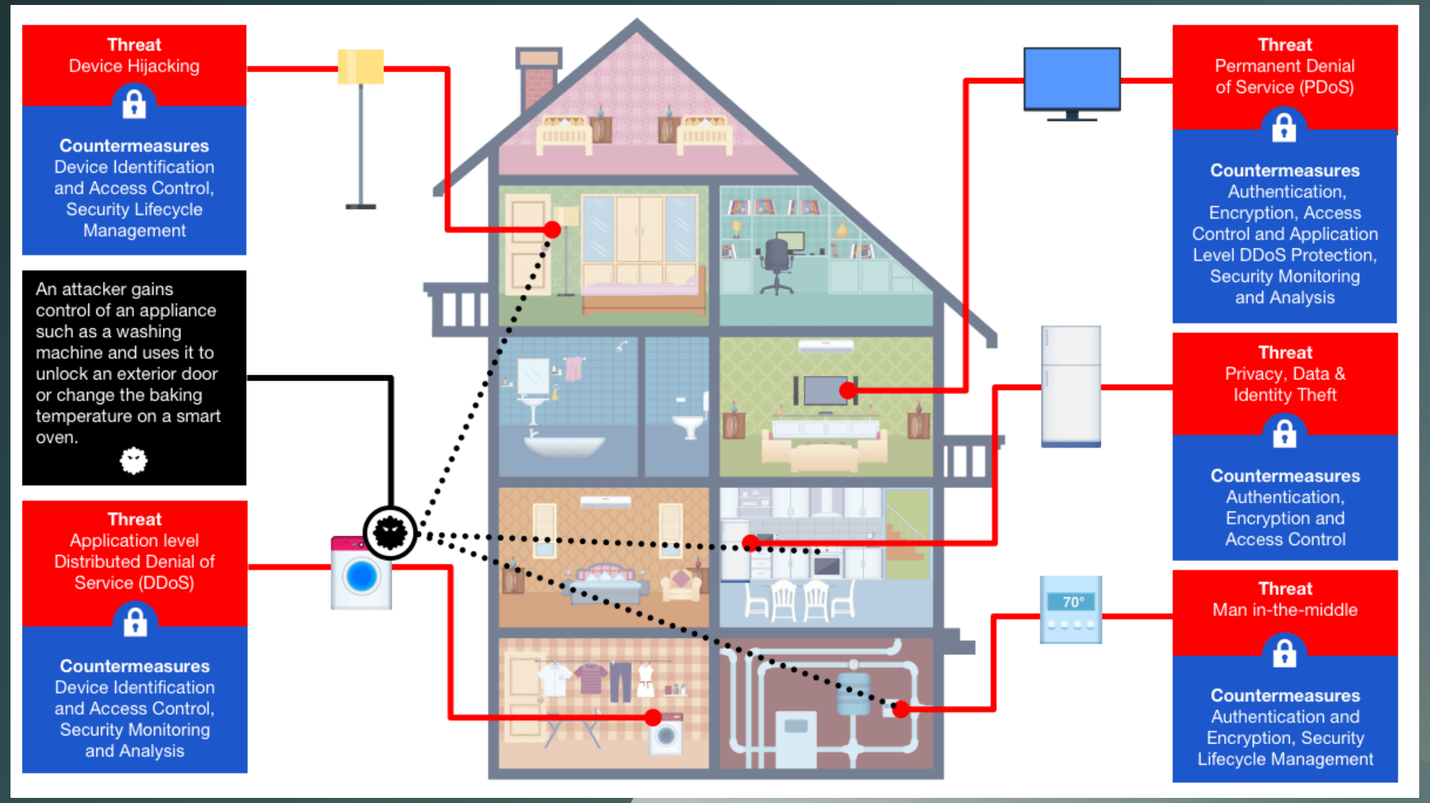
Home IoT Guardian

Reclaiming privacy in a connected world

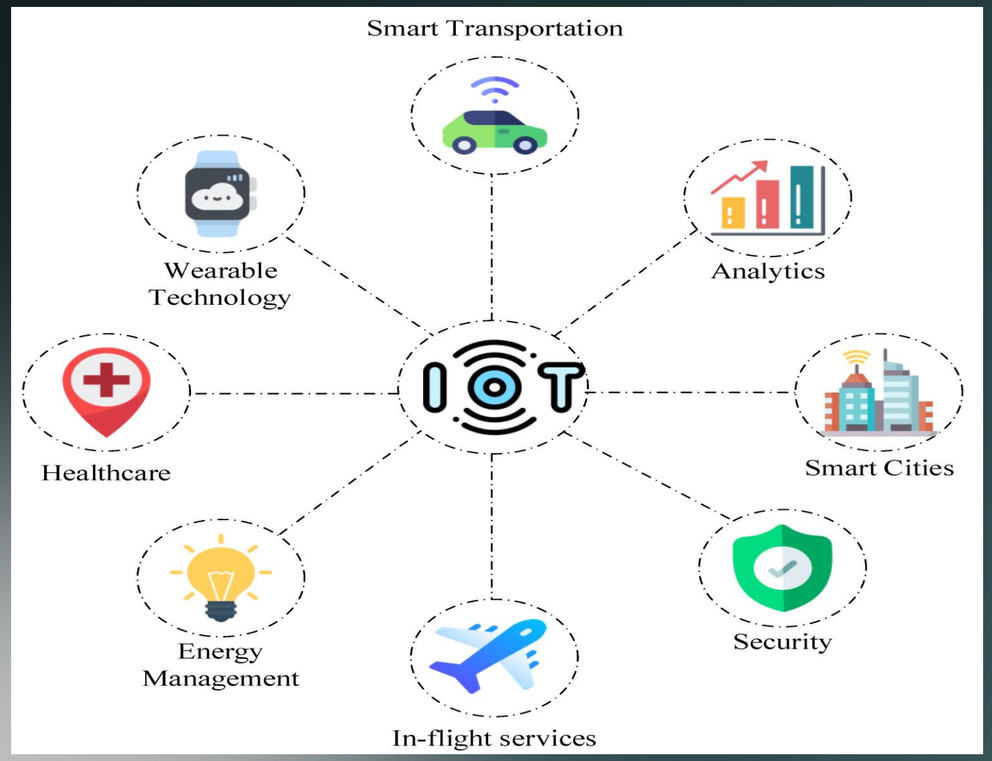
Vada Boyz

The Problem - Rising IoT Threats

- **Home networks vulnerable**: 820K daily attacks from botnets like Eleven11 and Mirai.
- **Weak passwords & firmware** expose cameras, thermostats to spying & DDoS.
- **75% devices at risk**; cyber costs hit $10.5T annually.
- Families face **privacy invasions**—e.g., unauthorized surveillance.
- **2025 surge:** Botnets compromised 86K+ devices for 5.6 Tbps attacks.



