INDUSFACE™

CASESTUDY

From 200+ Days to 72 Hours: Rapid Vulnerability Remediation with AppTrana WAAP

ABOUT THE CUSTOMER:

A leading U.S.-based third-party benefits administrator (TPA) specializing in flexible benefits plans and COBRA (continued health coverage compliance) management. With a strong nationwide presence, the company serves over 2,000 clients across various industries. Operating in the HR and employee benefits domain, the company leverages technology to streamline compliance and efficiency while ensuring accuracy and fostering long-term client partnerships.

KEY CHALLENGES:

1. **Delayed Vulnerability Patching**

   The customer was an existing user of Indusface WAS (DAST Scanner) and Penetration Testing services. They relied on their internal team to manually patch detected vulnerabilities. Constraints such as third-party dependencies, limited security resources, and competing development priorities often delayed remediation for weeks or even months, leaving applications exposed to potential threats.

2. **Security Operations Running in Silos**

   The customer used Cloudflare WAF for protection against cyber threats like DDoS and bot attacks. However, they faced challenges in utilizing its virtual patching capabilities effectively. Cloudflare WAF did not seamlessly integrate with other third-party DAST scanners (in this case, Indusface WAS), making virtual patching difficult.

   Even when virtual patching was possible, the customer had to manually create and configure security rules within Cloudflare WAF and test for false positives - a complex, time-consuming process requiring deep tool expertise and a huge learning curve.

3. **Increased Risk Exposure & Compliance Challenges**

   The delays in vulnerability patching heightened the risk of exploitation. Meeting compliance requirements was challenging, as vulnerabilities remained open beyond acceptable security standards.

4. **High Operational Costs & Overhead**

   Managing multiple security solutions, manually configuring custom rules, and relying on internal teams for vulnerability patching led to increased operational costs. The customer needed a streamlined, cost-effective solution to enhance security measures.

SOLUTION:

During a Quarterly Business Review (QBR) with Indusface, the customer was introduced to **AppTrana WAAP's SwyftComply offering,** the only WAAP solution in the industry that promises a clean, zero-vulnerability report within **72 hours.**

They decided to onboard one site as a proof of concept (PoC) and experienced the following benefits:

1. **Automated Vulnerability Patching in 72 Hours**

   Unlike other WAF providers, AppTrana WAAP's SwyftComply is the only solution that autonomously patches all Critical, High, and Medium (CHM) vulnerabilities within 72 hours at the WAAP level, eliminating manual effort from security teams.

   A key advantage was that the Indusface Managed Services team handled the virtual patching process end-to-end; identifying vulnerabilities, creating patches, thoroughly testing them, and deploying them. This eliminated the need for the customer to manually create or manage virtual patches, significantly reducing time spent on WAF operations.

As a result, the window of exposure was reduced by 200+ days, and the customer consistently received a **clean vulnerability report** for audits and compliance.

2. **Seamless CI/CD Integration for Developer-Friendly Security**

The customer also integrated the Indusface WAS (DAST Scanner) into their CI/CD pipeline, enabling early vulnerability detection during development.

While SwyftComply handled automated patching at the WAAP level, developers only needed to manually fix vulnerabilities requiring direct intervention, such as open ports where virtual patching was not feasible. This reduced security bottlenecks in the development cycle.

3. **A Unified Platform for Detection, Protection & Compliance**

By transitioning to AppTrana WAAP, the customer consolidated multiple security functions under a single platform, gaining benefits such as:

- Automated + manual pen testing for vulnerability scanning
- Faster Remediation with Virtual Patching & Fully Managed Security Services
- DDoS & Bot Mitigation
- Zero-Day Protection
- AI-Powered Behavioural Threat Detection and Prevention

By eliminating the need for an additional WAF vendor, security operations were simplified, and overheads were reduced. The combined DAST + WAAP solution by AppTrana also resulted in 30% cost savings per website.

4. **Instant Deployment with No Downtime**

The customer was fully onboarded **on the same day,** with zero downtime - ensuring business continuity while enhancing security.

RESULTS:

- Cost Savings with a Unified Security Solution – By replacing Cloudflare WAF and consolidating security measures under AppTrana WAAP, the customer achieved a 30% reduction in expenses as compared to earlier, while gaining enhanced protection
- Vulnerability Remediation within 72 Hours – Reduced the vulnerability exposure window from 200+ days to just 3 days.
- Faster Audits & Compliance – Clean vulnerability reports ensured seamless security audits and regulatory compliance.
- Enhanced Operational Efficiency – Eliminated the efforts required by internal security teams to create WAF rules