January 2026

Artificial Intelligence
Trust is Everything

Executive Summary

Artificial Intelligence (AI) has become an integral part of our lives, transforming the way we live, work, and interact with each other. However, as AI-driven systems continue to grow in complexity and influence, a pressing concern has emerged: trust. In this white paper, we will explore the importance of trust in AI solutions and discuss the limitations of public and private AI approaches.

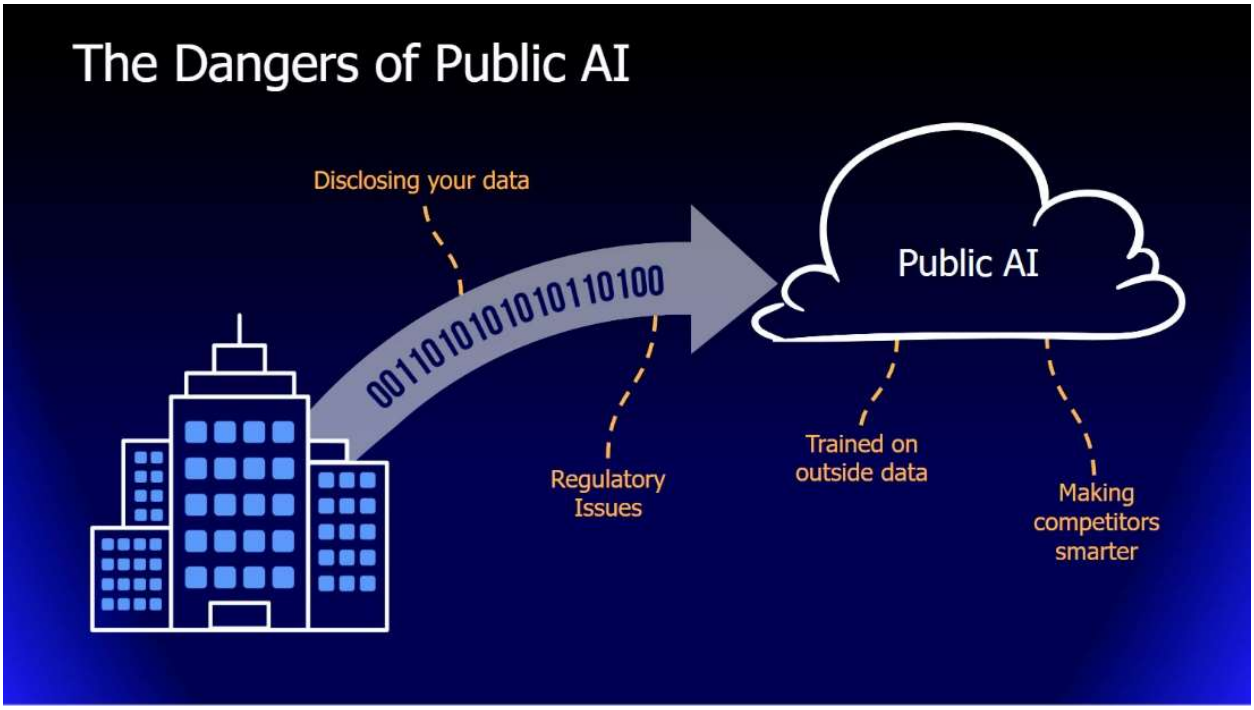
Public AI Challenges

Public AI systems have become ubiquitous, with applications ranging from social media to ride-hailing services. These platforms rely on vast amounts of user data to function effectively, often without providing adequate safeguards for protecting this sensitive information. As a result, public AI has become increasingly vulnerable to malicious activities such as:

- **Data breaches**
  The unauthorized access and theft of sensitive user data have become commonplace in the tech industry.

- **Cyber attacks**
  Malicious actors are constantly probing for vulnerabilities in public AI systems, with devastating consequences.