The Problem - Scale of the Crisis



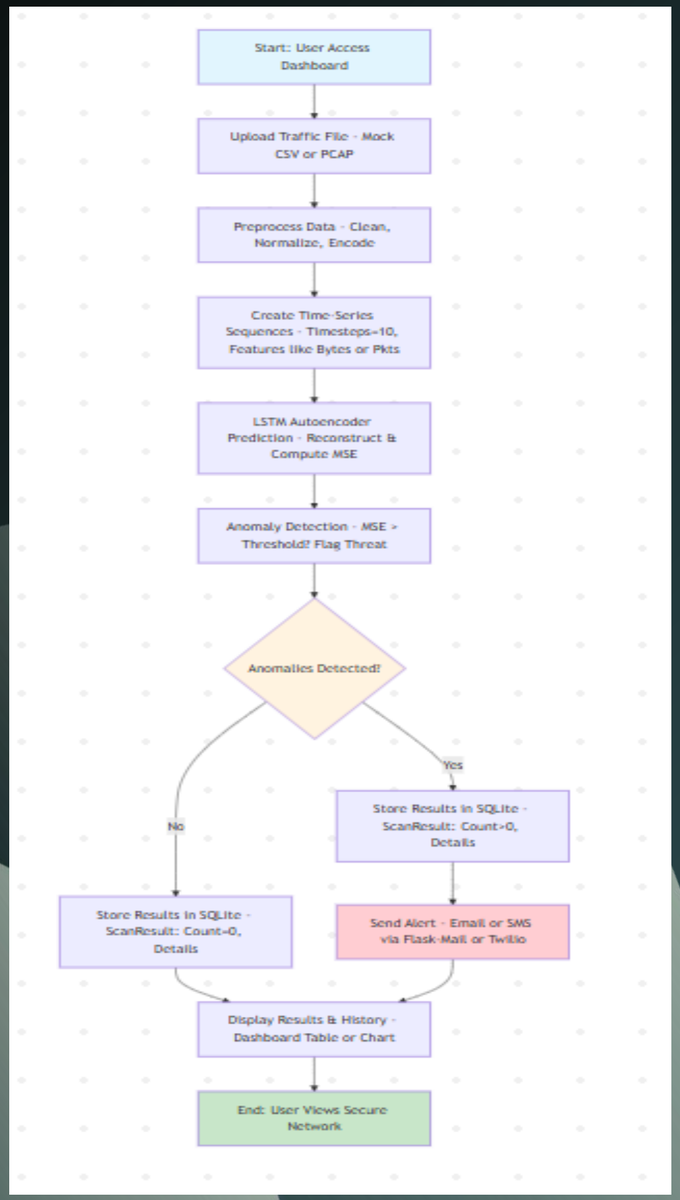
Global IoT devices: 18B in 2025, up 50% YoY

High-impact breaches: NVRs and IP cams most vulnerable per reports.

Economic toll: Billions in losses from privacy & infrastructure attacks.

Underserved market: Homes lag behind enterprise security.

Home IoT Guardian



AI-Powered Threat Detection

AI-driven web dashboard for anomaly detection in network traffic. Uses LSTM ML to spot threats (e.g., data spikes) with 85%+ accuracy.

Real-Time Alerts

Phishing, ransomware, and social engineering are tactics used to steal or damage data.

Freemium model

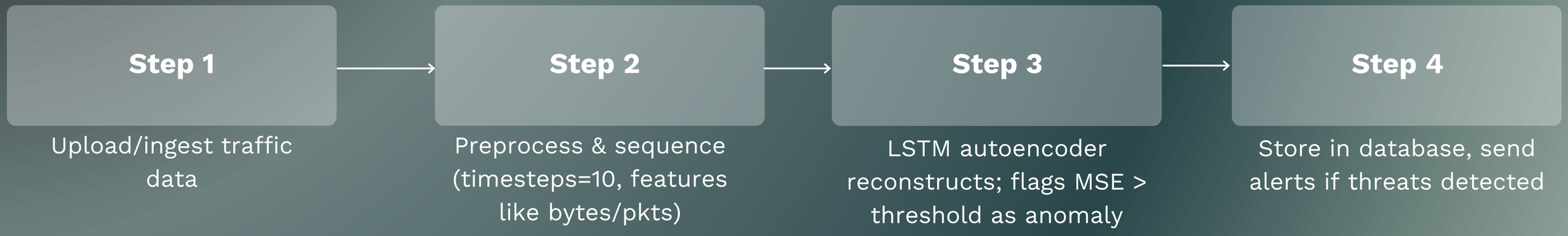
Free scans, Rs. 399/month premium for edge integration

Scalability and Privacy

Scales to routers with federated learning for privacy

How it works - core technology

Tech stack: Python/Flask, scikit-learn/Keras (200K params model), Postgres (SQLite for demo)



How it works - User flow

Upload

User uploads traffic file via dashboard.

