INDUSFACE™

CASE STUDY

Bandhan Life

LIFE INSURANCE · INDIA ENTERPRISE

AppTrana WAAP | Managed Service

> "AppTrana WAF is disrupting the market with a compelling cost-value proposition for businesses by including autonomous vulnerability remediation and high-value services such as managed custom rules, security assessment, and risk-based managed cloud WAF protection."

Aniket Gandhi
AVP, Information Security Governance,
Bandhan Life

Bandhan Life

- Trusted by 300,000+ customers
- 99.73%+ claim settlement ratio

PRODUCTS USED

- ✓ AppTrana WAAP
- ✓ SwyftComply AI — autonomous virtual patching
- ✓ Behavioral DDoS & Bot Mitigation
- ✓ API Protection
- ✓ Managed VAPT & Daily Scanning (WAS)
- ✓ 24×7 Managed Security Services

Autonomous Protection at Scale: How AppTrana Keeps Bandhan Life's 300,000+ Customers Secure

In recent years, Bandhan Life Insurance made large changes to its technology and infrastructure. These changes included migrations between content delivery networks (CDNs), a full brand transition, and updates to its technology stack. During these changes, Bandhan Life used Indusface AppTrana to protect its applications. AppTrana also decreased the time that vulnerabilities stayed exposed and kept security coverage continuous across the environment.

RESULTS AT A GLANCE

During the recorded period:

- ✓ 10.34 million attacks blocked
- ✓ 13,000+ exploit attempts blocked by custom rules
- ✓ 0 security incidents escalated to Bandhan Life's team
- ✓ Vulnerability remediation reports delivered within SLA
- ✓ 5 million+ DDoS attacks blocked
- ✓ 24×7 managed security coverage
- ✓ 2.4 mn attacks blocked by app-specific virtual patches
- ✓ Remediation process aligned with IRDAI timelines
- ✓ Quarterly board-ready insights benchmarked against the insurance industry

ABOUT BANDHAN LIFE

Founded in 2008, Bandhan Life Insurance, formerly Aegon Life Insurance Company, is an Indian life insurer offering individual and group insurance through online and offline channels.

For more than seven years, Bandhan Life has run its application security through Indusface's AppTrana platform, protecting its internet-facing footprint from attacks. The relationship began in 2019 with Indusface's WAS service helping Bandhan Life with vulnerability assessment and penetration testing (VAPT) and has since expanded to include web application and API security, CDN, DDoS and bot mitigation, and executive security reporting across the organization.

Today, AppTrana protects Bandhan Life's internet-facing applications while a dedicated Indusface security engineer validates findings, fine-tunes security policies, and works alongside its security team to address risks before they affect customers.

KEY SECURITY CHALLENGES

Protecting a changing application environment with a lean security team

Bandhan Life needed to solve four challenges at once: keep every application protected through infrastructure and CDN changes, close vulnerabilities before they reach production, meet IRDAI's continuous monitoring and remediation requirements, and turn security data into board-ready insights and reviews without adding operational complexity.

© 2026 Indusface Pvt. Ltd. All rights reserved.

01 Vulnerabilities outpacing a continuously shipping codebase

Bandhan Life's application team works in short sprints with releases every couple of weeks. This meant that periodic pen testing and remediation cycles were not fast enough to identify and remediate vulnerabilities. The security team needed a faster way to identify vulnerabilities and protect validated findings while developers worked on permanent code-level fixes within scheduled release windows.

02 Keeping protection accurate as infrastructure changed

The transition from Aegon Life to Bandhan Life required new and legacy applications to run in parallel across two CDNs before the old applications were decommissioned. Each change altered the normal traffic baseline. The team needed real-time, adaptive protection without creating coverage gaps or false positives. With thousands of customers accessing its applications daily, maintaining low latency was equally important. Bandhan Life tracked application performance independently through a third-party monitoring tool.

03 Meeting IRDAI compliance with a lean security team

IRDAI's Information and Cyber Security Guidelines require continuous application security monitoring, timely remediation, and closure of high-risk vulnerabilities and audit findings within defined timelines. Bandhan Life also tracks remediation of critical and high-severity vulnerabilities against internal SLAs. Meeting these requirements called for continuous vulnerability scanning, effective remediation workflows, autonomous virtual patching, and audit-ready evidence without increasing the operational burden on its security team.

04 Turning security data into board-ready insight

The board asked for a risk picture every quarter. Collating it meant pulling logs, reconciling them, and rebuilding the narrative from scratch each time. Bandhan Life needed consistent, industry-benchmarked insights that could help its CISO explain the organization's risk posture and security trends to leadership.