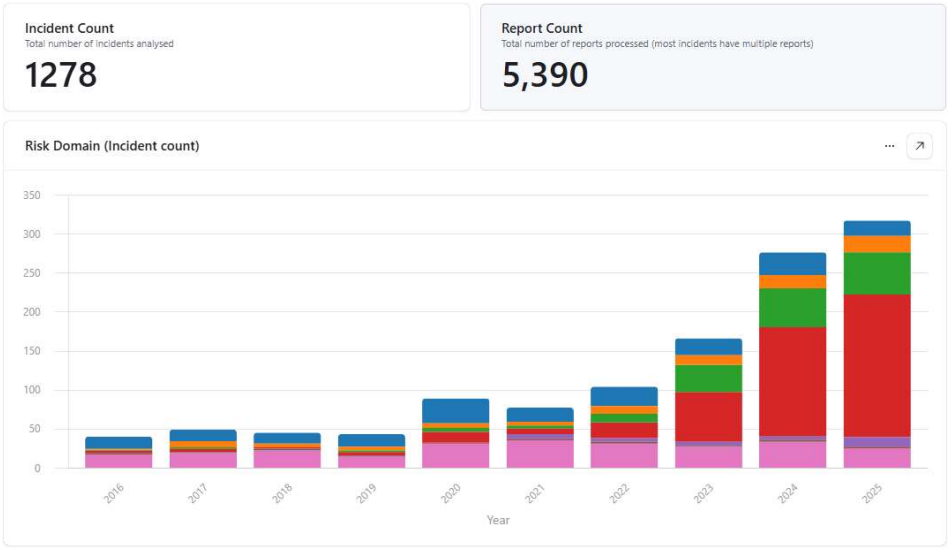
- **Algorithmic manipulation**
  Public AI algorithms can be exploited or manipulated by malicious individuals or organizations to spread misinformation or influence public opinion.



Real Obvious Solutions For Real World Problems™
www.realobvious.com info@realobvious.com +1.719.439.8399

Public AI Risks

As the use of AI increases, the number of reported AI incidents increases. Over the past 10 years, the Massachusetts Institute of Technology (MIT) AI Risk Initiative has seen a dramatic rise in the number of AI incidents.



Reported AI Incidents (source: MIT AI Rick Initiative https://airisk.mit.edu/)

Public AI systems pose several risks to individuals and organizations, including:

- **Data breaches**
  The unauthorized access and theft of sensitive user data.
- **Cyber attacks**
  Malicious actors probing for vulnerabilities in public AI systems.
- **Algorithmic manipulation**
  Exploiting or manipulating public AI algorithms for malicious purposes.
- **Misinformation**
  Spreading false information through public AI platforms.

These risks can have serious consequences, including:

- **Financial loss**
  Theft of sensitive financial information leading to financial losses.
- **Reputation damage**
  Spreading misinformation that damages an individual's or organization's reputation.
- **Safety risks**
  Manipulating public AI systems for malicious purposes, such as hacking into critical infrastructure.

Private AI Challenges

While Private AI offers numerous benefits in terms of security, control, and compliance, it also presents several challenges that must be addressed by organizations considering this approach. Two primary scenarios arise when implementing Private AI:

- Cloud (Outsourced) Private AI Services
- Self-Hosted Private AI Services

Cloud (Outsourced) Private AI Services

In this scenario, the organization outsources its Private AI services to a cloud provider. This approach offers several advantages, including scalability, flexibility, and cost-effectiveness. However, it also requires a great deal of trust in the cloud provider, as their employees and sub-contractors may have access to your sensitive data and control over the AI infrastructure.

The lack of explicit contractual and legal obligations between the organization and cloud provider can be a significant concern. While most cloud providers claim to adhere to industry standards for security and compliance, the actual implementation and enforcement of these measures may vary greatly. In many cases, the organization has little recourse if they suspect a breach or mismanagement of their data.

The following points highlight some of the challenges associated with cloud (outsourced) private AI services:

- **Data ownership**
  The cloud provider typically retains control over the data, which can raise concerns about ownership and intellectual property.

- **Security**
  Depending on the cloud provider's infrastructure and security measures, sensitive data may be vulnerable to unauthorized access or breaches.