Analysis

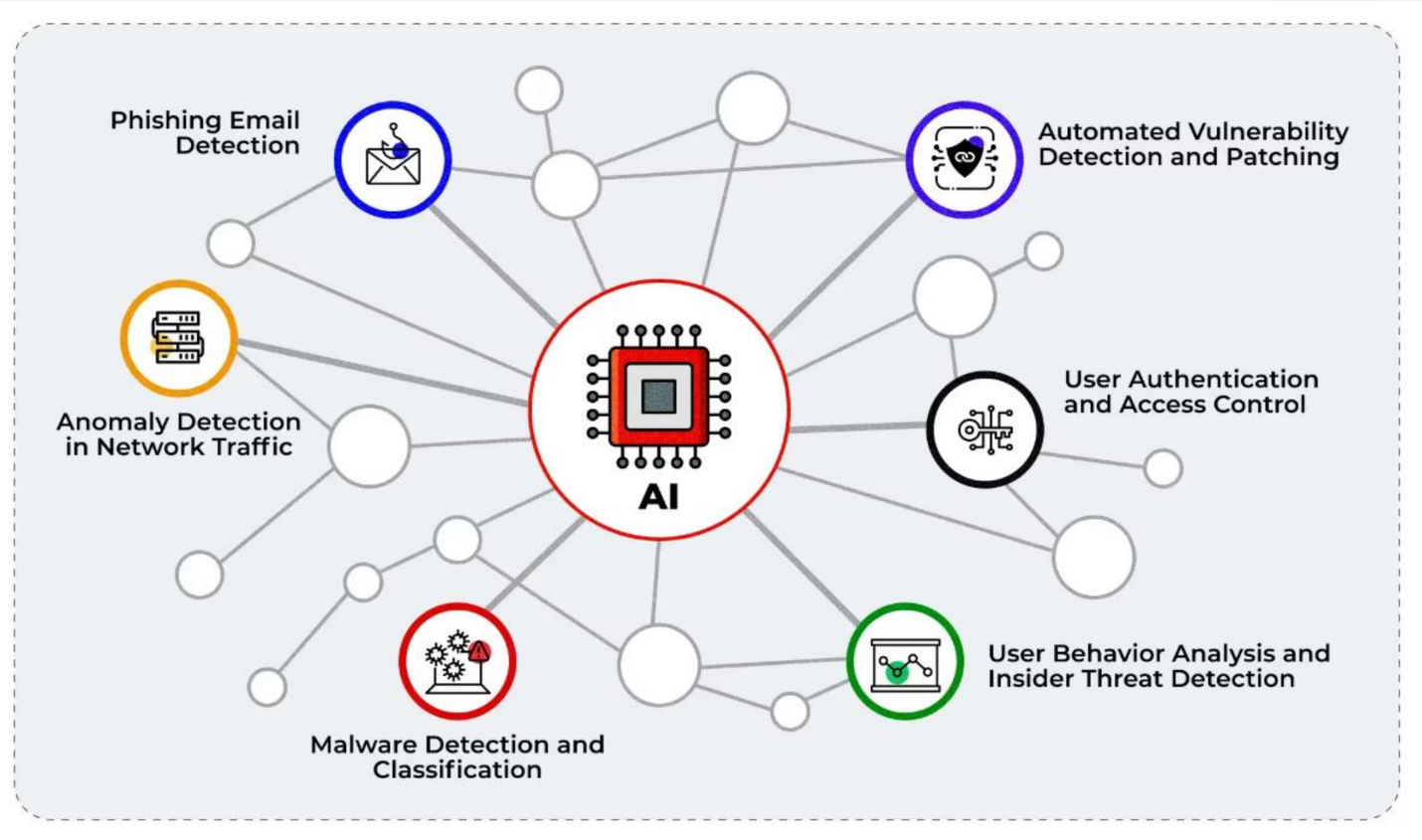
AI analyzes in <4min, detects >85% threats, <10% false positives

