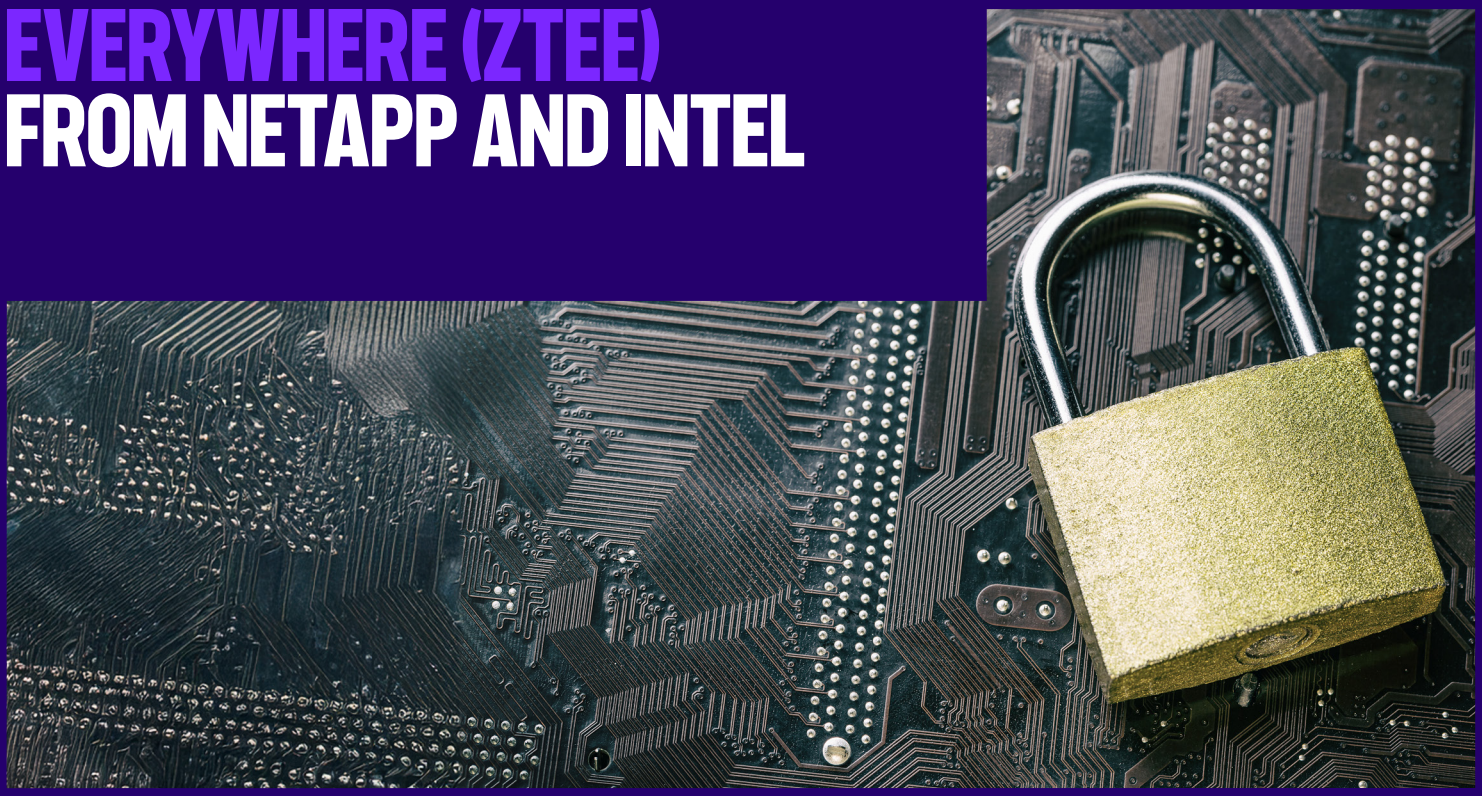
SOLUTION BRIEF

ZERO TRUST ENCLAVES EVERYWHERE (ZTEE) FROM NETAPP AND INTEL



Leverage confidential computing to close a major gap in your data protection continuum.

Enterprise companies and large government agencies are driving digital transformation and adopting new AI technologies to improve efficiency and optimize decision-making. These organizations are also increasingly turning to hybrid cloud infrastructure to rapidly scale AI and operations. While this move increases efficiency, it also exposes their systems and data to cybersecurity risks that can compromise data privacy and security.

