INDUSFACE™

case study

Darwinbox - Multitenant Application Protection Through Apptrana

WHAT IS MULTITENANCY?

The term “multitenancy” refers to a software architecture in which a single instance of the software runs on a server and serves multiple tenants. Systems designed in such a manner are often called shared systems. A tenant is a group of users who share common access with specific privileges to the software instance. With a multitenant architecture, a software application is designed to provide every tenant a dedicated share of the instance – including its data, configuration, user management, tenant individual functionality, and non-functional properties.

THE BUSINESS

Darwinbox is one of the leading HRMS (Human Resources Management System) businesses that provides a SaaS-based and end-to-end HRMS suite to the eEnterprise clients and has an agile, highly intuitive, and easy to-use product with user- centric design and understands the enterprise-level of complexity. Once the user logs into Darwinbox’s portal, they can perform multiple HRMS activities such as recruitment, onboarding, payroll management, employee management, time and attendance, rewards & recognitions, etc.

Presently, they are providing a frictionless experience to their customers by protecting their digital assets through Apptrana’s Next-Gen WAF solutions.

PROBLEMS TO SOLVE:

As per the Application architecture, for every customer, a unique subdomain was configured for accessibility, and the tenant was created. There were 450+ unique subdomains for which the customer (Darwinbox) wanted protection. Being a complex architecture, the customer was looking for a holistic, SaaS-based, and fully-managed security solution which is cost-effective and provides comprehensive coverage for Application security. The customer was looking for a trusted security partner who could take care of their application security need so that they could focus on their business.

The customer’s high-level requirement from a security partner was to:

- Identify and mitigate risks continuously, meet compliance requirements, and improve application delivery agility.
- Ensure business continuity through site availability, protection of brand reputation, and elimination of the security barrier for sales.
- Immediate, affordable, managed, and risk- based approach to application security.
- To provide a security solution that is simple and easy to map to its business use cases.

THE SOLUTION INDUSFACE PROVIDED:

We understood the client’s requirement and performed a detailed analysis to provide them with the best and suitable solution to address their requirements – to onboard 450+ unique domains. We proposed & deployed our SaaS-based, managed, advance application security solution “Apptrana”. It is a cost-effective solution and offers the following benefits to enhance their application security risk posture:

Managed Risk Detection: This helps in eliminating the application design’s weakness instantly and minimizes the attack surface for attackers to target and exploit. As all the 450+ domains were a clone of the application, we activated continuous scanning and performed the manual penetration testing on the primary domain and replicated the configuration to test all the 450+ domains.

- **On-demand Automated Scans:** We configured continuous scanning to identify the applications’ vulnerabilities and immediately secured it through the intelligent virtual patching functionality of Apptrana.
- **Manual Penetration Testing:** As the customer’s application handles user-critical data and undergoes frequent upgrades, we performed manual penetration testing to analyze the business-logical flaws in the application workflow and immediately secured the logical flaws through the intelligent virtual patching functionality of Apptrana. All the custom rules to patch the automated scanner and manual penetration testing findings were replicated on all the 450+ domains on-boarded.

SPOTLIGHT

Customer

darwinbox

SOLUTIONS DEPLOYED

- Indusface AppTrana

ABOUT THE COMPANY

Darwinbox is a cloud-based HRMS platform that automates HR processes from Recruitment, Core transactions (Leaves, Attendance, Directory), Payroll, Employee Movement, Employee Engagement, Talent Management, and People Analytics.

HEADQUARTERS

Hyderabad, India

SIZE

201-500 Employees; 500+ Clients

INDUSTRY

HR (Human Resources)

HIGHIGHTS

500+

The total number of tenants secured through Apptrana

90%

Caching ratio achieved and maintained through AppTrana CDN

50%

Improvement in performance observed across web applications

INDUSFACE™

case study

Darwinbox - Multitenant Application Protection through Apptrana

Managed Risk Protection: Updated with out-of-the-box core rules along with managed virtual patching and custom rules with zero false-positives from security experts, we built a strong security model through AppTrana ‘s next-generation and geo-based Web Application Firewall for web application protection. Here are the relevant features:

- **Managed DDoS Protection and Bot Mitigation:** A resilient auto-scaled infrastructure and protection against targeted as well as volumetric DDoS and bot attacks as part of the managed service from security experts.
- **Instant Protection Against Zero-Day Vulnerability:** Backed with a core signature development and research team that provides instant protection against new zero-day vulnerabilities and threats.
- **No False Positives:** Accurate rules and virtual patching from security experts with a zero false-positives guarantee and backed with an SLA.

Managed Security Service: Indusface security experts monitor the web traffic 24×7 to prevent sophisticated attacks such as Advanced DDoS, Bot attacks, and Zero-Day protection, etc. The managed security service team is continuously monitoring the threat landscape, detecting the anomalies, and updating the rule sets to progressively enhance the security posture of the application. Also, they monitor the application’s uptime to maintain site availability. All the custom rules designed by the managed security service team were replicated on all the 450+ domains.

Secured CDN: We activated the CDN service for all the 450+ domains and started caching the static content to boost the performance of the application. We ensured the traffic that can be served by the CDN is served swiftly from the nearest CDN POP to the user and when traffic must be directed to the server, it goes through AppTrana WAF and is protected against malicious traffic/attacks. Primarily, we started caching the static objects of the application which do not change significantly. E.g.: Images, JavaScript, CSS files, PDF files, Media files, and set the CDN to cache the following file extensions [Jpeg, jpg, png, gif, ttf, woff, woff2, swf, doc, mp3, mp4, mov, wav, flv, js, css]. Followed by that, we monitored and learned the application analytics to analyze and classify the frequently accessed content and activated the advanced CDN policies to further cache a wider range of content that was earlier deemed non-cacheable and unserviceable. The caching ratio was monitored at around 90% and the web application performance was enhanced by more than 50%.

RESULTS

By implementing Apptrana – Total Application Security solution that provides a variety of services such as Automated Scan, Manual PT (Pentesting), Next-Generation WAF, DDOS Protection (Layer 3 to Layer 7), Bot Protection, Zero-Day Protection, Managed Services, and Secured CDN services under one umbrella, the customer got a single point of contact for all their Appsec needs. All the 450+ subdomains were successfully secured through the Apptrana WAF solution. The managed security service team being a security partner, is continuously monitoring and enhancing the security posture of the application round-the-clock, interacting with the customer, taking the required security actions, and alerting the customer on a need basis. Also, periodic vulnerability assessments are helping the customer to know the application’s risk posture and immediate remediation at WAF is allowing them to keep their applications secured all the time.

KEY HIGHIGHTS

Multi-tenant Architecture setup with cloud-based WAF and activation of WAF for all the tenant Application.

License customization to secure all the subdomains

Replication of custom WAF policies across all the subdomains to maintain protection level.

Virtual patching of the application-specific vulnerabilities at WAF and propagation of the WAF policies across all the subdomains to maintain the protection level.