How A Global Enterprise Migrated 42 Apps With Zero Downtime

OVERVIEW

A publicly listed multinational enterprise, one of Asia's largest chemical manufacturing companies, migrated its entire application security stack from F5 WAF to Indusface AppTrana, completing the move across 42 production applications in under 48 hours with zero downtime.

While the trigger was an F5 renewal deadline, the reason was deeper. Their expanding digital ecosystem had outgrown what F5's self-managed model could sustainably protect, and the operational cost of maintaining it was rapidly increasing.

- **34.1 million application-layer attacks** blocked in 2025
- **$40K+** in annual operational security savings
- **<48 hours** for full managed migration from F5, zero downtime

ABOUT THE CUSTOMER

The customer is a publicly listed multinational enterprise operating across the chemicals and agricultural products industry, with a combined revenue exceeding $2 billion and operations spanning North America, Europe, Asia, and Africa.

Its application landscape spans corporate websites, customer portals, partner integrations, and backend APIs that power supply chain and operational systems across the different business units .

Prior to the AppTrana migration, the environment was protected by F5 WAF.

CHALLENGES WITH F5

1. Managed SOC is a Separate Subscription

   F5's managed SOC is not bundled into any WAF plan. It is available through F5 Distributed Cloud Services, a separate product with its own contract and pricing, typically positioned for enterprise budgets. Teams on typical F5 WAF plans handle all rule tuning, alert review, and traffic analysis in-house.

   As the application portfolio grew, so did the manual workload, without a proportional increase in headcount or tooling. The team needed a platform where managed protection was the default, not a separate procurement exercise.

2. Manual False Positive Tuning

F5 Advanced WAF includes learning-based tools to help identify false positives, but reviewing suggestions, validating them, and adjusting policies is entirely the security team's responsibility. There is no managed layer handling this on your behalf.

For a team already managing 40+ applications and around 450 APIs, this became a significant ongoing time commitment on top of an already stretched workload. Without dedicated WAF expertise to sustain that review cycle, policies drifted toward log-only mode to avoid disrupting legitimate traffic. Applications remained technically behind a WAF, but without active blocking in place.

3. Self-Managed Virtual Patching

When vulnerabilities were discovered, code-level fixes were tied to development release cycles, which meant vulnerabilities often took months to be addressed. While F5 provides regularly updated attack signatures, custom virtual patches for newly discovered vulnerabilities typically require teams to create and deploy WAF rules themselves. With no managed patching capability, applications remained exposed during remediation windows. The security team had no reliable way to close that gap quickly.

4. Scaling Multiplied Manual Work

With F5, each additional application required new policies, monitoring, and tuning, increasing operational overhead for the security team. There was no standardized onboarding, no automated baseline, just more manual effort. As the organization expanded its digital services, the security team's operational load scaled linearly with it.

5. Hard Renewal Date

The F5 contract renewal was weeks away. Any replacement had to onboard 40+ production applications rapidly, replicate existing protections, and go live without service interruption. There was no buffer for extended timelines or failed cutovers.

HOW APPTRANA SOLVED IT

1. Fully Managed Migration Before Renewal Deadline

Before committing a full migration, the team conducted a structured evaluation of platform capabilities against their security and operational requirements. AppTrana met the brief, and a proof of concept followed in 2024 to validate integration speed and protection accuracy across a subset of applications. Following sign-off, Indusface's team worked alongside the customer's engineering team to migrate all 42 production applications, analyzing traffic behavior, configuring security policies, and implementing DNS changes to route traffic through AppTrana. The entire migration completed before the F5 renewal date, with **100% availability maintained** throughout.

2. Managed SOC With Zero False Positive Guarantee

Unlike F5, where managed services require a separate contract, AppTrana's managed SOC is included across all plans. Indusface's security team took over continuous alert monitoring, rule refinement, and **guaranteeing zero false positives,** enabling the customer to run all applications seamlessly without disrupting legitimate traffic. Internal security engineers were freed from day-to-day WAF operations.

3. Autonomous Virtual Patching

   In addition to the core security rules, AppTrana's managed SOC added over 35 custom WAF security policies last year to block active exploit attempts against discovered vulnerabilities, providing immediate protection while development timelines ran their course. In total, 345 vulnerabilities were protected through virtual patching, with security policy patches deployed **within 72 hours** of discovery.

4. Hidden APIs Discovered and Protected

   AppTrana's automated API discovery identified approximately **450 API endpoints,** including shadow and zombie APIs that previously had no security coverage. These were brought under active protection. API discovery capabilities in F5 are typically available through Advanced WAF. On AppTrana, it is standard across plans.

5. Comprehensive Threat Detection

   AppTrana's behavioral detection continuously analyzed traffic patterns across all protected applications, automatically blocking malicious requests without manual rule intervention. Last year, the platform mitigated **34.1 million malicious requests**, including **9.38 million DDoS requests** and **10.67 million bot-driven attacks.**

KEY RESULTS

- **42** applications successfully migrated from F5
- **$40K+** in annual operational security savings
- **345 vulnerabilities** protected through virtual patching
- **~450 API endpoints** (including shadow and zombie APIs) discovered and protected
- **34.1 million** attacks blocked across applications
- **9.38 million** DDoS attack requests mitigated
- **10.67 million** bot-driven attacks prevented

The cost savings reflect the reduction in internal engineering hours previously consumed by F5 policy tuning, false positive management, and custom rule authoring; work now handled by AppTrana's managed SOC.

LOOKING AHEAD

The organization now operates on a WAAP architecture built for scale, where new applications can be onboarded quickly, APIs are continuously discovered and monitored, and the security team is no longer the operational bottleneck.

The shift from F5 was not just a platform change. It was a move from a self-managed model that demanded constant internal effort to a fully managed model where protection is continuous, accurate, and operationally light. As the organization's digital ecosystem grows, that foundation scales with it.

Looking for a **F5 alternative?** Talk to our team.