The Nillion Standard

The Intelligent Internet

Nillion

May 2025

Contents

1. The Nillion Standard

Every technological era is defined by its invisible foundations.

Electricity, the internet, the blockchain. Each began as an idea, then a network, then a world-changing standard. Not because everyone agreed, but because enough builders did.

We are now entering the most profound shift yet.

The software we use is starting to do more than follow instructions. It's learning, adapting, and making decisions.

Intelligence is no longer locked in tools, it's moving into agents and infrastructure.

But the foundation it runs on is broken.

Today's internet moves documents just fine. But it doesn't protect intent, because it wasn't built for that.

In 2024, the average data breach cost organizations $4.88 million, much of it from untracked "shadow data." Meanwhile, AI-driven technologies are expected to add $15.7 trillion to global GDP by 2030.

That's a future being built on data pipelines we cannot currently secure.

We are flooding civilization with intelligence, and we have no trustworthy substrate for it to run on.

That is the premise of Nillion.

Nillion introduces a new primitive: blind compute. The ability to process sensitive data without ever seeing it. It runs fast, scales across decentralized networks, and gives builders the tools to compose with privacy from the beginning.

This isn't theoretical. Blind compute is already live. Developers are already building with it, unlocking use cases that were impossible before.

A new standard is quietly forming around a simple idea: intelligence can't scale on infrastructure that wasn't built to protect it.

If you believe intelligence should be personal.

If computation should be private.

If you believe the next phase of the internet is still up for grabs.

Then this is your standard too.

The internet for intelligence. The Nillion Standard.

2. The Data Wars: An economy built on transparent glass

The last decade of internet growth was powered by a simple model: Extract data, lock it away and monetize the insights.

Every major platform followed the same playbook. Centralize user behavior. Silo it. Run proprietary algorithms. Sell the output. The more personal the input, the more profitable the system.

And now, AI has supercharged this loop.

In 2024 alone:

- Over **35 billion** records were exposed globally in public data breaches.
- **38%** of employees used unauthorized AI tools at work, contributing to the rise of "Shadow AI."
- AI training compute grew over **400%**, often fueled by data with no clear consent

Every new tool collects more personal data.

Every new model depends on systems users do not fully control.

As AI grows more powerful, the risks grow more invisible.

The result is an infrastructure crisis hiding beneath an innovation boom.

Today's intelligent systems rely on data pipelines that are insecure by design and incompatible with real user control.

There is no shared standard for how personal data should be protected during inference because big techs don't want one.

Centralized platforms thrive on control. The more they see, the more they own.

A shared standard would limit that visibility, and shift power toward users.

There is no open infrastructure for private collaboration between models and individuals.

In short, there is no internet for intelligence. Only a fragmented patchwork of corporate APIs and unaccountable logic.

As intelligence becomes ambient, the surface area for exploitation expands exponentially across financial systems, medical diagnostics, legal arbitration, government infrastructure, and even social trust.

We are feeding the intelligent systems with the raw material of our lives, and receiving no structural guarantees in return.

That is the war to define the base layer those systems will live on.

Transparent glass, or something better?

3. Why Privacy Compute Needs a Foundation, Not a Tool

Privacy is not a new problem.

But every attempt to solve it has run into the same wall: reality.

Over the past decade, privacy-preserving computation has made remarkable progress.

Each approach brings meaningful capabilities and addresses a different piece of the puzzle but despite that progress, adoption has remained limited.

Capability was never the missing component, it's orchestration that we need: a way to combine these tools into something greater than the sum of their parts.

These primitives represent the core pillars of privacy-preserving compute. Each valuable, but none sufficient on its own.

Fully Homomorphic Encryption (FHE): Too early

FHE is a gold standard in theory but a bottleneck in practice.

Encrypt everything, process without decrypting and reveal only the output.

Yes, it works in the lab but it crawls in production.

Even with recent breakthroughs and hardware accelerations, FHE is still far too slow for real-time use. For anything beyond a toy problem, the latency remains a major hurdle, especially for AI agents that need to respond instantly.

Trusted Execution Environments (TEEs): Too fragile

Some teams took the hardware path, using secure enclaves that let a chip process private data in isolation. Intel, AMD, and Nvidia all support some version of this.

TEEs depend on the integrity of the chip and the attestation process, which verifies that no unauthorized or malicious software has been installed preventing the enclave from silently leaking data.

They're best suited for stateless compute, where data doesn't persist for long and the surface for long-term risk is limited.

TEEs are useful, but only if the machine it runs on can be trusted.

Zero-Knowledge Proofs (ZK): Too narrow

The crypto-native approach uses math to prove that a computation happened, without revealing how.

ZK is powerful and is used in rollups, voting, and onchain privacy. They're useful for showing that logic was followed, not for keeping the underlying data private. The prover still sees the inputs, which makes it less suited for collaboration across trust boundaries.

Multi Party Computation (MPCs): Too heavy

MPC distributes trust across multiple nodes, enabling computation on private inputs without revealing them. It's natively distributed and has been a cornerstone of privacy research for decades.

But traditional MPC protocols face a practical wall: bandwidth.

