Fortanix®

Demystifying **Confidential Computing**

Decrypting **Confidential Computing**

From the obvious *(Steve Jobs unveils the iPhone)* to the obscure *(AT&T stops charging an hourly rate for internet access)*, there have been defining events that have served to shape the current landscape of the modern computing industry.

Few understood the vision, even fewer were convinced with the idea. Today, we all know how that panned out.

This tech industry is not new to such phenomena. Facebook metaverse is a more recent example.

One such phenomenon is happening right now.

> *"Trust is essential to build and grow organizations and can even be a significant competitive differentiation, especially in privacy and security sensitive industries. Technologies such as Fortanix Confidential Computing will be key in helping organizations build trust, avoid breaches of sensitive data, and ensure regulatory compliance globally."*

Amita Potnis
Research director, Future of Trust at IDC.

IDC

What is **Confidential Computing?**

For applications to access and process data, it must be unencrypted. Meaning to use the data, the application must be able to see the data. Hence, data in the memory of the device it is processed on, is unencrypted—potentially exposed to malicious agents. Probably why many organisations still prefer to keep their most sensitive data on-premises and avoid cloud migration.

Confidential computing fills this security gap by isolating sensitive data and code during data processing. It facilitates the processing of encrypted data in memory while mitigating the risk of its exposure to the rest of the system, thus delivering a higher level of control and transparency for users.

Data at Rest

Idle data is encrypted on servers in databases and is not moving through networks.

Data at Transit

Data is encrypted prior to transit on public and private networks.

Current Encryption Technologies

Data in Use

Data is protected in use by RAM encryption and hardware-based technologies that secure data during computation.

Confidential Computing

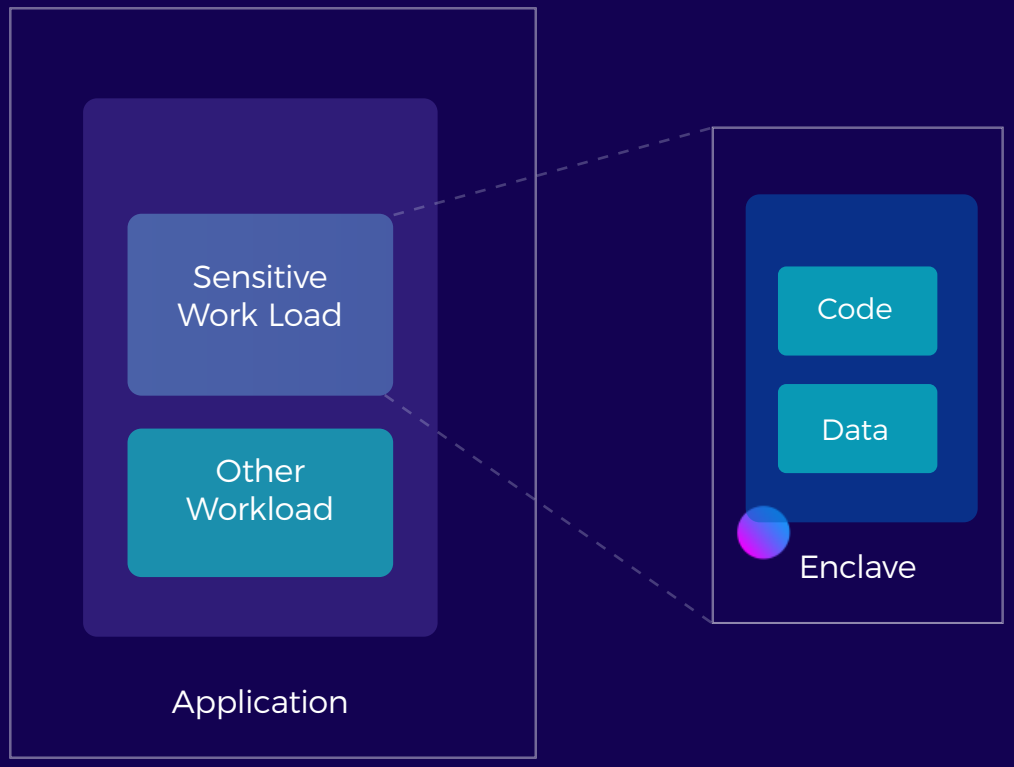
How Does It **Work?**

On a high level, confidential computing powers in-memory data processing capabilities, while the data remains encrypted. The one time that this data is unencrypted is when a system code allows the designated user to access it. In other words, the data remains encrypted and hidden from the cloud providers as well.

