



PNB Housing Achieves Continuous Compliance & Protection with AppTrana's AI-Powered Vulnerability Remediation

ABOUT THE CUSTOMER

PNB Housing Finance, a leading publicly listed housing finance company in India, serves millions of customers across 500+ cities. Its growing digital footprint includes portals for onboarding, loan management, and APIs for partner integrations - all critical to operations. Security and availability are vital for customer trust and compliance. PNB Housing has relied on Indusface AppTrana WAAP for comprehensive protection since shifting from a North American CDN-based WAAP vendor over 2.5 years ago.

CHALLENGES

At first, the solution worked, but the scale and hybrid nature of PNB Housing's applications soon exposed security limitations. Here are some of them:

- **Custom Port Support:** Certain critical applications operated on non-standard ports. Their existing WAF did not support these ports, leaving some applications unprotected and creating potential security gaps.
- **Lack of Integration Between Scanning and WAF Tool:** The organization relied on separate vulnerability scanning and WAF tools. Their existing WAF did not communicate with their scanner, making virtual patching of vulnerabilities difficult. This disjointed setup led to delays or missed protections, leaving critical applications exposed for longer than necessary.
- **Hybrid Application Landscape Exposed Gaps:** The company had some hybrid applications, combining web interfaces and APIs for back-end or partner integrations. Protecting API-heavy applications required custom rules, either manually created by the security team, which required significant time and resources, or implemented via their vendor's professional service at a heavy cost.
- **Support & Configuration Friction:** When issues arose, often due to complex traffic patterns or hybrid requirements, configuration updates took significant time to get implemented, which increased risk during critical incidents or deployments, thereby reducing operational confidence.
- **Traffic Routing Limitations:** Several applications required URL redirection and path-based routing to handle complex user flows or back-end services. For example, users logging in from different regions needed to be automatically redirected to their regional portals, and API requests for different services had to be routed to the correct backend systems.

SOLUTION

Indusface delivered a fully managed and adaptive WAAP solution that addressed every challenge while improving the organization's operational efficiency and security posture.

- **Seamless Support for Custom Ports:** The deployment was provided to handle applications running on non-standard ports, instantly closing the security gaps that previously left critical workloads exposed. This allowed the PNB Housing security team to protect every application uniformly without workarounds or manual monitoring, ensuring no part of the infrastructure was left vulnerable.

- **Integrated PTaaS and WAF for Instant Vulnerability Remediation with SwyftComply:** AppTrana WAAP's built-in PTaaS platform automatically scanned for vulnerabilities and sends them directly to the WAF for instant virtual patching with SwyftComply. This removed silos, cut down manual effort, shortened exposure windows, and eliminated the need for a separate scanner, keeping critical applications and APIs fully protected at lower cost.
- **Faster, Managed SOC-Driven Configuration Updates:** Indusface's managed services team worked as an extension of the customer's security team, offering 24/7 monitoring of attacks, SLA-backed response times, and instant configuration changes or rule deployments without false positives. This ensured that threats were neutralized in real time, giving the organization peace of mind that its sites remained protected (in block mode) continuously.
- **Holistic Protection for Hybrid Applications:** AppTrana delivered unified protection for web applications and APIs under a single framework. Automatic discovery enabled one-click onboarding, and the Indusface team seamlessly deployed custom rules and positive security models. This minimized manual effort for the customer and enabled the security team to focus on strategic initiatives instead of firefighting.
- **Dynamic, Policy-Driven Traffic Routing:** Indusface WAAP's flexible routing allowed path-based routing and regional redirects to be configured effortlessly. This ensured that users and API requests were always directed to the correct servers without delays, enabling the faster rollout of new applications and maintaining consistent security policies across all user journeys.
- **AI-Powered, Holistic Protection and Additional Capabilities:** AppTrana not only addressed the challenges but provided a holistic AI-driven solution supported by a dedicated managed security team. It delivered proactive protection from DDoS attacks, malicious bots, API abuse, and zero-day vulnerabilities. Combined with continuous vulnerability discovery, instant remediation, client-side protection, and a 100% uptime guarantee, the customer benefited from a single, comprehensive solution that reduced complexity, eliminated security blind spots, and strengthened their overall security posture.

RESULTS

- Over 44 million attacks blocked in a year, with 90% of sites facing bot attacks and 85% facing DDoS attacks
- 211 vulnerabilities virtually patched, and 22+ clean, zero vulnerability reports were provided for compliance
- 100+ custom rules applied over the year
- Customer protected with AppTrana WAAP for over 2.5 years with zero downtime

CUSTOMER QUOTE

"With AppTrana WAAP, every application runs in block mode and is safeguarded 24/7 with guaranteed 100% uptime. The depth of support, responsiveness, and commitment we experience with Indusface is truly unmatched. By partnering with Indusface, we have not only elevated our security posture but also achieved significant operational savings."

Anubhav Rajput (CIO & CTO, Head of Digital Transformation - PNB Housing Finance)