- **Regulatory compliance**
  Organizations must ensure that the cloud provider meets relevant regulatory requirements, which can be a significant burden.

Self-Hosted Private AI Services

In this scenario, the organization deploys dedicated private AI services on-premise, in the cloud, or in a hybrid multi-cloud configuration, with complete control over data and infrastructure. This approach offers several benefits, including:

- **Data ownership**
  Organizations retain full control and ownership of their data.

- **Security**
  With direct control over the infrastructure, organizations can implement robust security measures tailored to their specific needs.

- **Regulatory compliance**
  Organizations can ensure that AI services meet relevant regulatory requirements without relying on third-party providers.

However, this approach also requires a significant investment in developing processes and procedures to instill trust in the private AI services applications, data, and operations. The following points highlight some of the challenges associated with self-hosted private AI services:

- **Technical expertise**
  Organizations must invest time and resources in developing technical expertise to manage and maintain AI infrastructure.

- **Process development**
  Establishing effective processes for managing data, monitoring performance, and addressing security concerns requires significant investment.

- **Scalability**
  Internal AI services may struggle to scale with growing demands, requiring additional resources or investments.

Limitations of Private AI

While private AI has several advantages over public AI, it also has some limitations. These include:

- **Limited scalability**
  Private AI systems can be difficult to scale due to the need for secure data transmission and storage.

- **Manipulation by malicious actors**
  Even with data isolation, private AI systems can be manipulated by malicious individuals or organizations.

- **Biases and errors**
  Private AI algorithms can contain biases or errors that may lead to inaccurate or unfair outcomes.

The Rise of Trusted Private AI

In light of the limitations of public and private AI approaches, we propose the concept of Trusted Private AI as a necessary solution that balances confidentiality and security with integrity and transparency. A trusted private AI system must meet the following criteria:

- **Integrity**
  The ability to ensure data accuracy and consistency.
- **Validation**
  The capacity to verify the correctness of AI-driven decisions.
- **Cybersecurity**
  The safeguarding against unauthorized access or manipulation.
- **Safety**
  The protection of users from potential harm.

Trusted Private AI must be designed with security, integrity, and transparency in mind. This approach will ensure that user data is protected while also providing assurance around the accuracy and fairness of AI-driven decisions.

Benefits of Trusted Private AI

Implementing a trusted private AI solution has numerous benefits, including:

- **Enhanced trust**
  Users can have confidence that their sensitive information is being handled securely and responsibly.
- **Improved security**
  The isolation of user data reduces the risk of unauthorized access or theft.
- **Increased accuracy**
  Validated AI-driven decisions ensure that users receive accurate and reliable results.
- **Better alignment with regulatory requirements**
  Trusted Private AI meets or exceeds industry standards for confidentiality, integrity, and transparency.

These benefits are critical in today's digital age, where individuals and organizations must prioritize security, trustworthiness, and accountability.

Implementation and Adoption

Implementing a trusted private AI solution requires careful planning, execution, and ongoing maintenance. This includes:

- **Developing clear policies**
  Establishing clear policies around data confidentiality, integrity, and transparency.

- **Investing in cybersecurity**
  Implementing robust cybersecurity measures to safeguard against unauthorized access or manipulation.

- **Providing transparent communication**
  Communicating clearly with users about the benefits and limitations of trusted private AI.

By prioritizing trustworthiness, accountability, and security, organizations can unlock the full potential of AI while protecting their users' sensitive information.

Conclusion

In conclusion, trust is a fundamental requirement in AI solutions. Public AI systems are inherently vulnerable to malicious activities due to their open nature, while private AI falls short in terms of trustworthiness despite its advantages in security and confidentiality. We propose the concept of Trusted Private AI as a necessary solution that balances confidentiality and security with integrity and transparency.

By adopting trusted private AI, organizations can ensure user confidence and security, which is essential for unlocking the full potential of AI while safeguarding against malicious activities.

Recommendations

Based on our analysis, we recommend that:

- **Organizations prioritize trustworthiness**
  Prioritize trustworthiness in AI solutions to protect users' sensitive information.

