



SECURITY OVERVIEW

Built secure, from the ground up

How Shopnix protects your store, your customers and your data: across the network, servers, application, data and people.

1. Our approach

Security at Shopnix is designed into every layer of the platform and run by one accountable team. The appendix lists the controls in each layer. Nine layers work together, from the network edge to tested backups, so that no single failure exposes your business. The same team that builds the platform operates it, watches it and answers for it.

2. Network and infrastructure

- **Managed cloud servers** run and maintained by the Shopnix operations team, with Shopnix cloud, dedicated cloud and on-premise options.
- **Firewall around every server:** only the services the store needs are reachable from the internet.
- **Global CDN:** store images, themes and static files are served from Amazon CloudFront, which also absorbs traffic spikes at the edge.
- **Bot protection and rate limits:** abusive bots are detected and blocked; sign-up, login and contact forms are protected with Google reCAPTCHA.
- **Hardened servers** running current, supported releases of the operating system and server software.

3. Application security

- **HTTPS everywhere:** every storefront, admin screen and API call is encrypted in transit, with certificates issued and renewed automatically.
- **Payments on certified gateways:** card details are handled by PCI DSS-certified gateways such as Razorpay, PhonePe, Cashfree, PayU, Stripe and PayPal. Card data never touches your store.
- **Reviewed code:** every change passes design review, frontend and backend code review, and testing on staging before release.
- **Secure sessions** for shoppers and staff, with protection against common web attacks built into the platform.

4. Data protection

- **Isolated per store:** each store's catalogue, customers, orders and settings are kept separate. No store can access another's data.
- **Your data stays yours:** export products, customers and orders whenever you want, and take them with you if you ever leave.
- **Minimal collection:** we store what is needed to run your store, and nothing from your customers' cards.
- **Deployment choice** for data residency: run on Shopnix cloud, a dedicated cloud, or in your own data centre.

5. Access control

Role	What they can do
Owner	Full control of the store, billing and who has access.
Admins	Run catalogue, orders, staff and settings across the business.
Staff	Only the screens their role needs, chosen from about 190 named permissions.
API users	Each with their own API key, which can be removed at any time.

- **Single sign-on** for Store Manager with Google Workspace or Microsoft. Leavers lose access the day they leave.
- **Access reviews every month** for Shopnix staff with access to production systems.

6. Backup and recovery

What	How often	Why it matters
Full backup	Every day	Yesterday's store, always one step away
Weekly backup	Every week	A longer safety net for older changes
Separate copies	Three	One failure never takes your data with it
Restore drills	Every month	Proof the backups work, before they are needed

A documented recovery runbook brings back sign-in, catalogue, checkout and orders first, so you are selling again as quickly as possible.

7. Patching and maintenance

- **Critical security fixes within 48 hours.**
- Regular updates for everything else, scheduled around your sale calendar.
- Planned maintenance announced in advance and kept outside your peak hours.

8. Monitoring and incident response

Step	What happens
Detect	Round-the-clock monitoring of stores, servers, backups and certificates, with alerts to the operations team.
Respond	Critical issues are picked up within 15 minutes, including outside working hours.
Fix	Worked until resolved, with updates in your private WhatsApp group.
Report	A root-cause report and the steps taken to stop it happening again.

9. Change management

Every change follows a tracked pipeline: requirement, design and design review, frontend and backend development with code review, testing on a staging copy of your store, release with your sign-off, and close monitoring after release.

10. Your security reviews

We work with your IT and security teams on questionnaires, vendor assessments and audits, and walk them through this overview in detail. Ask your account manager, or talk to our enterprise team at shopnix.io/enterprise.

Appendix: technical controls

A summary of the controls behind the nine layers, for IT and security reviewers. Configuration details are shared under NDA during a security review.

Layer	Controls
1. Network	Deny-by-default host firewall on every production server; only required inbound routes open. Admin tools and database ports kept off the public internet. Server access restricted by source. Repeat failed logins blocked automatically. New services stay closed until reviewed. Public web routes separated from internal service routes. Traffic watched at edge and server level, with rate limits applied when abuse appears.
2. Servers	No root login; key-based access only, with keys rotated when team access changes. Production shell limited to a small named operations group, each login tied to a named account, no shared credentials. Only listed system users can connect. Login attempts capped and timed out. Critical patches within 48 hours of a verified impact; regular updates in planned windows. Authentication and service logs kept for incident tracing.
3. Core services	Web server hardened, unused modules removed, server signatures hidden. Database users scoped to least privilege, with separate users for application and maintenance work; remote database access closed. Directory listing disabled. Only required services run at startup. Web server, database, runtime and OS packages patched monthly.
4. App servers	Request type, length and format validated before any write. Server-side sessions, re-checked for privileged actions. Uploads checked for type and size and safely renamed; executable files blocked. Inputs normalised and outputs encoded. Strict type checks on totals, IDs and dates. Login, OTP and reset routes throttled per IP and per session.
5. Application	Validation in the browser and on the server, with the server as the final gate. Prepared statements for all database access. Session identity and ownership checked before account changes, coupon use and order actions. OTPs expire quickly, with resend cool-downs and retry limits. reCAPTCHA on high-abuse forms. Checkout follows strict state checks. Social login tokens verified with the provider.
6. Data	Store-level checks on every request: one store cannot read or change another's data. HTTPS for admin and storefront sessions; credentials and cookies only over TLS. Card data handled by payment gateways and never stored as raw card numbers. Logins, role changes and critical actions logged. Sensitive reads need an active session. Logs and backups kept for defined retention windows.
7. Access	Role-based access for owner, admin, operator and limited users, with about 190 permissions. Billing, orders and settings separated by role. Access reviewed monthly and stale access revoked promptly; temporary elevated access is time-bound. Sessions expire and sensitive tasks need re-authentication.
8. Monitoring	Web, runtime, authentication and application logs reviewed daily. Alerts on repeated authentication failures, abnormal spikes and service errors. Storefront and admin checked round the clock. Bot traffic, credential stuffing and request floods tracked and blocked at firewall and application level. Latency, error rate, CPU and memory trends tracked.
9. Backup and recovery	Daily backups of live order data and weekly full-store snapshots, automated and monitored. Three copies: production snapshot, offsite copy and cold archive. Backups checked for readability and completeness. Monthly restore drills. A documented recovery runbook with clear ownership. Restore order: login, catalogue, checkout and orders first.

Shopnix Enterprise · shopnix.io/enterprise · Talk to our enterprise team at shopnix.io/enterprise

15 years of building and running large-scale ecommerce in India. The Indian alternative to Shopify Plus. This document summarises our standard practices; your agreement sets out the final terms for your business.