How a Leading Brokerage Met SEBI Compliance with ~40 Clean, Zero Vulnerability Reports

SOLUTION HIGHLIGHT

6.5 million attacks blocked
130+ virtual patches deployed in 2025
100% uptime for 4 consecutive years

All while securing the **live trading platform**, onboarding **custom ports and socket-based traffic**, and meeting **stringent SEBI cybersecurity requirements** without interrupting a single trading session.

This is the story of how a leading Indian stock brokerage firm re-architected its application security without slowing markets, disrupting brokers, or compromising compliance.

ABOUT THE CUSTOMER

The customer is a leading Indian stockbroking and financial services organization operating at scale across equity trading, derivatives, and investment products. The firm supports a growing customer base of over **7.5 lakh investors**, with over **80,000 daily active users**, and processes high volumes of **time-sensitive trading transactions** every day.

For them, even brief disruptions, incorrect trade handling, or compliance gaps can have immediate business and regulatory impact.

THE CHALLENGE: WHEN TRADITIONAL WAFS STOP WORKING

The organization was already using **Akamai WAF** across parts of its banking ecosystem. However, its **stock brokerage and trading platforms had fundamentally different requirements.**

These platforms supported **live trading**, including an **EXE-based broker application**, customer-facing web and mobile apps, and backend systems communicating over **custom ports and socket-based connections.** Latency sensitivity, fixed market hours, and zero tolerance for disruption meant traditional web-only security controls were insufficient.

A HIGHLY COMPLEX, HYBRID TRADING ENVIRONMENT

The organization's trading ecosystem included:

- An **EXE-based desktop trading application** used by brokers
- **Customer-facing web and mobile trading applications**
- Extensive **API-driven integrations** with internal financial systems
- **Custom port-based and socket-level communication** supporting backend and trading workflows

This hybrid architecture significantly increased both **onboarding complexity and operational risk.**

WHY ONBOARDING WAS ESPECIALLY CHALLENGING

Sanity Checks Without a Safety Net

The presence of custom ports, socket connections, and tightly coupled backend systems made traffic validation extremely difficult. Any misconfiguration could directly impact **order execution, customer experience, or regulatory compliance.**

There was no room for trial or error.

Zero Downtime Was Non-Negotiable

Trading platforms operate on strict market schedules. Even brief interruptions could lead to financial loss, reputational damage, and regulatory scrutiny.

The organization required **WAF onboarding with zero downtime**, ensuring uninterrupted trading during deployment, testing, and go-live.

A Hard Limitation with the Existing WAF

The existing WAF **could not support custom ports and socket-based communication**, making it unsuitable for securing the stock brokerage and trading environment. This limitation triggered the search for an alternative.

More Than Security: Adhering To SEBI Compliance Regulations

At the same time, the organization had to meet multiple SEBI cybersecurity mandates, including:

- Critical vulnerabilities remediated within **24 hours**
- High-severity vulnerabilities fixed within **one week**
- VAPT report submission within **one month**, with findings closed within **three months**
- Revalidation of fixes within **five months**
- Use of **virtual patching** to mitigate risk until permanent fixes are applied, with audit-ready proof

Meeting these timelines consistently across a complex digital ecosystem was essential to maintaining regulatory standing.

THE SOLUTION: APPTRANA WAAP

The organization partnered with **Indusface AppTrana WAAP**, an AI-powered, fully managed application protection platform, to secure its trading and investment platforms.

The engagement focused on one core principle: **secure live trading systems without disrupting them.**

Zero-Downtime Onboarding of the Core Trading Platform

Indusface onboarded the customer's core trading application with **zero downtime**, led by its dedicated SOC team.

The application was first deployed in **monitoring mode** to observe real production traffic and establish accurate baselines. Protection was moved to **blocking mode only after thorough validation**, ensuring **zero false positives.** The entire activity was done by Indusface services team in consultation with the customer.

This process involved close coordination between Indusface and the customer's teams to validate traffic flows across **web, API, and hybrid components**, including **custom ports and socket-based communication**, all while trading remained uninterrupted.

Phased Expansion Across Applications

After successfully securing the core trading platform, coverage was expanded through a **phased rollout.**

Applications were onboarded incrementally, following a structured approach that included planned change of windows, comprehensive testing, and joint validation before moving to production. Indusface now protects around 60 applications.

Full-Spectrum Protection Across Application Types

AppTrana delivered unified protection across:

- Web applications
- APIs
- Hybrid applications

This ensured consistent security for **customer-facing, broker-facing, and backend systems.**

SEBI-Aligned Vulnerability Management and Virtual Patching

To meet regulatory requirements, AppTrana enabled:

- Continuous automated scanning and expert-led penetration testing
- Virtual patching to immediately mitigate exploitable risks
- Continuous monitoring and detailed logging for audit readiness
- Clear remediation guidance for development teams

This reduced exposure even when permanent fixes could not be deployed immediately.

Further with SwyftComply, they received clean, zero-vulnerability reports within 72 hours that helped them stay compliant with application security audit requirements.

AI-Powered, Fully Managed Security with Zero False Positives

Given the sensitivity of trading workflows, AppTrana maintained **zero tolerance for false positives.** AI-driven detection, combined with **24×7 SOC oversight,** ensured:

- Protection against volumetric and application-layer DDoS attacks
- Bot mitigation without impacting legitimate users
- API security enforced through positive security models
- Continuous tuning based on live traffic patterns

RESULTS

What started with a few critical applications expanded steadily over time. Today, **approximately 60 financial services applications** are protected using AppTrana. In the last one year, AppTrana WAAP has delivered:

- 6.5+ million attacks blocked across websites, APIs, and hybrid applications
- 130+ virtual patches created
- ~40 clean vulnerability reports delivered for SEBI compliance
- 100% uptime maintained for four consecutive years
- US$ 90K+ savings in operational costs and US$ 7 million+ in risk mitigation costs

This case study isn't about replacing a WAF. It's about proving that **high-frequency, SEBI-regulated trading platforms can be secured without downtime, without false positives, and without compromising compliance.** And that's what makes the result worth paying attention to.