INDUSFACE™

CASE STUDY

Protecting Bandhan Life Against Millions of Cyberattacks with Managed WAAP

SOLUTION HIGHLIGHTS:

- Discovered shadow applications & APIs
- **Blocked 1.5 million** DDoS, bot, zero-day and API attacks per quarter
- **Protected all the APIs** with positive & negative security models
- **Provided over 200+ virtual patches**
- **Saved thousands of dollars** required for hiring a dedicated security team

Bandhan Life

"AppTrana WAF is disrupting the market with a disruptive cost-value proposition to business, by including high-value services such as managed custom rules, security assessment, and risk-based managed cloud WAF at ~50% of the price point of other vendors who just provide a WAF with rules"

Kiran Belsekar (Executive VP – CISO & IT Governance, Bandhan Life)

ABOUT THE CUSTOMER:

Bandhan Life Insurance Limited (formerly known as Aegon Life Insurance Company) is an Indian life insurance company offering individual and group insurance online and offline. Founded in 2008, it is headquartered in Mumbai, India.

- Bandhan Life Insurance's distribution channels include banks, individual agents, brokers, and corporate agents, bancassurance partners, among others. The company offers term insurance plans, savings and investment plans, child plans, and unit-linked insurance plans (ULIPs)
- It was awarded as eBusiness Leader – Medium & Small at World BFSI Award by the World BFSI Congress

BUSINESS CHALLENGES & REQUIREMENTS

- As with any insurance provider, Bandhan Life had to integrate and collaborate with various agents, brokers, banks, and more. Hence, to keep the business protected, having a multi-layer security approach has always been a prime factor in their security journey
- The company had already deployed on all the basic security aspects like endpoint security, authorisation, and so on. However, due to the consistent decentralisation of their applications and increased usage of microservices & third-party tools, they were actively searching for a WAAP that could significantly improve their security posture
- Their primary requirement from the WAAP is to act as an additional layer of security and protect them from threats. Additionally, they were looking for a WAAP that could identify shadow assets & APIs and ensure that no applications/APIs remain hidden from their line of sight
- Another crucial requirement from Bandhan Life was that the WAAP should be capable of protecting them from open vulnerabilities while they fix and test the vulnerabilities in code before deploying – as managing vulnerabilities on hundreds of applications demanded some time to patch

- Due to limited resources in their security team, they wanted the WAAP provider to manage their entire application security journey and keep them updated with alerts and cyber attack reports in real time
- For all the above requirements, they identified multiple WAAP vendors in the market. However, most of the vendors provided many services as add-ons, and the cost of value wasn't justified from Bandhan Life's perspective.

SOLUTION BY INDUSFACE:

Indusface supported Bandhan Life in completing its entire application security requirements in 4 steps

Discovery & Onboarding

- Auto-discovered application and APIs on the AppTrana WAAP and provided a documented inventory to the customer
- Generated OpenAPI specification file (Swagger 3.0) automatically with pre-filled details
- Deployed the finalised applications on the AppTrana WAAP in the block mode with 0 downtime

Scanning

- Ran DAST scans on the applications and the infinite API scanner to identify OWASP's top 10 vulnerabilities across the entire ecosystem
- Identified the business logic vulnerabilities with the help of a manual pen test
- Came up with a detailed report for the open vulnerabilities along with the risk metrics of impact they are posing to the business

Autonomous Protection

- Protected all the critical, high and medium-level open vulnerabilities via virtual patching within a 72-hour time frame
- Developed custom API security models for internal and external users
- Blocked all kinds of external DDoS, bot, zero-day, and vulnerability-focused attacks at the WAAP level
- Created custom rules specific to internal/authenticated users for enhanced protection

Monitoring & Reporting

- In case of targeted attacks, the **24*7 support team** made sure to alert these attacks to the Bandhan Life and create **virtual patches** immediately to thwart them in real-time
- The management team of Bandhan Life were provided with a **consolidated report for quarterly business review,** which they could utilise to improve their security posture

Bandhan Life found Indusface's AppTrana WAAP to provide the best cost-to-value offerings for their needs, as other vendors were charging at least 50% more for similar solutions.
Since 2019, Indusface has been acting as the extended security team for Bandhan Life, making them a trusted partner.

RESULTS:

- Provided auto-discovery and protection for applications and APIs
- Provided **custom protection for external and internal users**
- **Millions of DDoS, bot, zero-day, and API attacks** blocked over a span of 5 years
- Thanks to the AppTrana value-added managed services team, Bandhan Life **saved thousands of dollars** on the hiring costs of a dedicated security team