Data Integrity | Cyber Resiliency | Data Protection

A NEW ERA OF TRUST

The Problem:

Organizations and government struggle in their mission to maintain the accuracy and reliability of data across complex and hybrid systems, risking critical decision-making on potentially compromised information. The integrity of data is under constant threat from sophisticated cyber attacks, system malfunctions, and human error, which can disrupt business operations and hurt revenue and the costs of storage and compute are rising exponentially.

The Solution:

Walacor solves this problem with our next generation secure data platform that guarantees **DATA INTEGRITY** and sovereignty through detectable immutability, unique encryption keys, and chain of custody.

In an era where data is the most valuable asset, and AI is reshaping our analytical landscape, Walacor provides a guaranteed data store with built-in integrity. **With Walacor, you can harness the power of data and AI with confidence, ensuring every decision is informed by data you can TRUST while reducing COSTs dramatically.**

"The Achilles heel of the Hybrid Space Architecture is data integrity."
  -United States Space Force Lt. General Michael Guetlein

walacor

Risks to AI and ML Systems

A threat to data is a threat to AI & ML Ops trust and operation

- The Risks: training data integrity, **data poisoning,** AI model integrity, stealing model parameters (model extraction).

- Tampering with security policy is global system problem. **ZT policies must be tamper-proof.**

- Potentially disastrous consequences in areas like autonomous weapon systems, logistics management, and cyberwarfare.

- **Walacor partners with Mission Partners** to integrate Blockchain with MLSecOps and unlocks new possibilities for secure transparent and decentralized machine learning.
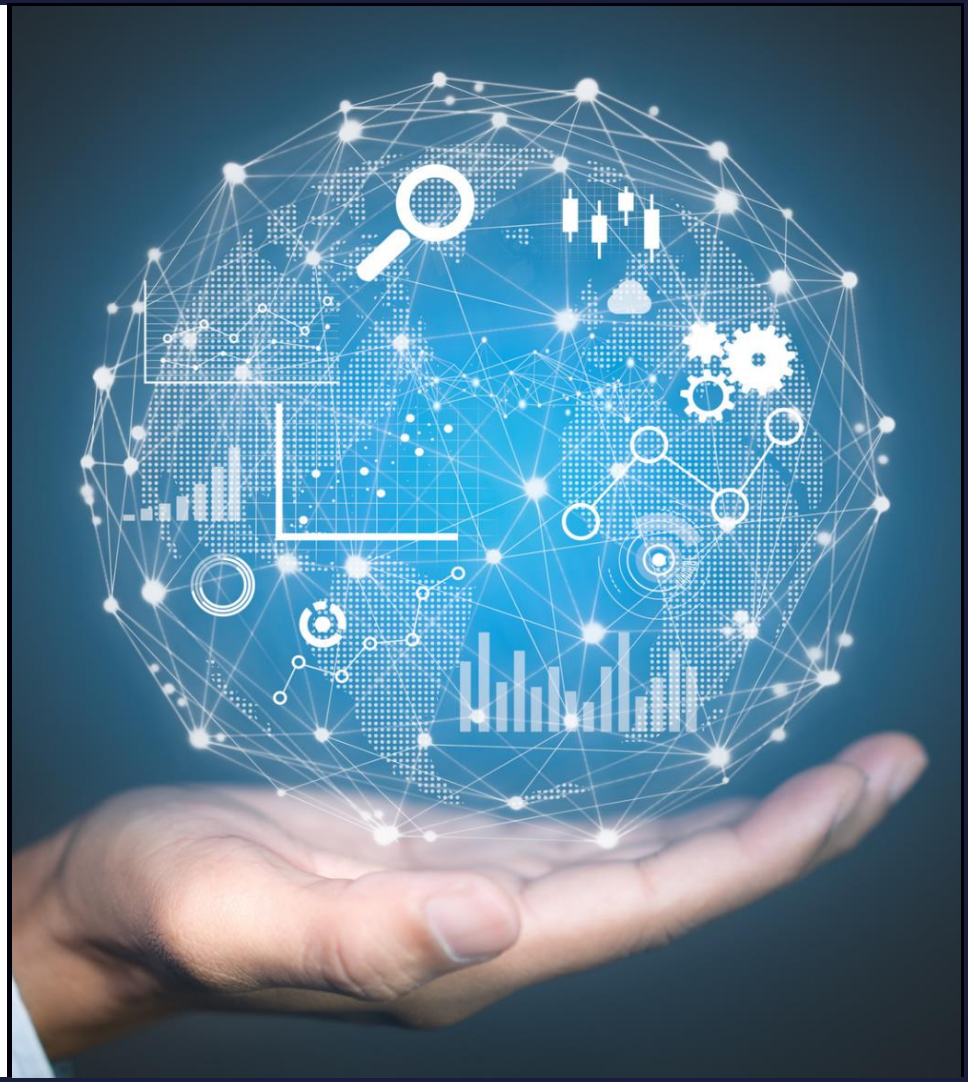
PERSISTENT
DATA INTEGRITY