So How is It Done?

It's done via the hardware creating a Trusted Execution Environment (TEE), also known as a secure enclave— isolated from the untrusted code. Think of it as a safe corner within a safe locker. What's the untrusted code, you ask? Everything except the designated user with the encryption keys—the OS, the Cloud provider, and every other application running on the system.

The TEE decrypts the private data for computation using the encryption keys. As the code and data rest inside the enclave while being worked upon, they're secluded, safe, and inaccessible to the rest of the system.



Business **Value**

Data protection from malicious attackers and exposed points of interceptions

You cannot use what you can't see. Confidential Computing secures data in its most vulnerable stage—when in use. The data being processed and the techniques that go into it — are only accessible to authorized code, invisible to anyone else—including the OS and CSP.

Ensuring regional data compliance

Confidential Computing enables agencies to build enclave-based applications to protect data in use in a dedicated cloud that meets government security and compliance requirements.

Data security while migrating workloads between different environments

Do not wish to share your business logic processes? Want to guard your machine learning processes and inner workings of a certain application that's integral to enhancing your business processes? Confidential Computing makes that possible.

Allowing developers to create applications while moving and processing data across different cloud platforms and applications.

Businesses at present avoid sharing proprietary data with third-party agencies and other organizations—for obvious concerns around confidentiality. With Confidential Computing, they can share resources, data sets, algorithms, and proprietary applications— as they collaborate on the project without worrying about secrets leaking in the process.

Confidential Computing **in Healthcare**

The healthcare data for creating new medicines and clinical therapies is collected, aggregated, and disaggregated at regional, national, and international levels of analysis.

This growing data repository often inter-twines protected healthcare information (PHI) with other sensitive information. For example, the social interactions disclosed by track-and-trace applications that are subject to stringent data privacy laws.

Public awareness of the type and scale of the data being generated and applied within healthcare has raised legitimate questions about the security of the gathered data and the scope of the data privacy regulations that govern its use.

This is where Confidential Computing comes to the rescue.

> *"BeeKeeperAI was created with the mission to change the future of healthcare with AI, by solving the healthcare data access problem. With Fortanix Confidential Computing technology, we can remove the barriers to accessing critical clinical data which is essential to developing, validating, and deploying high quality, impactful algorithms resulting in optimal health and healthcare."*

Dr. Michael S. Blum
MD, CEO, Co-founder, BeeKeeperAI

BeeKeeperAI®

Benefits

One-Stop cloud ready solution for encryption and all things data security

Healthcare organizations can reduce the cost of complexity of data security by consolidating or replacing multiple encryptions, HSMs, key management, tokenization, and secrets management systems with a single integrated system with standardized cryptographic interfaces.

Complete control and visibility into sensitive health data

Healthcare organizations can reduce the cost of complexity of data security by consolidating or replacing multiple encryptions, HSMs, key management, tokenization, and secrets management systems with a single integrated system with standardized cryptographic interfaces.

Achieve HIPAA and other regulatory compliance

Use Tokenization to comply with HIPAA regulations by substituting electronically protected health information (ePHI) and non-public personal information (NPPI) with a tokenized value.

Use the scale of cloud without compromising security

Confidential computing powered by secure enclaves allows a variety of enterprise use cases to run on the cloud without compromising the security.

Confidential Computing **in Finance**

While digitization does help financial institutions to mitigate digital theft, fraud, and money laundering activities, it also generates mountains of data. They are also subject to regulations that vary drastically between countries and markets.

For example: there are regulations like PCI DSS for credit card data, GDPR for EU data across the globe, GLBA, SOX, and other different laws across the world. As these organizations scale, it's critical to ensure that the sensitive data is protected and meets the compliance requirements.

Here is how Confidential Computing can help the Financial Services.

> *"Financial institutions face immense pressure to earn trust and avoid threats, but the inability to share data hinders the industry from effectively managing the risks from fraud and money laundering. With Fortanix Confidential Computing technology, Consilient's federated machine learning solution, Dozer, moves across financial institutions securely, allowing each to leverage industry insights while enhancing data security or data privacy."*

Gary M. Shiffman
Co-founder and CEO of Consilient

CONSILIENT

Benefits

Trusted Execution Environment (TEE) or “enclaves” for secure processing of financial data

TDEE increases the security of application code and data and offers cloud-based data security services with granular privacy controls, and cloud-optimized specifically for financial services.

