INDUSFACE™

CASE STUDY

Migrating from Cloudflare WAF to AppTrana WAAP for Enhanced Security & Performance

ABOUT THE CUSTOMER:

The customer is a direct-to-consumer (D2C) company based out of New York, specializing in selling collectible and personalized products, including jewellery, home décor, and memorabilia. With millions of customers across North America, they are known for offering unique, high-quality items that cater to a wide range of consumer interests.

Their infrastructure was deeply integrated with Salesforce, and as part of a bundled offering, they opted for Cloudflare's Add-On WAF, which was provided through Salesforce's partnership with Cloudflare at a bundled price.

While this seemed like a cost-effective solution at the time, the company soon encountered security and performance limitations that impacted their ability to provide a seamless and secure user experience.

CHALLENGES:

Despite using Cloudflare's WAF, the company faced multiple challenges that made it difficult to secure their applications and maintain optimal performance.

1. **Lack of Granular Controls & Inefficient Threat Management**

- Every new attack required the customer to manually create custom rules, delaying mitigation and leaving applications vulnerable for extended periods.
- High false positives led to legitimate traffic being blocked, negatively impacting the user experience.
- Cloudflare WAF required manual tuning for specific security policies, making it harder to fine-tune protections for evolving threats.

2. **Performance Bottlenecks & Site Slowness**

- The company frequently experienced website slowdowns as Cloudflare's WAF took longer to inspect and process each request, adding delays to response times.
- Delays in rule execution and security policy application increased server load, further slowing down the website.

3. **Limited Support for Urgent Threats**

- The bundled Cloudflare plan with Salesforce did not include managed security services, requiring the in-house team to handle security incidents independently.
- The company faced delays in getting timely support, making threat resolution time-consuming and leading to increased downtime and operational disruptions.

4. **Unmonitored Vulnerabilities & Lack of Proactive Protection**

- The organization's vulnerabilities on APIs, websites, and open-source /third-party integrations remained unmonitored, leaving critical data exposed to potential exploits.

- Without continuous security assessments and proactive patching, emerging threats often went undetected, increasing the risk of breaches.

These challenges collectively weakened the company's ability to maintain a secure, high-performance digital platform, ultimately impacting business continuity, customer trust, and operational efficiency.

SOLUTION:

To overcome these challenges, the company migrated to AppTrana WAAP (Web Application and API Protection) - a fully managed security platform offering AI-driven protection that provided with granular threat controls, real-time monitoring, and expert-driven attack mitigation.

1. **Granular Security Controls & Automated Threat Mitigation**

- AI-powered threat detection blocked over 90% of DDoS, bot, and zero-day attacks in real-time, minimizing security risks upfront.
- Custom security rules, created and managed by Indusface's expert team, ensured precise protection, eliminating false positives and blocking only malicious traffic.
- Zero-touch attack mitigation allowed security incidents to be handled without manual intervention, significantly reducing the customer's security team's workload.

2. **Optimized Performance & Faster Content Delivery**

- Intelligent traffic filtering and faster in-line threat analysis reduced processing delays, lowering server load and improving site responsiveness.
- Edge caching with CDN accelerated content delivery
- During the high-traffic events, AI-powered rate limiting ensured seamless performance to a vast majority of users

3. **24/7 Security Management & Expert-Led Threat Mitigation**

- With Indusface's managed security services, the company no longer had to rely on its internal team for security incident management.
- Round-the-clock expert support ensured immediate threat response, preventing downtime and operational disruptions.
- Proactive security insights and attack trend reports helped the company anticipate threats and continuously improve its security posture.

4. **Continuous Vulnerability Monitoring & Proactive Protection**

- AppTrana's embedded DAST scanner provided real-time vulnerability detection across applications and APIs, ensuring critical threats were identified and prioritized for action.
- Autonomous Vulnerability Patching within 72 hours reduced the company's exposure time from months to days, addressing critical security gaps swiftly.
- Quarterly attack trend analysis and security recommendations from the Indusface managed services team helped the company continuously refine its security processes and strengthen its defense strategy.

RESULTS:

Securing Growth Without Compromising Performance

By switching to AppTrana WAAP, the company achieved significant improvements in both security and performance:

- **100% Uptime & Faster Page Loads** – Optimized traffic filtering and smart caching improved website availability and response times.
- **100% Managed Threat Mitigation** – Expert-led incident response eliminated the burden of manual security management.
- **Zero Critical Vulnerabilities Left Unattended** – Continuous vulnerability assessments and autonomous patching in 72 hours strengthened overall security.
- **Enhanced Customer Experience** – Reduced false positives ensured uninterrupted access for legitimate users, improving engagement and retention.

With AppTrana WAAP, the company no longer had to compromise between security and performance. They now operate with peace of mind, knowing their applications are fully protected, high-performing, and resilient against evolving threats.