The **Trust** First Secure Data Platform

Confidence in Every **Byte**

Only Walacor **Guarantees Data Integrity with Provable Immutability at the Data Element Level**

Key Differentiators

The Walacor Platform uniquely provides in one solution:

- ✔ Trust that you are making decisions based on valid data
- ✔ Always-on, record-level quantum-resistant encryption
- ✔ End-to-end chain of custody control for auditable data provenance
- ✔ Detectably immutable data storage, audit, and logging
- ✔ Tamper-proof event logging based on distributed ledger technology
- ✔ Zero Trust secure data layer architecture
- ✔ Broad interoperability
- ✔ Customer data sovereignty
- ✔ Built in deduplication & reduction of significant costs
- ✔ Next-generation ransomware and cyber attack resilience

walacor

A New Era of Trust

The Walacor Platform is a **secure data management platform** that solves these problems and enables you to **trust your data** by defending against threats **both inside and outside of a data store** and reduces risk to your Enterprise.

- Guaranteed **persistent data integrity**

- **Always-on encrypted data platform, cannot be turned off**

- Natively **quantum-resistant**, AES 256, able to adopt quickly

- Data element, record, or object store-level encryption **with unique keys**

- Enables rapid **detection** of unauthorized alteration or deletion of data

- Embeds an **immutable**, **auditable** chain of custody into the data lifecycle

- Provides for **data sovereignty**

- Broad **interoperability** with existing systems. Massively **scalable**. Ease of use

Walacor is the foundational data layer for a Zero Trust environment

The Walacor Platform provides the Wall Around your Core data

Walacor: A Defense Forward, Dual Use Secure Data Company

Our Purpose

Walacor exists to protect the lifeblood of national security – **data** – at the **data element** level.

Walacor's software platform provides a **foundational data trust layer** to ensure critical systems operate securely, without compromise.

Walacor ensures **every byte of data**, no matter where it is stored or how it's accessed, is authentic and untouchable.

Why Trust in Data Matters

Trust Enables National Security
Without secure, untampered data, operational readiness and mission success are impossible

Data Integrity: the Next Battlefield
Warfare is now waged in cyberspace and via AI, where data manipulation can cripple systems and compromise lives.

Zero Trust Cybersecurity Demands Data Integrity at the Foundational Level
"Zero Trust" is the new standard for cybersecurity. But to work, it needs to be applied at the <u>**data element level***</u>.

* Data element = the smallest unit of information, representing a single piece of data, within a database

The Walacor Team: Proven Expertise in Data Integrity

Walter Hancock
Co-Founder, CEO & CTO

Lara George
Co-Founder, President

Rob Zitz
Head of Government

We have built and delivered technology platforms and solutions for the Fortune 500 and are leaders in Guaranteed Data Integrity.

Genesis Solutions

Hyperion
(Acquired by Oracle)

MCM

citibank

ARTHUR ANDERSEN

NGA, NRO, CIA, DHS

Founders' experience includes executing projects for:

J.P.Morgan

NEUBERGER BERMAN

Altisource

Advisory Board (Partial)

Charlene Leubecker Cyber Thought Leader	CIA	
Bob Gourley Quantum Thought Leader	DIA	

Chris Perretta Financial Services	State Street, GE Capital	
Touchstone Futures Army	Retired Generals & Cyber	

walacor

Ensuring data <u>integrity</u> – at the <u>data element level</u>

Data Integrity, Not Cyber Attacks, Are What Most Worry Space Command's Cyber Boss

