INDUSFACE™

CASE STUDY

Web Application Security at Scale for a Global Pharma Leader

ABOUT THE CUSTOMER

The customer is a $10 billion+ global pharmaceutical company with operations in over 80 countries. It is known for developing, manufacturing, and marketing a broad portfolio of pharmaceutical products worldwide.

To support its business operations, the company relies on a wide range of digital applications. These include systems for product distribution, regulatory workflows, employee services, and partner collaboration.

As this digital footprint expanded, securing these applications became essential to protect sensitive data, maintain business continuity, and uphold trust with healthcare partners and regulators.

The company has been **a valued Indusface customer for over a decade**, relying on its expertise to adapt to changing security needs over the years.

CHALLENGES

Initial Priority: Secure Document Exchange

The company's journey toward application security began with the need to secure a critical application used for exchanging confidential documents with global stakeholders. This platform supported large file transfers, often tied to regulatory and legal workflows. It was essential to maintain high performance while ensuring that the data always remained secure.

Growing Attack Surface with Limited Visibility

As the company evaluated its attack surface, it discovered that several applications, such as timesheet portals, survey tools, trade documentation systems, and employee stock platforms, were accessible over the internet with little to no centralized protection. There was no consolidated view into whether these assets were being targeted or how they were being accessed.

Performance without Compromise

Many applications were bandwidth-intensive or tightly integrated with business systems. Any security solution needed to deliver strong protection without impacting application speed, usability, or uptime.

Vulnerability Management Delays

The organization faced delays in discovering vulnerabilities and rolling out patches across environments. This created a window of risk, especially for legacy or less frequently updated apps.

Business Risk in a Regulated Industry

The data at risk includes intellectual property, formulations, compliance records, and workflows. A successful attack could result in regulatory penalties, production disruptions, or a loss of competitive advantage.

HOW APPTRANA HELPED

The company partnered with Indusface and adopted the AppTrana Application Security Platform to establish a unified, intelligent, and fully managed security across its application landscape.

From Siloed Protection to Centralized Coverage

The journey began with securing a high-risk file-sharing application in a UAT environment to validate AppTrana's compatibility and performance under heavy data loads. Once that was successful, the security team used insights from the initial assessment to identify and map other exposed applications across departments.

These internal portals, including HR tools, trade documentation systems, and employee platforms, were then systematically onboarded into the AppTrana platform, ensuring they were no longer overlooked or operating without security controls. What started as a narrow deployment became a full-scale rollout to unify protection across the company's entire web-facing surface.

Visibility Where There Was None

With AppTrana deployed, the company gained real-time visibility into attacks and anomalous behavior across all applications. The platform's AI-powered capabilities continuously monitored for patterns that indicated abuse, ensuring rapid identification of threats across the entire application stack.

Security Without Disruption

AppTrana's phased deployment ensured there was no disruption to day-to-day operations. Applications that handled large data volumes or served critical business functions continued to operate at full performance, protected by AppTrana at the edge, without code changes or downtime.

Blocking Bot-Led Targeted Attacks

Once protection was live, AppTrana's AI-powered engine began detecting patterns of non-human traffic across several applications. These included bots mimicking browser user-agents like Mozilla or using command-line tools such as python to probe for open vulnerabilities.

These bots would first scan for weaknesses and then launch targeted attacks based on what they found, a sequence that had previously gone undetected due to a lack of centralized visibility.

AppTrana's intelligent bot management blocked these attacks at multiple layers:

- Fingerprinting and behavioral analysis identified suspicious automation such as scripted cURL calls, headless browser scans, and rapid API probes
- AppTrana's protection ensured that requests from known scanners and probing tools never reached business logic
- Legitimate users were unaffected, as the system continuously adapted policies to avoid false positives

This stopped attack campaigns before exploitation attempts could begin, significantly reducing overall risk and eliminating the need for manual intervention by the customer's team.

Protecting Vulnerabilities Before They Could Be Exploited

To stay ahead of security risks, a continuous vulnerability discovery model was implemented through AppTrana's expert-led Penetration Testing-as-a-Service (PTaaS). These regular assessments helped uncover new or open vulnerabilities across applications, including those inherited from third-party components or legacy code.

Importantly, AppTrana provided SLA-backed autonomous remediation for all discovered vulnerabilities. This meant that virtual patches were deployed instantly on the WAAP, preventing the exploitation of open vulnerabilities before development teams patched on code.

This combination of proactive detection and reduced MTTR without slowing internal release cycles.

- By ensuring that no known vulnerabilities remained exposed in production, the company was also able to support its compliance goals more effectively, particularly around data protection, zero exposure, and audit readiness, all without adding operational burden.

Staying Available During High-Volume Attacks

The company's most business-critical site, responsible for order management of generics, became a frequent target of DDoS attacks aimed at disrupting access for legitimate users.

AppTrana's AI-powered mitigation engine blocked 99% of these attacks automatically, identifying and filtering malicious traffic at the edge in real time.

These protections were reinforced by AppTrana's 24/7 managed security team, which actively monitored attack patterns, fine-tuned policies, and ensured that any large-scale or evolving threats were contained without affecting application performance.

To further strengthen reliability, AppTrana offered a guaranteed uptime of 100%, backed by a built-in failover architecture, which helped the company maintain continuous service availability even during active attacks, without requiring internal firefighting or infrastructure changes.

RESULTS:

With AppTrana in place, the company transformed its application security posture:

- Over 500,000 attacks blocked every quarter across all the web applications
- Over 180K DDoS and 220K+ targeted vulnerability exploitation attacks prevented per quarter
- Zero successful breaches reported post-deployment over the last 11 years
- All identified vulnerabilities were virtually patched before any of the exploit attempts succeeded
- Non-human traffic blocked using behavior analysis and header-based fingerprinting
- 99% of DDoS attacks are mitigated automatically by AppTrana's AI engine
- New applications onboarded quickly and securely, with no performance trade-offs