MPC performs well in structured, narrow use cases like digital signatures, voting, and auctions where the algorithm is simple and the inputs are well-defined.

The math behind it is sound but making it usable at scale is a different story. The widespread adoption has been slowed by engineering complexity and performance trade-offs.

These methods have been used to secure computation on infrastructure that was never designed for privacy.

Nillion starts from a different premise.

Rather than relying on any single technique, Nillion composes multiple primitives to push beyond their individual limits, unlocking performance, security, and flexibility that none can achieve alone.

And that begins with a set of principles.

4. Foundational Principles of Blind Computation. *A belief system for the intelligent internet*

If we were building the internet today to interact with intelligence, what would we demand from it?

We wouldn't settle for storing data behind passwords and permissions.

We wouldn't hand our data to centralized processors and hope they behave.

We wouldn't rely on math alone to secure the most personal information on Earth.

We would start with principles.

Principles of an internet built to serve people, not big techs.

Principle One: Data Sovereignty

Every human, system, or agent must retain control over the data they generate.

That means more than just choosing where it gets stored. It means having a say in how it's processed.

Because at the end, if data can't flow securely, it can't be used meaningfully.

Sovereignty is what makes collaboration possible.

Principle Two: Blind Computation

The internet should allow everyone to compute without exposing their underlying inputs.

In the age of AI, computation is the new communication and we believe that communication must be blind by default.

Principle Three: Modular Privacy, Not One-Size-Fits-All

Not every use case requires the same level of security.

Builders need a flexible system that lets them compose their own trade-offs: latency, anonymity, throughput, decentralization.

The future is a marketplace of private agents, each tuned to a different purpose.

Data Sovereignty, Blind Computation, and Modular Privacy form the foundation of Nillion's architecture, they are what Blind Compute enables.

Because if intelligence is the new phase of the internet, then privacy must be the engine that drives it.

Nillion isn't some encryption trick, and it's not a single product either. It's a different way of thinking about how we compute, especially when the data actually matters.

5. Economic Ripples at Global Scale. *T*he birth of the intelligent internet

Blind compute changes the way we handle data, which is a revolution on its own. But most importantly, it opens the door to entirely new economic models.

For decades, privacy was treated as overhead and users had to compromise.

But with Nillion, privacy becomes a growth primitive.

We're no longer just protecting data, we're activating it.

$15.7 Trillion in Unlocked GDP

Some estimates that AI will add over $15.7 trillion to global GDP by 2030. But that projection assumes a world where high-value data remains monopolized by big tech.

It assumes the internet we had is the one AI will run on.

But with blind compute powering a new internet layer, the gains from AI compound.

Imagine:

- Sovereign health networks where citizens control and monetize their biometric data
- Enterprise AI copilots trained on sensitive internal documents, without risk of leakage
- Global credit rails powered by encrypted reputation, not outdated scoring agencies
- Cross-border machine-to-machine trade, enabled by private agents transacting in zero-trust environments

This is the foundation intelligent systems have always needed, but never had.

And it creates an entirely new class of economic factor.

In the next chapter, we look at how these principles translate into architecture.

6. The Petnet. *T*he privacy-enhancing fabric for modular intelligence

Blind compute is a space for inventing how privacy and intelligence work together.

Different use cases demand different balances of privacy, usability and performance.

A trading algorithm needs low latency and input secrecy.

A medical assistant needs compliance, auditability, and cryptographic guarantees.

An onchain agent might need full decentralization, but only for certain operations.

Most existing systems force developers to choose between usability and privacy.

Nillion unlocks a third path: modularity.

At the heart of this is the Petnet. A privacy-enhancing network composed of independent node clusters that run custom configurations of PETs (Privacy-Enhancing Technologies).

Each cluster is built to handle specific trade-offs:

- Some prioritize speed
- Some prioritize security
- Some prioritize jurisdictional compliance

Builders don't have to settle for a monolithic architecture anymore.

Nillion's infrastructure is modular at its core, with the Petnet providing Blind Modules that handle privacy-preserving storage and computation.

These include:

nilDB
Encrypted, queryable storage across a decentralized network of blind nodes without exposing the raw data.

nilCC
Private computation on sensitive inputs including AI workloads, without revealing them to any single node.

Nillion's architecture turns PETs into primitives, and primitives into composable intelligence, the same way Ethereum turned cryptographic signatures into programmable money.

Just as Solidity unlocked a generation of financial tooling, Blind Modules will unlock a generation of privacy apps and new revenue streams for crypto.

This is what it means to build the internet for intelligence.

In the next section, we zoom in on the layer that ensures this system runs honestly, and is governed collectively.

7. NilChain. *T*he incentive spine of the intelligent internet

Computation may be blind, yes, but integrity can't be.

For Nillion to scale globally, it needs more than secure compute.

It needs a way to ensure nodes behave honestly, clusters stay resilient, and access remains open to anyone, anywhere, without trusting a central authority.

That's what NilChain solves.

1. Staking for Integrity
Nodes commit stake to participate in Petnet clusters. Misbehavior, whether provable collusion, dropped shares, or incorrect participation, is punished by slashing.