THE SOLUTION

How AppTrana addressed these challenges

The Indusface AppTrana platform combines autonomous vulnerability remediation with expert oversight. A dedicated security engineer reviews exceptions and validates custom policies, maintaining AppTrana's zero-false-positive commitment. Vulnerability remediation reports are delivered within SLA-defined timelines.

01 Autonomous vulnerability remediation for security compliance

Waiting for code-level fixes can leave vulnerabilities exposed for weeks or months. AppTrana provides a single view of vulnerabilities identified and their protection status at the edge. A majority of vulnerabilities are autonomously patched through security policies. For a small minority of vulnerabilities (<5%), that require custom policies, the managed security team creates and validates application-specific virtual patches and ensures zero false positives within the SLA.

This process reduces the vulnerability exposure window from weeks to near real time. Development teams can continue fixing vulnerabilities at the source through their normal release cycles while applications remain protected. SwyftComply AI provides vulnerability remediation evidence to support applicable compensating-control requirements, including those relevant to IRDAI compliance. AppTrana also supports CI/CD integration to help Bandhan Life incorporate application security into development workflows.

THE REMEDIATION LOOP

01 Continuous scanning
Automated scans and AI-Pentesting across applications

→

02 Critical vulnerability found
Validated against live attack telemetry

→

03 Virtual patch at WAF
SwyftComply deploys the virtual patches autonomously at the edge, with expert validation

→

04 Expert-verified, audit-ready report
Vulnerability remediation reports, delivered within SLA timelines

© 2026 Indusface Pvt. Ltd. All rights reserved.

02 An extension of Bandhan Life's security team

AppTrana's 24×7 managed security services extend Bandhan Life's security capabilities across its application environment. The managed team monitors applications, investigates threats, creates and fine-tunes security policies, and responds to incidents. During the infrastructure transition, some applications required specific routing configurations. The managed security team handled these changes at the application level, ensuring protection remained seamless throughout the transition.

The managed security team works closely with Bandhan Life's team to maintain its policy of closing critical and high-severity vulnerabilities within defined internal SLAs. This combination of autonomous protection and dedicated security expertise enables Bandhan Life to operate applications in full block mode while maintaining protection without disrupting legitimate traffic.

03 Behavioral DDoS and bot protection through infrastructure changes

Bandhan Life migrated its CDNs and ran rebranded applications alongside legacy ones, repeatedly shifting traffic patterns and changing the baselines used by rate-limiting policies. AppTrana's Behavioral DDoS and bot protection engines learn per-application traffic baselines and identify anomalies associated with volumetric and application-layer attacks. The Indusface managed security team reviewed and retuned policies as traffic patterns changed through the transition.

Since then, AppTrana has blocked millions of DDoS and bot attempts, with no DDoS-attributable downtime and no incidents escalated to Bandhan Life's security team. This allows the team to maintain protection without having to manage every security event itself.

04 Executive-ready insight, built for the boardroom

Ahead of each quarterly board meeting, Indusface compiles Bandhan Life's leading attack sources, attack categories, and most-targeted applications, benchmarking the findings against the wider insurance industry. A dedicated security engineer turns this data into executive-ready insights, giving Bandhan Life's CISO a current, industry-benchmarked view of the organization's security posture and a clearer basis for board-level discussions.

Bandhan Life's experience with Indusface shows how autonomous application protection, managed security, and expert oversight can help security teams keep pace with a changing application environment. By protecting validated vulnerabilities while developers work on permanent fixes, adapting security policies through infrastructure changes, and providing audit-ready remediation evidence, AppTrana helps Bandhan Life reduce exposure windows and stay aligned with its security and compliance requirements.

ABOUT INDUSFACE

Indusface is a leader in autonomous application security, protecting thousands of business-critical web, API, and AI applications for global enterprises across 45+ countries. As AI-driven exploitation outpaces traditional patching cycles, its flagship AppTrana platform continuously discovers vulnerabilities and autonomously mitigates exploitable risks through AI-powered virtual patching. With SLA-backed, zero-false-positive protection and 24/7 expert oversight, AppTrana defends organizations against API abuse, DDoS attacks, malicious bots, AI threats, and zero-day exploits, keeping them protected long before code fixes ship.

Backed by leading institutional investors, Indusface maintains a 4.9 rating on Gartner Peer Insights and is recognized in research by Gartner, Forrester, and IDC. Its globally distributed cloud spans North America, Europe, the Middle East, and Asia-Pacific to deliver low-latency protection and regional data residency at scale, while maintaining ISO 27001, SOC 2, PCI DSS, and GDPR-aligned compliance.

Learn more at indusface.com.

© 2026 Indusface Pvt. Ltd. All rights reserved.