Oct. 24, 2024 | By Shaun Waterman

AIR&SPACE FORCES MAGAZINE

ALL DOMAIN, LAND WARFARE, NETWORKS & DIGITAL WARFARE

'Poisoned' data could wreck AIs in wartime, warns Army software acquisition chief
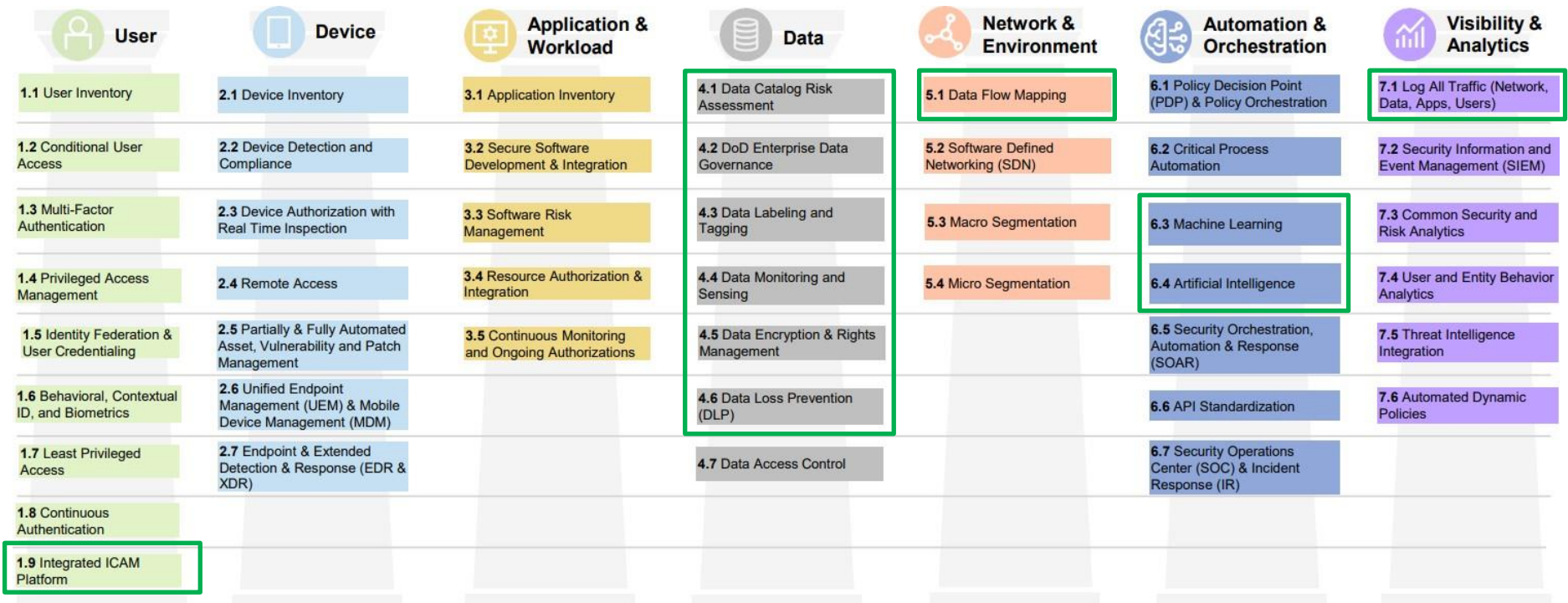
BREAKING **DEFENSE**

"If our adversary can **poison** our data, we're going to start getting the **wrong information back out from our artificial intelligence**. It's going to say, 'Day is night, night is day. Black is white, white is black.'
- Paul Blahusch, CISO, Department of Labor.

walacor

Walacor Solves The Zero-Trust Secure Data Layer Problem Horizontally

DoD Zero Trust Capabilities – Where does Walacor play a role?

