INDUSFACE™

CUSTOMER SUCCESS STORY

Niva Bupa

HEALTH INSURANCE · INDIA ENTERPRISE

AppTrana WAAP | Managed Service

> "AppTrana's autonomous remediation protects vulnerabilities at the WAF edge, before they turn into a compliance problem. This has given our developers much-needed time to fight threats that move faster than we can respond to manually. Indusface has also served as our extended security team, providing round-the-clock monitoring and support. Together, this gives us confidence that our applications stay protected without slowing our own team down."

JP Mohapatra
VP & Chief IT Security Officer, Niva Bupa

niva Bupa Health Insurance

- 20 million+ customers
- India's 3rd largest standalone health insurer by gross written premium

PRODUCTS USED

- ✓ AppTrana WAAP
- ✓ SwyftComply — autonomous virtual patching
- ✓ Behavioral DDoS & Bot Mitigation
- ✓ 24×7 Managed Security Services

How Niva Bupa stays protected with Autonomous Virtual Patching & 24x7 Managed Services

AI-powered scanners now discover vulnerabilities faster than organizations can remediate them, making autonomous protection more important than ever. Niva Bupa Health Insurance uses Indusface AppTrana to close that gap through autonomous virtual patching and a fully managed 24×7 security service.

RESULTS AT A GLANCE

- ✓ Sustained uptime through peak business season
- ✓ Rapid vulnerability remediation aligned to compliance timelines
- ✓ Compliance-ready vulnerability remediation reports
- ✓ No false positives disrupting legitimate traffic, even at peak
- ✓ Millions of attacks blocked every month
- ✓ 24×7 managed security team

ABOUT NIVA BUPA

Niva Bupa Health Insurance serves more than 20 million customers across India and runs its application security through Indusface's AppTrana platform. AppTrana protects Niva Bupa's entire public-facing footprint, from customer portals to partner integrations to internal servicing platforms.

Working closely with Niva Bupa's team, Indusface's fully managed AppTrana platform runs continuous monitoring, DDoS and bot protection, and autonomous virtual patching. Indusface also built custom traffic reporting for Niva Bupa's seasonal business peaks.

KEY SECURITY CHALLENGES

Enforcing protection in real time, without the operational overhead

Three problems had to be solved at once: patch validated vulnerabilities within regulatory timelines, enforce security policies at the edge without dropping real customers, and do both without adding any operational overhead.

01 Vulnerabilities and zero-days outpacing remediation

An AI-scan, VAPT cycle, or red-teaming project now discovers vulnerabilities faster than most organizations can remediate them. Production fixes are often delayed by release cycles, legacy code, uptime requirements, or limited developer capacity. A validated critical vulnerability stays exploitable for every day it waits on a release window, Niva Bupa wanted to ensure edge protection before developers could fix on code.

02 Meeting application security compliance

Cyber Security Guidelines for the insurance industry in India require continuous application security monitoring, timely remediation, and closure of high-risk vulnerabilities and audit findings within defined timelines. Niva Bupa needed to deliver 24×7 protection, quickly patch validated vulnerabilities, and maintain audit-ready compliance across its applications without increasing the operational overhead.

03 Enforcing security policies without disrupting real users

Tightening WAAP policies always carries the risk of catching legitimate traffic along with attacks. Without a reliable way to distinguish the two before a rule goes live, teams either delay enforcement or spend cycles manually tuning policies.

THE SOLUTION

How AppTrana addressed these challenges

The Indusface AI Platform pairs autonomous protection with a human-in-the-loop review, so every rule is verified before it blocks and a named security engineer owns the outcome.

01 Autonomous, compliance-aligned vulnerability remediation

Waiting for code-level fixes or manually creating WAF rules can leave exploitable vulnerabilities exposed for weeks. AppTrana correlates vulnerability findings with live attack telemetry to prioritize the most critical vulnerabilities. Virtual patches are deployed autonomously at the edge. Whether vulnerabilities are identified through Indusface's AI-assisted scanning or Niva Bupa's own VA/PT and red-teaming exercises. AppTrana provides vulnerability remediation reports within SLA-defined timelines. Development teams continue code-level remediation on their normal release schedules while applications remain protected. This also enables Niva Bupa to demonstrate remediation progress well within compliance requirements.

THE REMEDIATION LOOP

01	→	02	→	03	→	04
AI scan		Critical vulnerability found		Virtual patch at WAF		Expert-verified audit-ready report

02 An extension of Niva Bupa's security team

To help Niva Bupa meet the continuous monitoring and remediation requirements without expanding its security team, AppTrana combines a dedicated security engineer, a 24×7 managed security service, and autonomous vulnerability remediation into a single operational model. The managed team continuously monitors applications, investigates threats, optimizes security policies, and responds to incidents, while Executive AI Insights provide leadership with clear visibility into attack trends and security posture. When validated vulnerabilities are identified, AppTrana translates them into application-specific virtual patches using natural-language policy generation and expert validation before deployment, enabling rapid, audit-ready protection without disrupting production.

03 Behavioral DDoS insights

Traffic spikes can look like DDoS attacks, making it difficult to separate genuine users from malicious traffic. AppTrana's Behavioral DDoS continuously learns Niva Bupa's normal traffic patterns and identifies anomalies across both volumetric and application-layer attacks. Security experts validate and fine-tune policies while custom traffic reports provide visibility into which applications see the most traffic and how requests with and without cookies behave. This helps tell a genuine surge from an attack.

04 Managed WAF deployment without false-positive disruption

Moving a WAF into block mode is often delayed by concerns around false positives and business disruption. AppTrana's False Positive Monitoring watches traffic continuously to distinguish genuine attacks from legitimate user behavior before a rule is enforced. Exceptions are validated by an Indusface security expert before deployment. As a result, Niva Bupa runs its applications securely with no false positives disrupting genuine customer traffic.

Modern application security is no longer defined by how quickly vulnerabilities are discovered. It's defined by how quickly they are remediated. Niva Bupa's partnership with AppTrana shows how autonomous vulnerability remediation, backed by expert oversight, helps organizations reduce risk and stay compliant.

ABOUT INDUSFACE

Indusface secures the web, API, and AI applications of thousands of organizations across 95 countries. Backed by leading institutional investors, Indusface is recognized by Gartner, Forrester, and IDC for its innovation in application security and meets globally accepted security and compliance standards, including ISO 27001, SOC 2, PCI DSS, and GDPR. Its globally distributed cloud infrastructure spans Asia, the Middle East, Europe, and North America, enabling low-latency protection and regional data residency for enterprises worldwide.

AppTrana is Indusface's autonomous enterprise application security platform that continuously discovers vulnerabilities, autonomously remediates exploitable risks through virtual patching, and protects applications against DDoS, bot, API, AI, and zero-day attacks. Combining AI-powered intelligence, expert governance, and SLA-backed protection, AppTrana helps organizations reduce the time from vulnerability discovery to protection while delivering compliance-ready reports with zero false positives.