This creates financial alignment between privacy, uptime, and honest behavior.

2. Governance for the Standard
NilChain supports upgradeable governance structures. Builders and contributors can propose new primitives, vote on protocol changes, and steer the evolution of the Petnet fabric as blind compute moves into new domains and expands to incorporate new PETs.

Think of it as the coordination layer for a modular privacy economy where not all modules are equal and not all trade-offs are static.

NilChain also ensures the infrastructure remains secure, flexible, and responsive to its own growth.

Without it, Blind Compute would rely on offchain trust or centralized infrastructure where access is controlled, and someone always holds the kill switch.

Privacy infrastructure doesn't matter until people can actually build with it, and prosper from it.

The most powerful ideas in crypto: programmable money, permissionless apps, verifiable compute scaled because developers could actually build with them.

That's the role of the Secure Stack: Nillion's reference architecture for privacy-native applications.

Each stack component is a pattern. Together, they show what's possible when blind compute is built in from the start.

1. Secure Vault. *B*lind storage with permissionless logic.
A personal data hub which developers can build on to allow individuals and organizations to store their encrypted information, everything from identity credentials to medical files to trading strategies, and selectively authorize compute access without ever revealing the data itself.

Use cases:

- Self-sovereign health records
- Encrypted customer segmentation
- Secure memory layer for AI agents

2. Secure Inference. *P*rivate inference on high-value inputs.
Instead of exposing sensitive inputs to OpenAI, Google, or Anthropic, Secure Inference routes user queries through nilCC, allowing for blind computation on context-rich data, even across multiple organizations.

Think of it as your brain, private by default.

You remember things, reason through them, and take action without anyone watching what's going on inside.

That's exactly what the Secure Stack enables for applications:

- Secure Vault is your memory. It stores sensitive data, securely and privately.
- Secure Inference is your reasoning. It processes that data to generate insights, without exposing it.
- Secure Signer is your action. It verifies, signs, and responds, without leaking your intent.

Use cases:

- Administrative assistant that processes your documents without seeing them
- HR copilots that know your org structure without leaking it
- Private meeting copilots that align teams without leaking context to Big Techs
- Research agents that analyze patient data to advance cancer treatment without breaking confidentiality

3. Secure Signer. *D*elegated authority with blind verification.
An embedded module using nilVM to sign messages, verify actions, or trigger smart contracts. All without exposing the user's intent or identity.
It's a blind brainstem for agentic actions.

Use cases:

- Co-signing AI agents with rules-based control
- Private authorization for enterprise access
- Encrypted intent verification for DAOs or multisigs

The Secure Stack is a blueprint that shows developers how to think in this blind new world.

Every vault, every LLM, every signer is a signal: Intelligence without privacy is never progress, it's merely exposure.

As more developers reach for these tools, we'll see a wave of applications that don't just protect user data, they make it useful again.

8. The Builders' Oath. *T*he culture of the intelligent internet

Every movement that rewires the world begins with a cultural spine.

Bitcoin had its cyberpunks.

Ethereum had its programmable philosophers.

Nillion is summoning its blind warriors to create a new standard, the Nillion Standard.

If you're a developer, founder, or thinker helping build the intelligent internet, you're already a blind warrior.

And it demands an oath.

The Blind Warrior's Oath

We build on privacy by default because privacy is a human right.

We don't extract, we compose.

We believe computation should be blind.

We respect context as capital.

We leave no data behind in the systems we create.

We require our network to be open to all builders and accessible for all users.

We optimize for the unseen.

We don't demand trust.

We allow for verification, blindly.

Because nothing is ever revealed.

This is the principle we run on.

Nillion gives builders tools to build with privacy.

But more importantly, it gives them a standard to protect.

In the final section, we'll show how anyone, developer or not, can step into that standard and help shape what comes next.

9. Joining the Network. *H*ow to become part of the intelligent internet

The internet for intelligence won't be built by a single person.

It will be built by a network of conviction. Developers, validators, researchers, agents, and users aligned around a single principle:

Blind Computation is the foundation of intelligent infrastructure.

Nillion exists to make that principle usable.

Now it's time to make it unstoppable.

If you're a developer

You can start building with Blind Modules right now.

- Use nilDB for encrypted, queryable storage
- Use nilCC to run private LLM inference pipelines
- Use nilVM to sign, verify, or authorize actions blindly

Get grants. Join testnet clusters. Compose your own Petnet configuration.

You don't need to know cryptography. You just need an idea that shouldn't require trust.

If you're not technical

You still have skin in the game.

Nillion's architecture rewards more than code.

- Validate nodes and stake into privacy clusters
- Propose governance changes on NilChain
- Contribute to documentation, education, or community initiatives
- Evangelize the shift from surveillance AI to sovereign AI

The New Nill Pill

This isn't a red pill or a blue pill.

It's a Blind Pill.

You don't need to rage against surveillance.

You don't need to wait for regulation.

You don't need to trust any system to start changing it.

You just need to build on new primitives.

The internet of intelligence is already forming.

And Nillion is shaping it.