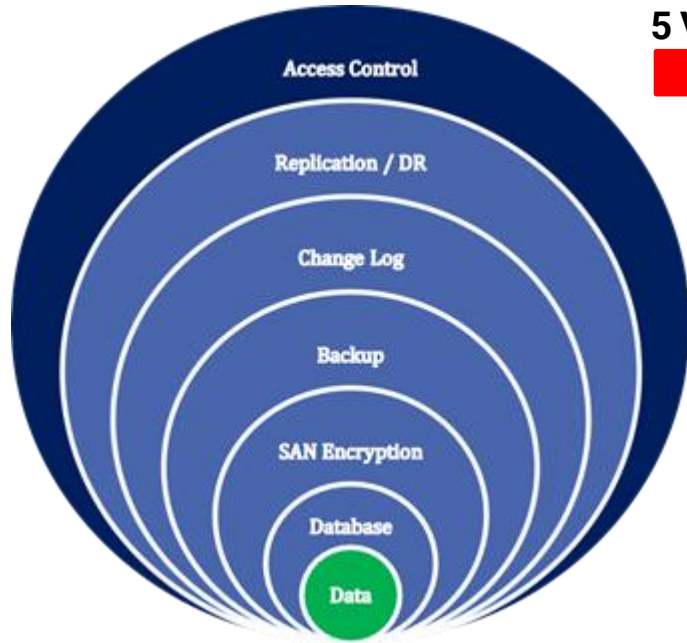| User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	2.1 Device Inventory	3.1 Application Inventory	4.1 Data Catalog Risk Assessment	5.1 Data Flow Mapping	6.1 Policy Decision Point (PDP) & Policy Orchestration	7.1 Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	2.2 Device Detection and Compliance	3.2 Secure Software Development & Integration	4.2 DoD Enterprise Data Governance	5.2 Software Defined Networking (SDN)	6.2 Critical Process Automation	7.2 Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	2.3 Device Authorization with Real Time Inspection	3.3 Software Risk Management	4.3 Data Labeling and Tagging	5.3 Macro Segmentation	6.3 Machine Learning	7.3 Common Security and Risk Analytics
1.4 Privileged Access Management	2.4 Remote Access	3.4 Resource Authorization & Integration	4.4 Data Monitoring and Sensing	5.4 Micro Segmentation	6.4 Artificial Intelligence	7.4 User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Management	3.5 Continuous Monitoring and Ongoing Authorizations	4.5 Data Encryption & Rights Management		6.5 Security Orchestration, Automation & Response (SOAR)	7.5 Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		4.6 Data Loss Prevention (DLP)		6.6 API Standardization	7.6 Automated Dynamic Policies
1.7 Least Privileged Access	2.7 Endpoint & Extended Detection & Response (EDR & XDR)		4.7 Data Access Control		6.7 Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

Walacor keeps all kinds of critical data safe with data integrity across all pillars at scale

The Solution: Guaranteed Data Protection at Data Element Level

Traditional Approach
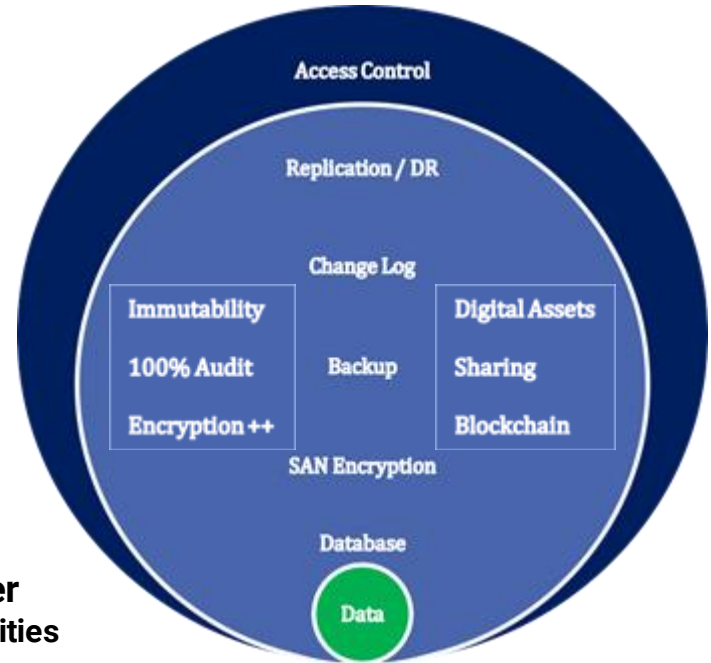Complex – Costly – **Multiple Vulnerabilities**

walacor
Protection at **Data Element** Level

5 Vulnerable Layers

Access Control

Replication / DR

Change Log

Backup

SAN Encryption

Database

Data

1 Strong Layer
With More Capabilities

Access Control

Replication / DR

Change Log

Immutability

100% Audit

Encryption ++

Backup

Digital Assets

Sharing

Blockchain

SAN Encryption

Database

Data

Walacor's software enhances cybersecurity, data integrity and solves AI data poisoning by applying quantum-resistant encryption at the <u>data element level with 100% Data Audit & Assurance.</u>

walacor

The Solution: Enabling Zero Trust Cybersecurity at the Bit **Level**

The Walacor Platform sets a new **standard for cybersecurity, data integrity, and data resilience** by incorporating **quantum resistant, AES-256+ key encryption** at every data element level or submission.