Achieving Unparalleled Compliance

The data owner solely stays in control of their critical data enabling them to comply with all international compliance requirements for data security in the cloud.

An added layer of Tokenization

Processed data can be tokenized before it is transferred back to the cloud.

Tamper-proof audit logs

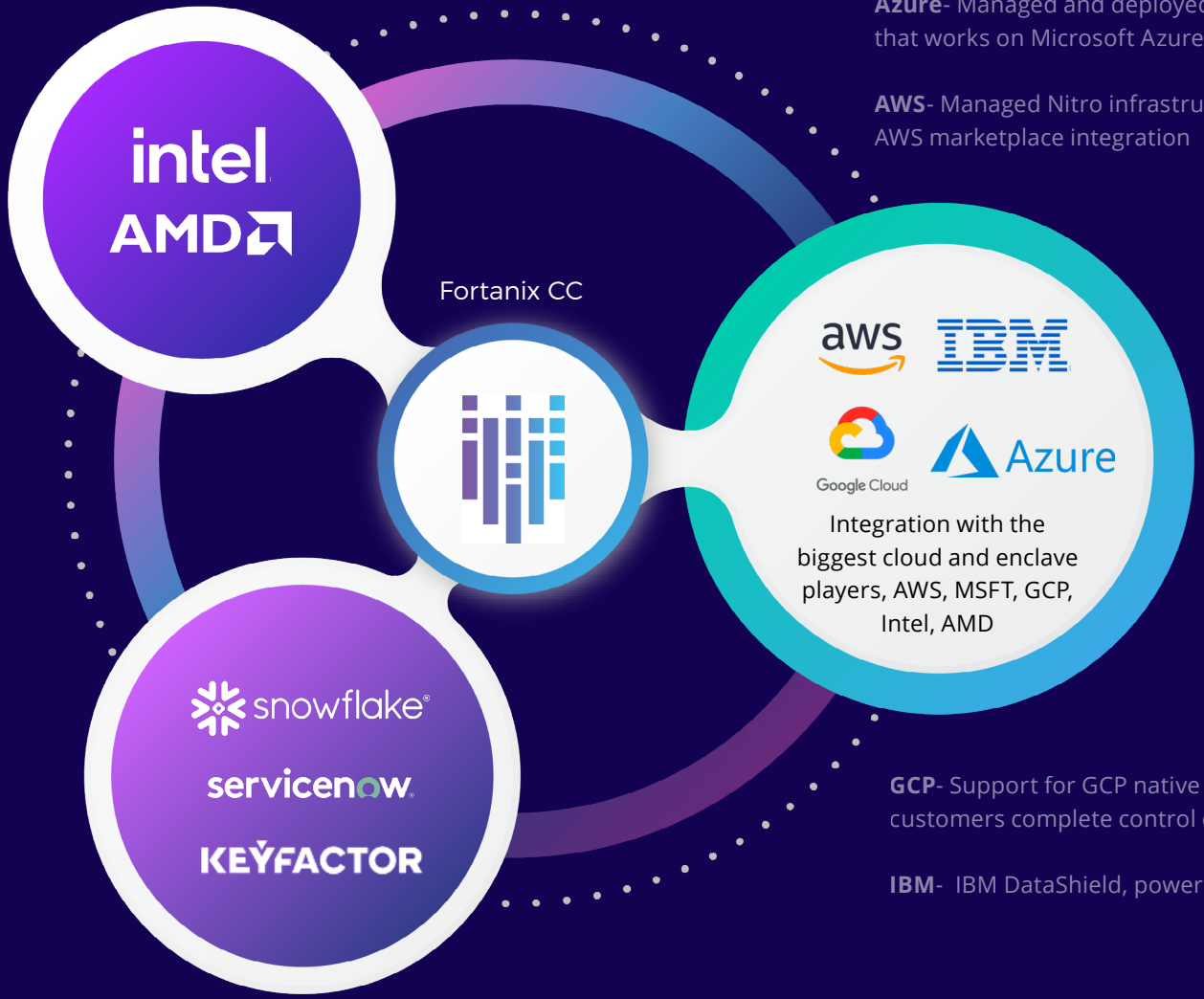
All-access to personal data is automatically logged in a centrally viewable tamper-proof global audit trail by Fortanix. There is never any dispute about who accessed which data and when.