Review

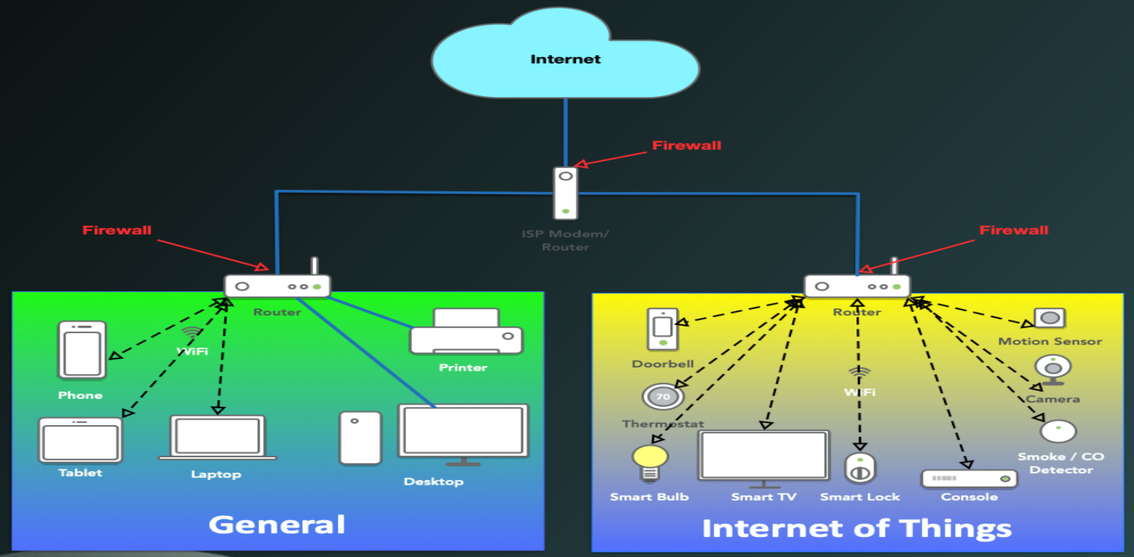
View results/history; get email/SMS alerts

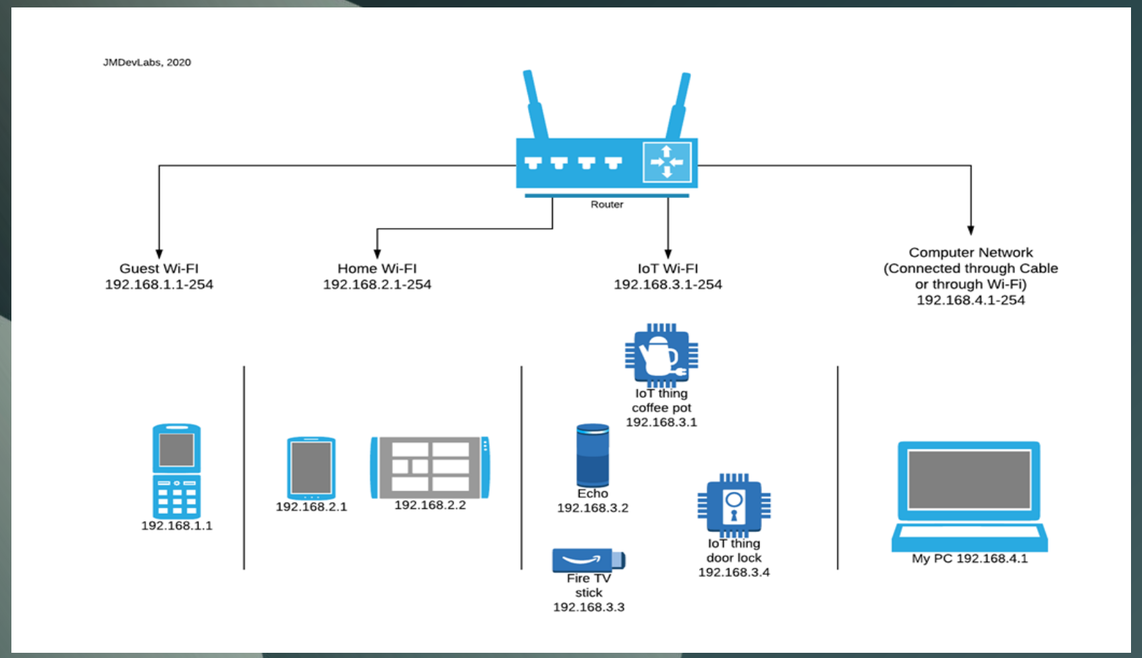
Expansion

Real-time edge ML on routers



Future Integrations





Router Firmware Integration

Embed AI anomaly detection directly into router firmware (e.g., Netgear, TP-Link) Enables always-on protection with OTA updates; white-label for revenue share (10-20% on premium models)