Quantum Resistant Encryption

Database
Data Store
Data Warehouse
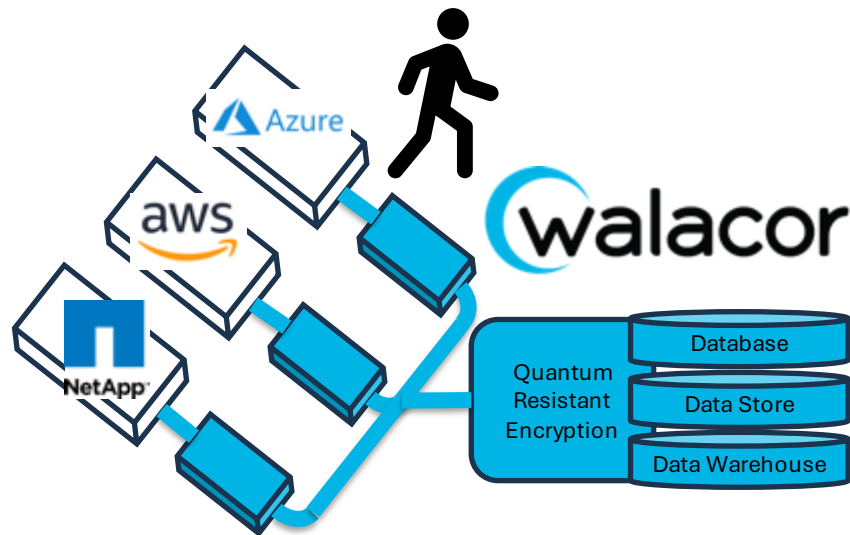
Finalist AUSA Army Linchpin X-tech AI

Deploy on premise, in the cloud or hybrid with Perfect Trusted Replication even in a Contested or Congested Environment, when the Networks are down you can trust your Data

Use as standalone, high security database platform for mission-critical applications guaranteeing Digital Sovereignty

Integrates with existing databases to enhance secure data by replacing or sitting side by side with Legacy Systems

"Zero Trust is the new paradigm for Cybersecurity. Walacor is a foundational element of our Zero Trust Architecture (ZTA) for the Cloud and on the Edge. Any government agency or enterprise that wants to ensure the integrity of its data needs to talk to Walacor."
Glen Gulyas, President **Available Networks**

Walacor: Available on AWS, Azure, and on Premise

Why Now?

The Walacor Platform addresses the evolving cyber threat landscape, in which data breaches are increasing, and cyber assaults are becoming more sophisticated and costly.

DOE, CISA, DOD & OPM are agencies that have been recently breached

150+ ZB of data created in 2024, doubling every year.

92% of enterprises have a multi-cloud strategy, sprawling data across locations and platforms.

3 years average IT hardware refresh, creating opportunities for vendor lock-in.

75% of organizations suffered at least one ransomware attack last year.

"... Damage from cyberattacks will amount to **$10.5 trillion annually by 2025 - a 300 percent increase from 2015 levels.**"
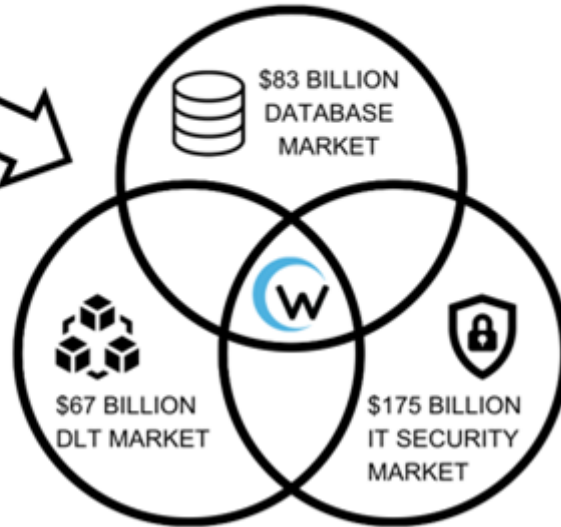
walacor

Total Addressable Market - Data as an Asset is Critical > $250 Billion

2024: $197.5B MARKET

$58 BILLION DATABASE MARKET

$3.5 BILLION DLT MARKET

$136 BILLION IT SECURITY MARKET

2030: $325B MARKET

$83 BILLION DATABASE MARKET

$67 BILLION DLT MARKET

$175 BILLION IT SECURITY MARKET

Quantum Resistant Market expected to hit $500 Billion in 2030[1]

$500 BN TAM

$200BN SAM

$100 BN SOM

SPHERICAL INSIGHTS

[1] https://www.globenewswire.com/en/news-release/2023/03/08/2623391/0/en/Global-Cybersecurity-Market-Size-To-Grow-USD-501-6-Billion-By-2030-CAGR-11-6.html

"As more organizations use **AI** to enhance their operations, they risk inadvertently introducing new cyber-related threats. This creates a significant and growing **demand for advanced cybersecurity solutions**."
McKinsey & Company

walacor

Massive and Rapidly Growing Market Need

49% of organizations are evaluating or experimenting with AI, but **only 4% currently have pervasive adoption**.