Fortanix **Confidential Computing Ecosystem**

Breadth of integrations allows to run and apply Fortanix CC across any environment and any use case

Intel, AMD

Support for Confidential Computing powered by Intel SGX and AMD.

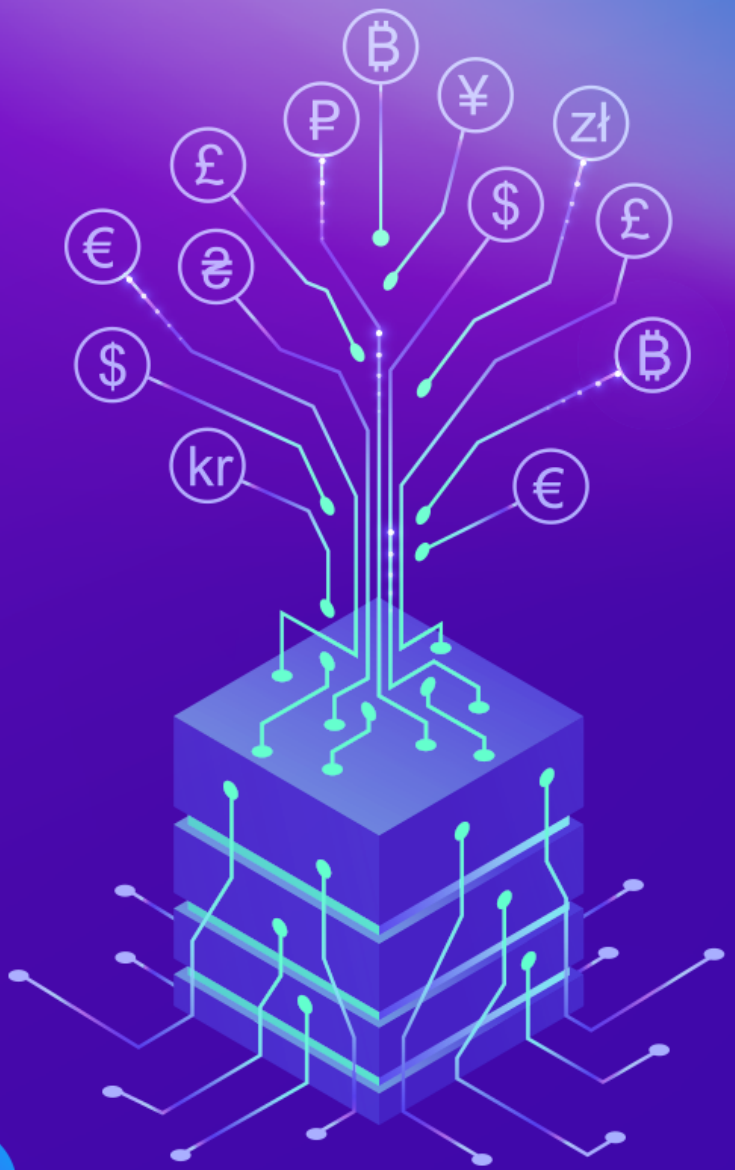


Azure- Managed and deployed infrastructure that works on Microsoft Azure AKS

AWS- Managed Nitro infrastructure support./ AWS marketplace integration

GCP- Support for GCP native services to give customers complete control over their data.

IBM- IBM DataShield, powered by Fortanix



Why The Time to **Invest Is Now!**

Over the last year and a half, most organisations have quadrupled their digital transformation initiatives, processing more data than ever—in turn becoming more data-driven. The surge in the frequency of online operations and activities is off the charts.

From remote collaboration to healthcare consultations to financial transactions, users actively share their personal data across various online platforms, creating potential points of interception of this sensitive data. Think about it, hybrid clouds, mobile devices, smartphones, IoT devices, wearables, remote cars and more—all are riding upon your sensitive personal data. As a consumer, it is essential to have trust in these platforms' ability to securely house and process your data.

Confidential computing generates a private data environment that safeguards this data not only from any external threats but also makes it inaccessible to cloud providers and third parties—even if compelled by external factors.

Clearly, the time to invest in confidential computing was yesterday.

Need a more personalized solution?

Get in touch with us here.

Looking for a free demo?

CLICK HERE.