Anomaly Handling & Device Isolation

On detection (e.g., traffic spikes), auto-quarantine via VLAN segmentation or MAC blocking to contain threats. Use SDN APIs for dynamic rerouting; notify users for remediation (e.g., firmware updates)

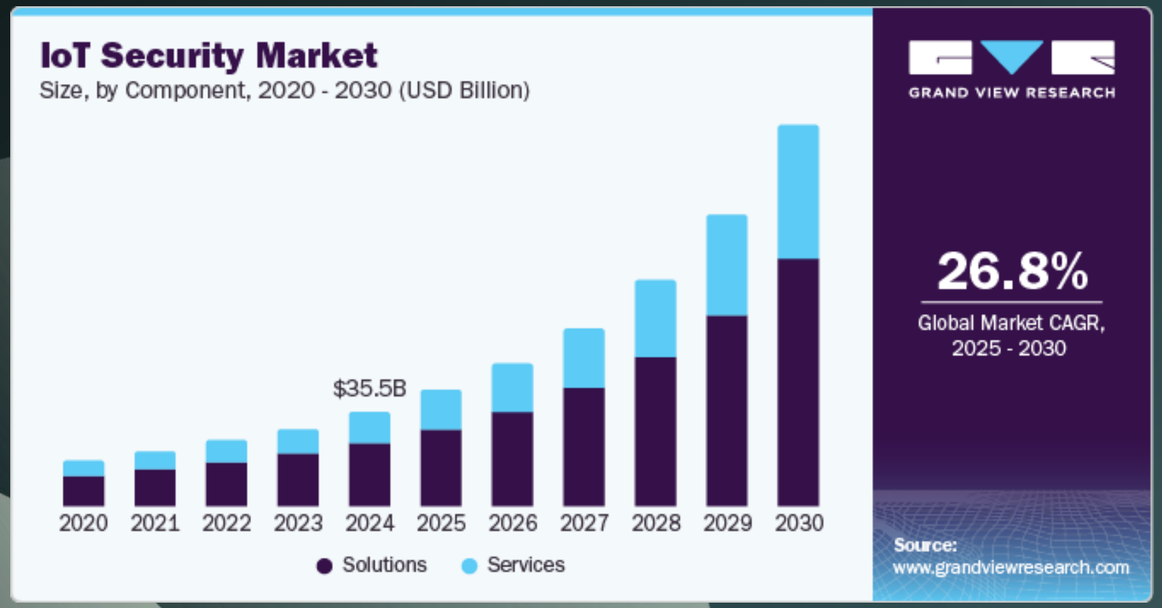
Secure, simple device onboarding

Devices are verified using hardware signatures/serial numbers etc. Users will be warned if they try to install an unverified device, and these devices will be added to an isolated layer.

Overall Benefits

Scales to edge computing for real-time security; boosts user retention 20-30% via trust-building; addresses 70% of home IoT risks from unauthorized devices.

Market Potential



TAM

$270M in 2025 for India IoT security, growing to $2.34B by 2033 at 31% CAGR—driven by 2B connected devices by end-2025

SAM (Home Segment)

$54M (20% of TAM, focusing on urban households with 10+ IoT devices)

SOM

$5.4M Year 1 (1% capture, targeting 5M Indian homes at $1.08 ARPU; 5% conversion from free trials)