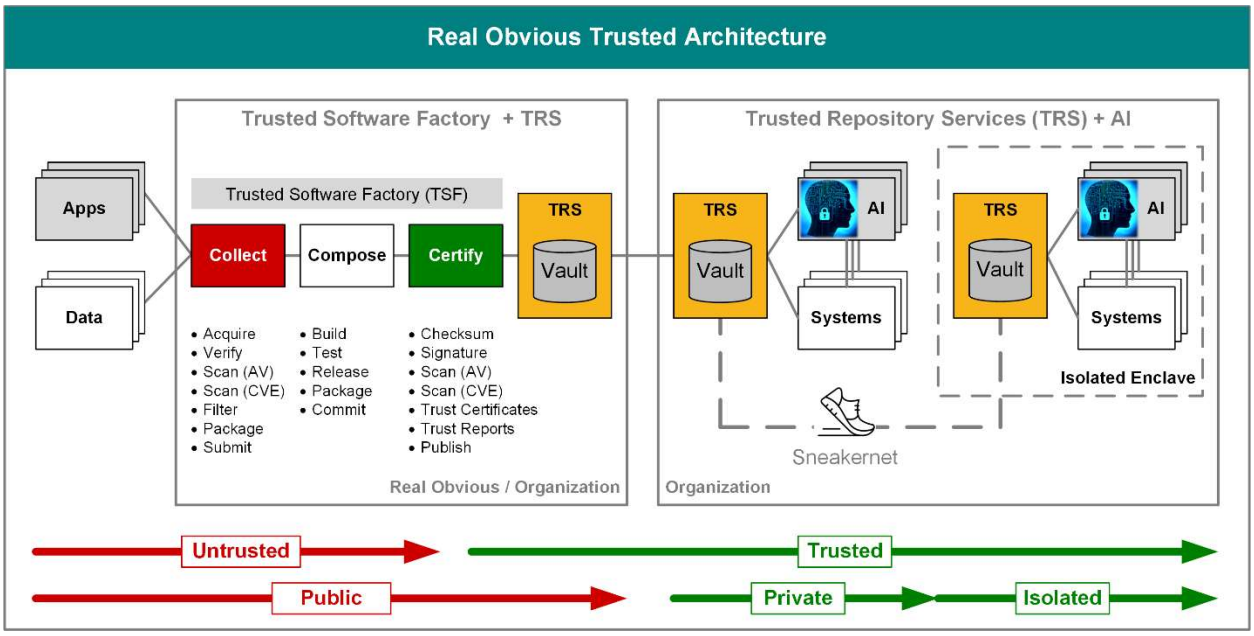
- **Invest in cybersecurity**
  Invest in robust cybersecurity measures to safeguard against unauthorized access or manipulation.

- **Communicate transparently**
  Communicate clearly with users about the benefits and limitations of trusted private AI.

By following these recommendations, organizations can ensure that their AI solutions are secure, trustworthy, and effective.

About Real Obvious

Real Obvious Artificial Intelligence is a Trusted Private AI service that helps businesses protect their most valuable assets – data and intellectual property. Our secure, enterprise-class solutions are built on Zero Trust principles and deploy in isolated enclaves, so you can trust that your information is safe.



Real Obvious Trusted Private AI services isolates and protects customer data assuring compliance with HIPAA, PII, PCI-DSS, CMMC, GDPR, GLBA, SOX, FISMA, and more. Our simple, cost-effective approach makes it easy to deploy and maintain. Our scalable architecture supports single node (small) to high availability clusters (large) deployments on premise and across hybrid multi-cloud environments.

Our team of experts provides solution consulting and software services that are tailored to your needs. Our extensive dark site experience eliminates the need for Internet exposure reducing the risk of IP theft. Our high-trust approach means you can rely on us to keep your data and secrets secure.

Real Obvious AI – The smart choice for enterprise-class Trusted Private AI solutions

Real Obvious Solutions For Real World Problems™
www.realobvious.com info@realobvious.com +1.719.439.8399