# How a Global Payments Provider Secures 40 Million Daily

## ABOUT THE CUSTOMER

The customer is among the top five global payment service providers, operating in more than 40 countries and serving over 1.5 million businesses, including banks, financial institutions, and large enterprises. The platform processes over **40 million payment transactions daily** in a regulated financial services environment. Any disruption, latency increase, or security incident directly impacts transaction success, partner confidence, and compliance obligations.

## CHALLENGES

As the organization adopted a cloud-first application architecture, modernizing security required addressing certain key challenges while maintaining bank integrations, transaction continuity, and regulatory controls.

- **Limited Scalability of On-Prem Security Infrastructure:**
  The existing security stack was based on an on-premises F5 WAF and load balancer architecture. While reliable, scaling required manual provisioning and careful traffic planning. This resulted in limited elasticity during traffic spikes, increased operational complexity and higher risk during peak payment periods. The security layer was not designed for dynamic, cloud-scale transaction growth.

- **Strict Static IP Requirements from Banking Partners**
  The platform operated within banking networks that relied on static IP whitelisting as a core trust mechanism.
  Key constraints included:
  - Pre-approved IP ranges enforced by banking partners
  - Change management and re-approval for any IP modification
  - High risk of transaction disruption if IP continuity was broken

  Most cloud-based security solutions relied on dynamic or shared IP models, making them unsuitable for bank-integrated payment traffic.

- **Usage of Non-HTTP Payment Protocols**
  The payment platform used custom TCP ports for host-to-host banking integrations and backend payment processing. These protocols were deeply integrated into existing systems, could not be modified without significant re-engineering and weren't supported by many cloud WAF and CDN platforms. This limited the organization's ability to extend security controls beyond standard web traffic.

- **Strict Latency and Availability Requirements**
  Payment processing required consistently low latency and high availability. Even small delays could impact transaction success rates and downstream settlement processes.
  The organization needed security controls that would not introduce performance variability into live payment flows.

- **Fragmented Vulnerability Management**

  Beyond perimeter protection, the organization faced challenges with fragmented vulnerability management across applications.

  They wanted to bring together continuous vulnerability discovery, immediate risk mitigation through virtual patching and have faster remediation cycles and audit readiness.

  Most vendors focused primarily on perimeter protection through WAF capabilities, leaving vulnerability discovery and risk remediation to separate tools or manual processes. This created gaps in visibility, slower remediation cycles, and higher operational overhead for security teams.

- **24×7 Monitoring and Rapid Incident Response**

  As the engine behind millions of businesses worldwide, this payment provider ensures that shop owners and entrepreneurs can trade with confidence. To protect these daily livelihoods, they needed security operations focused on:

  - **24/7 Vigilance**: Monitoring live traffic around the clock so no business is left vulnerable, regardless of the time zone.
  - **Instant Protection**: Stopping active threats in real-time to keep global checkout lines moving without interruption.
  - **Seamless Customer Experience**: Expertly tuning the system so legitimate shoppers never face friction while bad actors are kept out.
  - **Verified Trust**: Maintaining clear, automated audit trails that simplify regulatory compliance and provide transparency.

  Whether operating in the cloud or across a hybrid environment, the goal remained the same: uninterrupted, secure commerce for everyone.

## Solution: AppTrana WAAP

The organization chose Indusface AppTrana, a cloud-native application security platform built for high-scale, regulated businesses, enabling scalability while preserving existing infrastructure and performance requirements.

- **Seamless Cloud Migration with Static IP Support**

  AppTrana enabled the organization to move application security to the cloud while retaining dedicated static IP addresses.

  This preserved existing IP whitelisting with banking partners, ensured uninterrupted transaction flows, and removed the risk of integration failures caused by IP changes.

- **Support for Custom TCP Ports**

  AppTrana provided full support for custom TCP ports, allowing the organization to protect existing payment workflows without modifying application architecture.

  This removed a major barrier to cloud adoption and ensured backend integrations continued to operate as designed.

- **Zero-Disruption Onboarding and Performance Integrity**

  The WAF was deployed in blocking mode from Day 1 to protect against OWASP using close to 400 pre-validated security policies to protect live payment traffic without impacting existing transaction flows.

  Additional custom rules were progressively enabled as traffic patterns were observed and validated, allowing protection to be strengthened in a controlled manner without introducing false positives.

  Further, Indusface's 24×7 managed SOC continuously monitors live traffic and fine-tunes policies as required, ensuring strong protection while maintaining low latency, even during peak transaction volumes.

- **Unified Security and Vulnerability Management**

  AppTrana brought application protection and vulnerability management into a single managed platform, enabling:

  - Continuous automated scanning and expert-led testing
  - Autonomous virtual patching to reduce exposure to exploitable risks
  - Clear remediation guidance for engineering teams
  - Detailed logging and reporting to support audits

  This reduced operational overhead while strengthening the organization's overall security posture.

## RESULTS

The transformation delivered measurable impact across security, performance, and operations. Today, the organization operates its payment platforms with cloud-scale resilience and bank-grade controls, without compromising performance or partner integrations.

Just in the last one year, AppTrana WAAP has delivered:

- **18.54 million** attacks blocked across 23 web apps, APIs, and hybrid applications.
- **2.43 million API attacks mitigated**, securing high-volume payment and partner-facing APIs from abuse and exploitation
- **~US$80,000 in operational cost savings** and **US$ 5.83 million in risk mitigation value**, driven by reduced exposure and faster threat response
- **100% uptime** maintained since migration, including during peak transaction periods