Private and publics sectors are rapidly transitioning from traditional cybersecurity defenses to innovative Zero Trust strategies. DoD to implement Zero Trust cybersecurity strategies across the department by the end of **FY 2027**.

By 2028, 70% of file and object data will be deployed on consolidated, unstructured data storage platforms, up from 35% in early 2023.
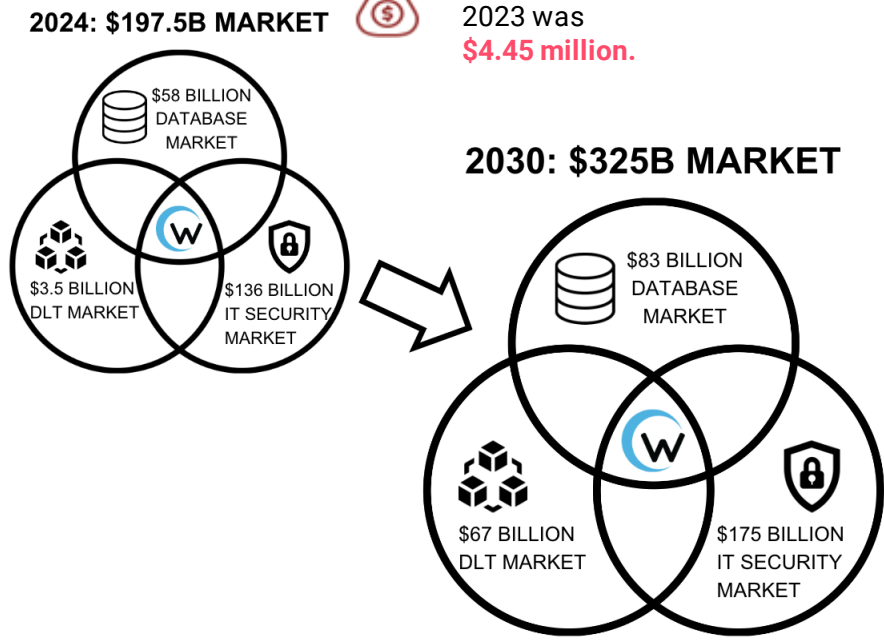
45% of experts say cyber threats are the top concern for business interruption.

72.7% of organizations were affected by ransomware attacks in 2023.

The global average cost of a data breach in 2023 was **$4.45 million.**

2024: $197.5B MARKET

$58 BILLION DATABASE MARKET

$3.5 BILLION DLT MARKET

$136 BILLION IT SECURITY MARKET

2030: $325B MARKET

$83 BILLION DATABASE MARKET

$67 BILLION DLT MARKET

$175 BILLION IT SECURITY MARKET

walacor

Created Trusted AI/ML Models

Problem
- As AI becomes more embedded in business processes, the threat of training data tampering increases, risking the creation of biased AI models
- Complex data processing for AI necessitates robust data integrity measures to prevent biases, privacy breaches, and security vulnerabilities, especially critical in defense and high-stake industries

Walacor Solution
- A secure data platform that ensures the immutability of AI training data, protecting against poisoning attacks and guaranteeing the reliability of AI decision-making using **Object Validator.**
- Our solution safeguards operational integrity by maintaining a tamper-evident dataset, crucial for unbiased AI performance and maintaining a strategic advantage in mission-critical applications.
- The Walacor Platform is ideal for Digital Twins and has signed and implementing a Government Contract with the ability to scale.

Solving AI/ML Data Integrity & Security for the DoD

Leading data security and integrity solution company empowering the Department of Defense with Cutting- edge technologies to **Safeguard sensitive information**, ensuring operational readiness and **mission success.**

Government Contracts & Government Contracts Pending SIBR II direct, Digital Twins, Data Sovereignty, Guaranteed Identification Data, Security Policy Golden Copies, Security for AI

Contract vehicles:
ITES, NASA SEWP, NASPO, OMNIA, QUILT GSA

U.S. Department *of* Defense

Contact us for Mission Centric Use Cases:

lara@walacor.com | 917-816-5614

7315 Wisconsin Ave, Ste. 400W Bethesda, MD 20814

walacor