How a Fintech Unicorn Secured 6,000+ API Endpoints with AppTrana

SOLUTION HIGHLIGHTS:

- **Blocked over 800 million API attacks and 600+ million DDoS attacks every quarter**
- Discovered and protected over 6,000 API endpoints, including shadow and undocumented endpoints
- Strengthened protection with AI & custom rules tailored for each API behavior
- Achieved 72-hour SLA-based remediation for all critical, high, and medium API vulnerabilities
- Reduced AWS costs, ensured zero false positives, and maintained an audit-ready posture

ABOUT THE CUSTOMER

The customer is one of India's leading fintech unicorns, offering digital financial solutions designed for small and medium-sized businesses. Their platform helps businesses manage payments, track transactions, and streamline daily operations through a mobile-first, API-driven SaaS model. As the platform scaled rapidly, securing its growing API infrastructure became critical to ensure performance, reliability, and user trust.

KEY CHALLENGES:

The customer's API infrastructure was expanding rapidly in both volume and complexity. As API usage became central to business operations, performance, security, and cost efficiency had to be tightly aligned. Several key challenges emerged:

- **Zero latency was mission-critical.** APIs powered high-frequency, user-facing features across web and mobile apps. Any added delay could degrade the experience and increase churn risk.
- **Frequent API-targeted DDoS attacks** on critical endpoints were starting to impact availability and infrastructure stability.
- **The existing API gateway lacked the flexibility** to apply traffic limits based on individual endpoint sensitivity. A one-size-fits-all approach was no longer viable.
- **AWS ingress billing was rising sharply** due to a high volume of unwanted traffic, including malicious requests and automated abuse.
- **The security team could not efficiently block bot networks,** especially when traffic originated from entire CIDR (Classless Inter-Domain Routing) ranges. This led to repeated abuse through credential stuffing and scraping.
- **There was no visibility into shadow APIs** that may have been exposed outside the gateway, increasing the risk of unmanaged access points.
- **There was zero tolerance for false positives.** Even a single legitimate request being blocked could disrupt business-critical workflows for thousands of users.

KEY CHALLENGES:

These challenges highlighted the need for a security solution that could provide complete API lifecycle coverage. The customer required a platform that could scale with traffic, eliminate visibility gaps, reduce attack traffic, and adapt quickly to changes, all without compromising performance.

SOLUTION:

To secure their fast-growing API ecosystem, the customer adopted AppTrana's fully managed API security. They received complete coverage, including discovery, classification, real-time protection, monitoring, and continuous improvement. The solution helped address immediate threats while supporting long-term operational scale and stability.

- **Comprehensive API discovery, including shadow endpoints:** Continuous discovery enabled full visibility into all exposed APIs, including undocumented shadow APIs that were not routed through the API gateway. Over 6,000 APIs were discovered and brought under protection, helping eliminate blind spots and ensure complete coverage. Frequent API-targeted DDoS attacks on critical endpoints were starting to impact availability and infrastructure stability. There was zero tolerance for false positives. Even a single legitimate request being blocked could disrupt business-critical workflows for thousands of users.
- **Risk-based API onboarding and classification:** APIs were assessed and categorized based on their exposure, sensitivity, and functionality. High-risk endpoints, such as login, payment, and user data APIs, were prioritized for onboarding and stricter security enforcement, followed by a progressive rollout of protection across lower-risk APIs.
- **Positive security enforcement through schema validation:** A positive security model was applied to allow only well-structured and expected API calls. Requests with unknown fields, incorrect formats, or unexpected structures were blocked at the AppTrana level, significantly reducing the attack surface.
- **DDoS protection using AI:** AppTrana's AI-powered capability monitored traffic patterns in real time and set appropriate rate limits for each API based on its sensitivity and behavior. High-risk APIs like login and payment were given stricter controls. Smart Mitigation Rules were also used to block entire CIDR ranges linked to malicious traffic, helping stop large-scale DDoS attacks without affecting real users.
- **Bot mitigation:** AppTrana identified and blocked bot attacks targeting login and payment APIs. These included credential stuffing to hijack user accounts, carding attacks using stolen card data, and bots trying to exploit referral programs through fake account creation. By analyzing behavioral patterns, malicious automation was stopped without disrupting genuine users.
- **VPC Peering to reduce AWS ingress billing and improve performance:** Integration with the customer's AWS environment through VPC Peering enabled early filtering of traffic. This reduced ingress bandwidth usage and improved response times by keeping traffic within the cloud backbone.
- **AI-led monitoring with expert oversight:** API traffic was continuously monitored using AI models that detected anomalies and flagged unusual behavior. This was backed by Indusface's 24x7 managed security team, which reviewed alerts, fine-tuned protection policies, and ensured accurate detection without false positives.
- **Continuous discovery, change detection, and protection updates:** Newly exposed APIs were continuously discovered and brought under protection, while existing APIs were monitored for changes in schema or exposure. Based on these insights, security policies were proactively updated, and all critical, high, and medium vulnerabilities were remediated within a 72-hour SLA through AppTrana SwyftComply's autonomous remediation.

This end-to-end approach helped the customer gain complete control over their API ecosystem. It ensured high availability, strong performance, reduced operational overhead, and resilience against evolving threats, without compromising user experience or agility. It also helped them stay audit-ready at all times, with updated protections and zero vulnerability reports for compliance.

RESULTS:

A view of the 90-day attack trend:

- 800+ million API attacks blocked every quarter
- 600+ million DDoS attacks mitigated per quarter
- Over 6,000 APIs discovered and brought under protection, including shadow and undocumented endpoints
- ~30 million attacks blocked using custom rules and positive security models
- Implemented VPC Peering to improve response times and reduce AWS ingress bandwidth billing for the customer
- Zero false positives assurance
- All critical, high, and medium vulnerabilities remediated within a 72-hour SLA
- Stayed audit and compliance ready with complete API visibility, documentation, and protection in place