Get the most out of data without compromising privacy

Successful digital transformation requires the implementation and strict enforcement of robust data security policies for AI and cloud infrastructure. Zero Trust Enclaves Everywhere (ZTEE) from NetApp and Intel is a solution that addresses threats to data at rest, data in flight, and—perhaps most challenging—data in use. ZTEE closes the data protection loop by pairing Intel confidential computing with NetApp® ONTAP® software and enabling attribute-based access control (ABAC), retrieval-augmented generation (RAG), and large language models (LLMs).

ZTEE enables organizations to take full advantage of digital transformation by providing foundational data security at the hardware level. This approach not only protects data across the entire environment, but it also allows organizations to extract the maximum value from their data without compromising privacy.

Why ZTEE now

Before hardware enclaves for confidential computing, organizations used encryption, controlled environments, or advanced cryptographic methods (for example, fully homomorphic encryption and multi-party computation) to maintain data privacy during processing. Typically, these approaches are highly complex, incur performance overhead, or don't sufficiently protect data in plaintext memory. Confidential computing enables encryption of in-use data with lower overhead than purely cryptographic solutions. This advance simplifies the protection of data during processing and significantly reduces complexity.

Protect data and applications
Safeguard information at rest, in transit, and in use with ZTEE and trust services. Application isolation creates the smallest trust boundary for the greatest data protection and code integrity. VM isolation provides the most straightforward path to greater security and compliance with legacy applications. And trust services provide uniform attestation of trustworthy environments.

Meet security demands with ABAC RAG LLMs
With ZTEE, ABAC policies are applied to RAG frameworks that combine LLMs with information retrieval systems. ZTEE eliminates the cybersecurity risk associated with open-source options. It's also optimized to streamline maintenance and scalability and can integrate with your ABAC vendor of choice.

ZTEE protects data in use by providing trusted execution environments for ABAC RAG LLMs. These secure, isolated environments prevent unauthorized access and modification to applications and data. They also enable the highest levels of sensitive data confidentiality, computational integrity, and data privacy.

PROVEN SECURE

NetApp is the only enterprise storage vendor validated to store top-secret data.

- FIPS 140-2 and FIPS 140-3
- Department of Defense Information Network (DoDIN) Approved Product List (APL)
- Common Criteria
- NSA Commercial Solutions for Classified (CSfC) Component List

Support use cases that rely on sensitive data
ZTEE provides a way for organizations to overcome security and policy challenges associated with new services that rely on deep analytics or collaborations. Too often, these services are restricted or blocked because the data is private, regulated, or otherwise confidential.

KEY BENEFITS

- Solution commercially available today
- Dual encryption of data at rest
- Algorithms and data protected for immutability
- Only need-to-know access to data, including administrators
- Encryption of data in motion
- Application operations encrypted while in use
- External configuration verification of the processing enclave
- Specific queries and data used for insights are kept private
- Data, applications, and algorithms shielded from third-party viewing

With ZTEE, applications that were stuck on premises because they handle sensitive data can be moved to the cloud or deployed in hybrid environments. ZTEE addresses concerns about data security risks in the cloud. It also helps organizations maintain control of data if the cloud provider is subject to regulatory or legal requirements outside the organization's preferred framework.

Embrace confidential computing with Intel SGX and Intel TDX
Protecting your systems and data has never been more critical, especially when working with sensitive, confidential, or regulated data. Intel confidential computing solutions are designed to protect data in use with isolation, encryption and control, and verification capabilities to help you unlock new opportunities for business collaboration and insights.

Intel® Software Guard Extensions (Intel SGX) enables application- or function-level isolation. Whether in the cloud, at the edge, or on premises, your sensitive computations and data are kept more private and secure from cloud service providers, unauthorized administrators, the OS, and other privileged applications.

PRIMARY ZTEE USAGE SCENARIOS

UNLOCK DATA SILOS

- Improve collaboration.
- Monetize insights.
- Detect fraud.

BROADEN CLOUD USAGE

- Move sensitive or regulated data and workloads to the cloud.
- Improve TCO and agility.

ENABLE DEFENSE IN DEPTH

- Stop sophisticated, persistent threats that target keys, GenAI, and edge data.
- Reduce the risk of data in use.
- Expand AI access.

