How a Leading BFSI Enterprise Migrated 187 Applications to AppTrana with Zero Downtime

OVERVIEW

A large banking, financial services, and insurance enterprise migrated its application security stack from Radware to Indusface AppTrana in early 2024, bringing 187 applications under an autonomous application security platform. The organization had outgrown what a self-managed WAF could efficiently handle and needed a platform that could scale with the business without adding headcount.

- **104.22 million** application-layer attacks blocked last year
- **$170,000+** in annual operational security savings
- **506 vulnerabilities** protected through virtual patching
- **187** applications fully migrated to the autonomous Cloud WAAP

ABOUT THE CUSTOMER

The customer is a large Indian financial and investment enterprise offering consumer loans, wealth management, commercial finance, investment banking, private equity, and related services.

With 187 internet-facing applications spanning customer portals, transaction systems, partner integrations, and APIs, consistent active protection across the infrastructure was a business-critical requirement.

Before migrating to AppTrana, the environment was protected by Radware WAF.

CHALLENGES WITH RADWARE

1. False positive resolution fell entirely on the customer

   When Radware's WAF blocked a legitimate request, fixing it was a manual process: identify the false positive, create a portal exception, and contact support if needed. That cycle, repeated across hundreds of applications, wasn't sustainable without dedicated WAF analysts. Over time, security policies shifted toward log-only mode to protect business availability. Applications were technically behind a WAF, but not actively blocking anything.

2. Application-specific virtual patching was an enterprise add-on

Radware's auto-policy generation module came with a documented caveat: auto-generated rules were prone to false positives and needed manual validation before deployment. Patches written for vulnerabilities specific to customer applications required a separate managed services engagement. For a BFSI organization operating under continuous regulatory scrutiny, vulnerabilities could stay exposed for weeks or months while development remediation cycles run in the background, with no reliable way to close that window at the WAF layer.

3. DDoS protection introduced cost uncertainty during attacks

Radware's DDoS protection operated on a tiered Gbps model, with unlimited protection sold separately. With 60% of applications under active DDoS targeting, this wasn't a theoretical concern. Per-incident billing during attack peaks was a direct hit to budget planning, and costs tended to spike at exactly the moments when the security team had the least capacity to deal with them.

4. Managed SOC required a separate contract

Radware's managed SOC coverage sat outside its standard WAF plans. Continuous monitoring, alert management, and rule tuning all required a separate enterprise-tier engagement. For a team managing 187 applications without a large dedicated security function, this meant day-to-day WAF operations stayed in-house, and the workload grew with every application added

5. No built-in vulnerability scanning

Radware had no native DAST capability. Identifying application vulnerabilities required a separate third-party engagement, translating findings into a format the WAF team could act on, then requesting application-specific patches through managed services. Each step added time and coordination overhead. Across 187 applications, the result was a slow, fragmented vulnerability response pipeline.

6. WAF, bot management, and DDoS ran as separate products

Radware's WAF, Bot Manager, and DDoS protection were distinct modules with separate configuration interfaces and alert streams. Correlating a WAF alert with bot activity meant reconciling data across different dashboards. That friction compounded quickly at scale.

HOW APPTRANA ADDRESSES THE CHALLENGES

1. A managed migration to Cloud WAAP

The migration started in January 2024. Indusface's team worked directly with the customer's engineering and security teams to onboard all 187 applications. Traffic behavior was analyzed per application, security baselines were established, and DNS changes were coordinated to route traffic through AppTrana. There was no disruption to application availability and no impact on end users.

2. Zero false positives, guaranteed in writing

AppTrana's AI tunes protections per application before any security policy is enforced, building off each application's actual traffic patterns rather than generic signatures. Thresholds adjust continuously in real time, and when an edge case needs a human call, the 24x7 managed services team steps in to validate and fine-tune. All 187 applications run in active blocking mode from day one, with zero false positives guaranteed in writing.

3. Autonomous virtual patching at scale

   AppTrana's integrated DAST scanner continuously identifies vulnerabilities across protected applications and feeds findings directly into the patching pipeline, without requiring a manual handoff.
   Last year, the platform protected against 506 vulnerabilities: 341 through core WAF rules and 165 through application-specific custom security policies. Custom security policies are deployed within hours of discovery, and a clean, zero-vulnerability report is ready within 72 hours, helping the team stay compliant. Previously, closing the same exposure window could take months

4. Unmetered DDoS with no per-incident billing

   AppTrana includes unmetered DDoS protection across all plans. With 114 applications under active DDoS targeting last year, the shift to predictable, unlimited coverage saved the customer $23,936 in annual monitoring costs.

5. Managed SOC is included across all plans

   Indusface's security team takes over continuous monitoring, alert review, and security policy tuning across all protected applications. All 187 applications moved into active blocking mode without the internal exception management overhead the team had been carrying. By transitioning day-to-day monitoring and security operations, the customer saved $119,680 last year.

6. Behavioral detection across 187 applications

   AppTrana's behavioral analysis engine continuously models traffic patterns across all protected applications, separating legitimate financial service traffic from attack traffic without manual rule intervention. Last year, the platform blocked 104.22 million malicious requests: 35.06 million DDoS requests across 114 sites, 15.6 million bot-driven attacks across 116 sites, and 41.16 million blocks from custom security policies deployed across 151 sites

7. One platform, one view

   WAF, bot management, DDoS scrubbing, API security, and DAST scanning are natively integrated under a single managed service and portal. The security team has full threat visibility across the entire estate in one place, with no context-switching between product modules.

KEY RESULTS

- **187** applications migrated with zero downtime
- **104.22 million** malicious requests blocked in 2025
- **35.06 million** DDoS attack requests mitigated across 114 sites
- **15.6 million** bot-driven attacks prevented across 116 sites
- **506** vulnerabilities protected through virtual patching (341 core rules, 165 custom security policies)
- **$170,000+ i**n annual operational security savings

The savings came from three areas: eliminating the manual work of maintaining block mode across 187 applications, reducing developer hours spent on code-level remediation, and avoiding per-incident DDoS monitoring costs.
With 15.6 million exploit attempts logged last year, the cost of a single successful breach in BFSI puts the platform investment in a very different context.

LOOKING AHEAD

The organization now has an application security architecture that fits the scale and risk profile of a large BFSI enterprise. New applications are onboarded quickly, vulnerabilities are remediated within hours of discovery, compliance reports are ready within 72 hours, and the security team is no longer the operational bottleneck.

In the BFSI industry, a single breach carries lasting financial and reputational consequences, and that foundation matters well beyond what the numbers show.

Migrating from Radware? Talk to our team.