

What is

Magen is a **parametric, liquid, and permissionless** insurance marketplace. Our strength lies in three core architectural pillars:

- **Market-Driven**

Both Covered Tokens (CT) and Yield Tokens (YT) are priced purely by supply and demand, creating a real market for risk. Users can enter or exit protection and yield positions at any time, instantly, and at the prevailing market price.

- **2. Frictionless**

Magen is fully permissionless and automated, with no KYC for any type of position. As a parametric system, payouts are triggered automatically when predefined conditions are met. There are no claims to file and no discretionary committees: once the event is verified, compensation is executed programmatically, typically within 30 days or sooner.

- **Solvency by Design**

Magen operates as a closed and overcollateralized system. Every potential payout is backed 1:1 by USDC locked in protocol vaults before coverage is issued. This removes counterparty risk entirely—the capital required to pay claims is already secured on-chain at the moment protection is purchased.

How it works

1. Insurance Pool Creation

A Liquidity Provider (LP, can be a DeFi Protocol, DAO, Risk-Curator or Institution) deposits USDC into the Magen Vault. For every USDC deposited, the system mints a pair of tokens: **Covered Token (CT)**, **Yield Token (YT)**. These tokens are seed in the Insurance Pool (IP) in a ratio that reflects the CV value (the premium paid and the risk perceived).

2. Active Trading

The **Insurance Pool (IP)** is now live and active. Participation is fully permissionless, and users can interact with the pool in three distinct ways:

a. Insurance Buyers

Users seeking protection can purchase insurance by acquiring **Coverage Tokens (CV)**.

Holding CV tokens grants exposure to insured capital in the event of a covered incident.

b. Protocol Insurers

Users who wish to underwrite risk act as protocol insurers by holding **Yield Tokens (YT)**.

Their return is derived from the residual value of the pool, represented by the value of YT.

c. Liquidity Providers

Liquidity Providers can supply CV and YT to the Insurance Pool and earn **trading fees and liquidity-driven yield** generated by market activity.

3. Settlement & Claim

At maturity, or upon the occurrence of a covered event, the oracle determines the final state of the Insurance Pool based on verifiable on-chain data. Possible Outcomes:

a. No Event Occurs

- No exploit or adverse event is detected.
- **YT value converges to 1**, while **CV expires worthless (0)**.
- **YT holders** capture the insurance yield.
- **Liquidity Providers** earn the accumulated swap fees generated by trading activity.

b. Partial Hack

- Only a portion of the insured funds is affected by an exploit.
- **CV value reflects the percentage of funds compromised.**
- **YT captures the remaining, unhacked portion of the pool value.**
- Payouts are distributed proportionally based on the verified loss ratio.

c. Total Hack

- A full loss of the insured funds is detected.
- **CV value converges to 1**, while **YT converges to 0**.
- CV holders receive the full insured amount.

For CV Holders, Positions are verified using **on-chain snapshots** taken at the time of the event. Claims are processed automatically, with payouts completed in **less than 30 days**. **YT Holders** can **redeem their tokens instantly** once the final outcome is resolved.

Customers Personas



Social Media Strategy

-
1. **Business Owners** - 40% people underestimate how easily their business can be hacked.
- Hack intrusiveness: 100%
- Hackers often seek a quick fix or a quick win.
- Common attack vectors include social engineering, malware, ransomware, and DDoS attacks.
2. **Employee Business Owners**
- Business owners believe their business is more secure than it actually is.
- Hackers often seek a quick fix or a quick win.
- Common attack vectors include social engineering, malware, ransomware, and DDoS attacks.
3. **Office Staff**
- Business owners think business is public.
- Hackers often seek a quick fix or a quick win.
- Common attack vectors include social engineering, malware, ransomware, and DDoS attacks.
4. **Small Business Owners**
- Business owners are less concerned about security than larger companies.
- Hackers often seek a quick fix or a quick win.
- Common attack vectors include social engineering, malware, ransomware, and DDoS attacks.

Launch Strategy

-
- Initial Launch:**
1. Create a beta test message on Twitter and LinkedIn.
2. Create a group with 1000+ users from various industries, regions, and backgrounds - 1000 members - they are your first customers and your early adopters.

-
- Early Successes:**
1. Create beta messages, share them, and publish them on sites that have an early adopter culture.
2. Reach them out with an exclusive offer designed for early customers.

-
- Ongoing Launch:**
1. Use promotional messaging to keep them engaged.
- Social media
- Networking with other members
- Personal support teams, webinars
- Q&A forums and discussion groups.

-
- Ongoing Engagement (Advanced):**
1. New features for each user's personal interests and needs.
- Personalized emails, videos, and notifications.
2. Reach them off-channel:
- Personalized emails
- Personalized messaging