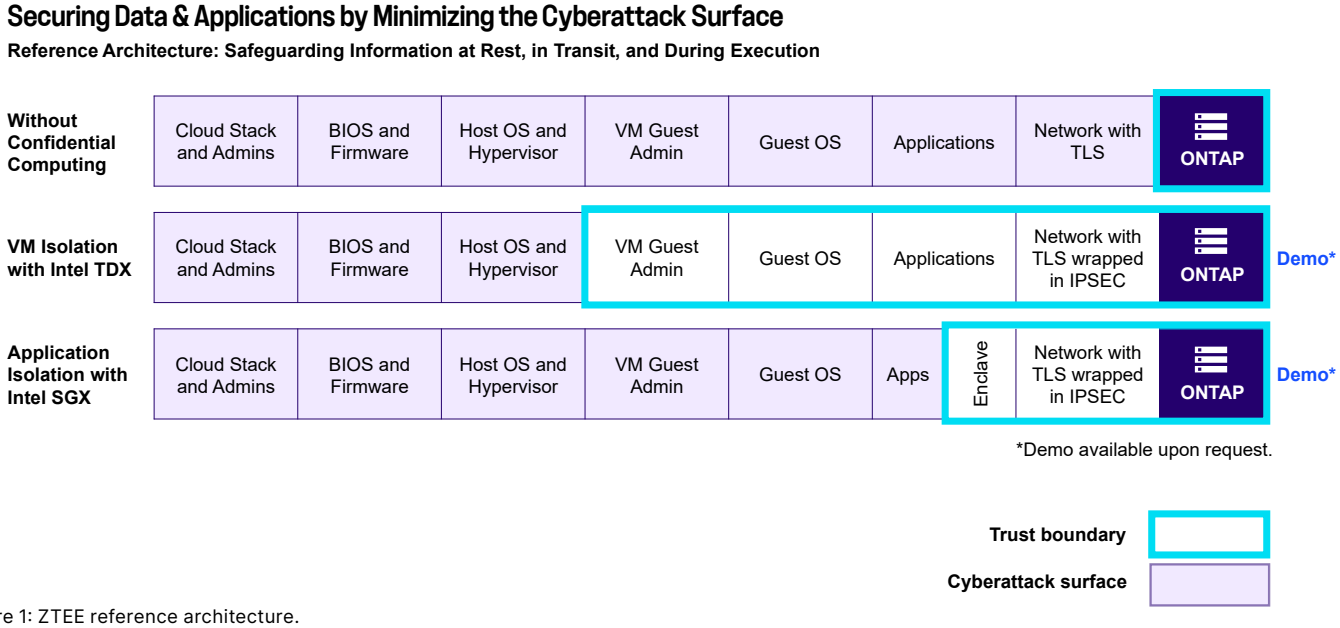


Figure 1: ZTEE reference architecture.

Intel SGX is the most researched and updated confidential computing technology on the market today. It provides the smallest trust boundary in the data center when compared to other confidential computing technologies. By protecting selected code and data from inspection or modification, developers can run sensitive data operations inside enclaves to help increase application security and protect data confidentiality. Also, the attestation capabilities of Intel SGX provide greater confidence that the software running in the enclave is exactly what is expected and previously agreed upon by all parties.

Whereas Intel SGX is for application and function isolation, Intel® Trust Domain Extensions (Intel TDX) offers isolation and confidentiality at the VM level. This technology separates the guest OS and VM applications from the cloud host, hypervisor, and other VMs on the platform. The trust boundary for Intel TDX is larger than the application-level isolation of Intel SGX. However, Intel TDX is designed so that confidential VMs are easier to deploy and manage at scale than application enclaves. Intel TDX offers a simpler migration path for existing applications to move to a secure ZTEE enclave.

Data that holds value for businesses often falls under stringent privacy regulations. Violating these regulations can result in stiff fines and other penalties. Alternatives to using personal data are available, but they often significantly slow down analysis and can even reduce accuracy. With Intel Xeon processors and Intel confidential computing solutions, businesses can create encrypted enclaves that help keep data and applications confidential, complying with regulations and improving data availability.

Intel TDX relies on VM isolation, which simplifies porting of existing applications to a confidential computing environment. In most cases, no application code changes are required. Application-based isolation with Intel SGX can help shrink the attack surface further, but more development effort might be needed to design code for the Intel SGX environment.

By offering both application and VM isolation, confidential computing solutions from NetApp and Intel provide flexibility to set the trust boundary you need for your workloads.

Contact us to schedule a one-on-one solution review and demo with a solution expert.

About NetApp

NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data services, and CloudOps solutions to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, harnessing observability and AI to enable the industry's best data management. As the only enterprise-grade storage service natively embedded in the world's biggest clouds, our data storage delivers seamless flexibility. In addition, our data services create a data advantage through superior cyber resilience, governance, and application agility. Our CloudOps solutions provide continuous optimization of performance and efficiency through observability and AI. No matter the data type, workload, or environment, with NetApp you can transform your data infrastructure to realize your business possibilities. www.netapp.com

NetApp