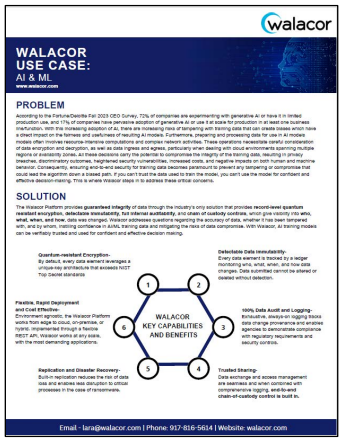

walacor

WALACOR
USE CASE:
AI & ML

PROBLEM

SOLUTION

WALACOR
KEY CAPABILITIES
AND BENEFITS

Email - lara@walacor.com | Phone: 917-816-5614 | Website: walacor.com

Walacor Use Case: AI & ML

Thank you for downloading this Walacor Use Case.

To learn how to take the next step toward acquiring Walacor's solutions, please check out the following resources and information:

For additional resources:
carah.io/WalacorResources

For upcoming events:
carah.io/WalacorEvents

For additional CrowdStrike solutions:
carah.io/WalacorProducts

For additional Cyber solutions:
carah.io/Cybersecurity

To set up a meeting:
Walacor@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/WalacorContracts

WALACOR USE CASE:
AI & ML

www.walacor.com

PROBLEM

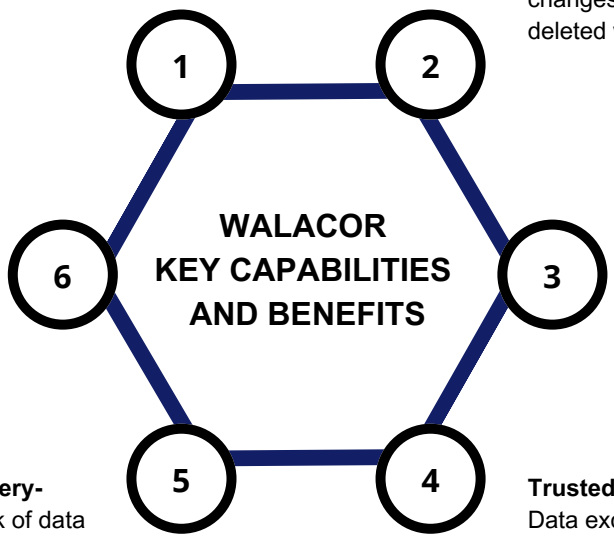
According to the Fortune/Deloitte Fall 2023 CEO Survey, 72% of companies are experimenting with generative AI or have it in limited production use, and 17% of companies have pervasive adoption of generative AI or use it at scale for production in at least one business line/function. With this increasing adoption of AI, there are increasing risks of tampering with training data that can create biases which have a direct impact on the fairness and usefulness of resulting AI models. Furthermore, preparing and processing data for use in AI models models often involves resource-intensive computations and complex network activities. These operations necessitate careful consideration of data encryption and decryption, as well as data ingress and egress, particularly when dealing with cloud environments spanning multiple regions or availability zones. All these decisions carry the potential to compromise the integrity of the training data, resulting in privacy breaches, discriminatory outcomes, heightened security vulnerabilities, increased costs, and negative impacts on both human and machine behavior. Consequently, ensuring end-to-end security for training data becomes paramount to prevent any tampering or compromise that could lead the algorithm down a biased path. If you can't trust the data used to train the model, you can't use the model for confident and effective decision-making. This is where Walacor steps in to address these critical concerns.

SOLUTION

The Walacor Platform provides **guaranteed integrity** of data through the industry's only solution that provides **record-level quantum resistant encryption, detectable immutability, full internal auditability,** and **chain of custody controls**, which give visibility into **who, what, when, and how**, data was changed. Walacor addresses questions regarding the accuracy of data, whether it has been tampered with, and by whom, instilling confidence in AI/ML training data and mitigating the risks of data compromise. With Walacor, AI training models can be verifiably trusted and used for confident and effective decision making.

Quantum-resistant Encryption-
By default, every data element leverages a unique-key architecture that exceeds NIST Top Secret standards

Detectable Data Immutability-
Every data element is tracked by a ledger monitoring who, what, when, and how data changes. Data submitted cannot be altered or deleted without detection.



Flexible, Rapid Deployment and Cost Effective-
Environment agnostic, the Walacor Platform works from edge to cloud, on-premise, or hybrid. Implemented through a flexible REST API, Walacor works at any scale, with the most demanding applications.

100% Data Audit and Logging-
Exhaustive, always-on logging tracks data change provenance and enables agencies to demonstrate compliance with regulatory requirements and security controls.

Replication and Disaster Recovery-
Built-in replication reduces the risk of data loss and enables less disruption to critical processes in the case of ransomware.

Trusted Sharing-
Data exchange and access management are seamless and when combined with comprehensive logging, **end-to-end chain-of-custody control is built in.**

Email - lara@walacor.com | Phone: 917-816-5614 | Website: walacor.com

The Trust Layer

Secure Your Data

Transparent data security that is tamper-proof, know the who, what and where through unique quantum resistance.

Easy Integration

Built with REST APIs, Walacor is simple to implement and integrates seamlessly within typical technology environments.

Detectable Immutability

Blockchain design simplifies data governance , integrity, and security, maintaining cost-effective enterprise controls and scalability.

The Use Case: Data Poisoning of a DoD AI Model

In AI poisoning attacks, attackers compromise the training data of AI models, leading to skewed decision-making. These subtle alterations in the data erode the trust and integrity of the AI system, inducing bias and flawed outcomes. The goal of these attacks is to manipulate deep learning models, steering their behavior to suit malicious interests. This can lead to:

- **Compromised Decision-Making:** AI poisoning can lead to skewed AI algorithms, resulting in flawed and unreliable decision-making, particularly detrimental in high-stakes defense scenarios.
- **Eroded Operational Integrity:** Maliciously altered AI models can undermine the integrity of critical operations, posing significant risks to mission success and warfighter safety.
- **Loss of Strategic Advantage:** AI poisoning can compromise the strategic advantage on the battlefield by feeding incorrect data to AI systems, leading to misinformed tactics and compromised battlespace awareness.

Success with Walacor:

- **Data Integrity Assurance:** Walacor's blockchain-integrated platform ensures the highest level of data integrity, preventing tampering or alteration of AI training data and/or data intelligence output, thus safeguarding against AI poisoning.
- **Real-time Anomaly Detection:** Employing unique cryptographic keys for each data entry, Walacor enables real-time detection of unauthorized changes, swiftly identifying and mitigating potential AI poisoning attempts.
- **Immutable Data Records:** By creating an immutable audit trail of data transactions, Walacor's technology maintains the authenticity of AI training datasets, ensuring they remain free from malicious manipulations that can be proven.

ABOUT WALACOR

Walacor’s platform represents the next generation of secure data storage with a trust-first approach that revolutionizes enterprise data, and database management systems. Focused on safe data sharing, integrity, and high performance, the platform builds a “wall around your core data” at the record level. The WalacorDB Platform effectively creates a self-defense weapon against cyber-attacks and misuse, internally and externally. Walacor offers a turnkey solution that creates a secure data store, integrating best practices, and leading quantum resistant encryption. Our data-centric architecture is built for use in a way that provides for optimal interoperability and data governance with a familiar look that allows for easy adoption. With unparalleled levels of visibility, audibility, and control, as well as seamless integration with existing infrastructures, Walacor is revolutionizing the cybersecurity movement around Zero Trust.

Email - lara@walacor.com | Phone: 917-816-5614 | Website: walacor.com