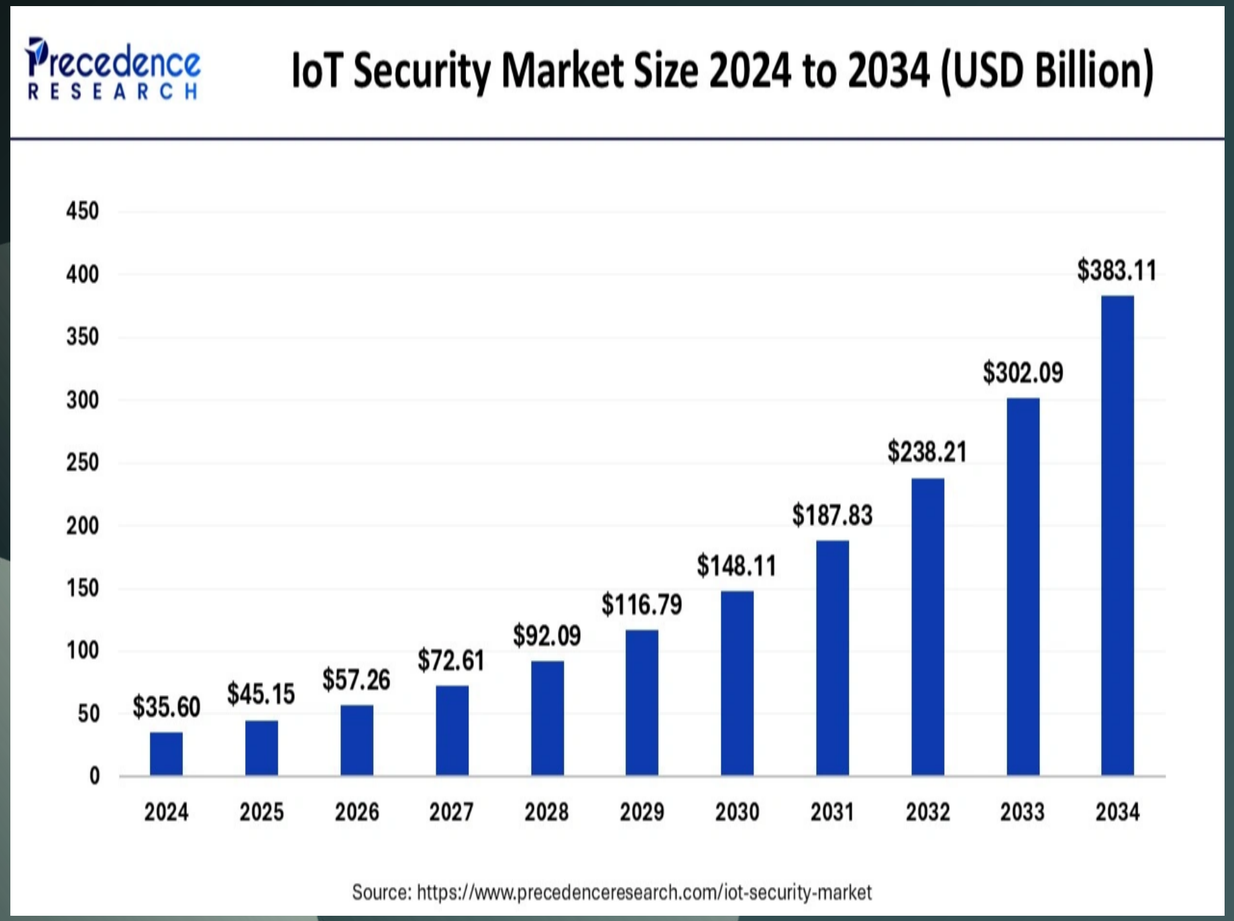
Drivers

Rapid IoT revenue to $26.93B in 2025; regs like DPDP Act & IT Act mandating data protection for IoT

Competitors

Global like Nozomi/Armis; local edge via affordable home focus over enterprise-heavy players.

Go-to-Market Strategy



Target

Urban homeowners/families with smart homes; 62M households by 2025, prioritizing Tier-1/2 cities

Channels

Freemium app on Google Play/Apple Store; e-commerce via Flipkart/Amazon; B2B partnerships with Jio Fiber & Airtel Xstream

Pricing

Free basic scans, ₹399/mo premium (subscriptions + router upsell bundles)

Launch

Q1 2026 beta in metros; marketing via SEO, YouTube influencers, and Smart Cities initiatives

Metrics

50K users Month 1, 75% retention; monetize via SaaS with ARPU ramp-up through telecom tie-ups

Thank You