wallarm

bayt

CASE STUDY

Bayt Modernizes Application Security

Eliminating Manual WAF Management and False Positives with Automated Protection

Overview

Bayt operates one of the Middle East's largest online job platforms, serving millions of users and high volumes of application traffic. Protecting this environment required strong security without impacting performance or user experience.

The company's legacy signature-based WAF created operational challenges. Manual rule updates, frequent false positives, and constant engineering intervention made the system difficult to manage and inefficient at scale.

By deploying Wallarm's Next-Generation WAF integrated directly with its NGINX web layer, Bayt replaced reactive rule management with automated threat detection. The result was a more stable security posture, reduced operational overhead, and a scalable protection layer that has supported their infrastructure for more than a decade.

About The Organization

Bayt is one of the Middle East's leading online recruitment platforms, connecting employers with millions of job seekers across the region.

High-traffic platform serving job seekers and employers across multiple countries

Infrastructure built on high-performance NGINX web architecture

Security must protect applications while maintaining low latency for users

> "Wallarm provides a rare combination of robust security, automated intelligence, and a low total cost of ownership. It effectively eliminates the 'management tax' associated with traditional security tools."

Challenges

Bayt needed to modernize its application security infrastructure and move beyond the limitations of a traditional signature-based WAF.

High Operational Overhead

The existing WAF required constant manual rule updates and tuning. Security engineers spent significant time addressing false positives and maintaining signatures, diverting resources away from more strategic security initiatives.

Service Disruptions from False Positives

Frequent false positives occasionally blocked legitimate user traffic, creating friction for customers and additional troubleshooting work for engineering teams.

Reactive Security Model

Because the legacy system depended on static signatures, the team was forced into a reactive "whack-a-mole" model—responding to issues after they occurred rather than preventing them through automated analysis.

The company needed a more intelligent solution that could automatically analyze traffic behavior, reduce false positives, and operate efficiently at scale.

Solution

Bayt discovered Wallarm through a technical discussion with the company's founder on Hacker News. This early interaction gave the team direct insight into the architectural philosophy behind the product and confirmed that it aligned with their technical requirements.

During their evaluation, Bayt focused on several non-negotiable requirements:

- Native on-premises deployment to maintain full data control
- Ultra-low latency to ensure no impact on user experience
- Seamless integration with their NGINX web layer
- Lower total cost of ownership than traditional security tools
- An architecture capable of automated threat detection

Wallarm was the only solution that met all of these requirements without compromise.

Because the platform integrates natively with NGINX, Bayt was able to deploy the solution directly within its existing infrastructure. Automated behavioral analysis replaced manual rule tuning, dramatically reducing operational overhead while maintaining strong protection against modern threats.

Outcomes

After deploying Wallarm, Bayt achieved a shift from reactive security management to long-term operational stability. Key outcomes included:

- Elimination of manual WAF rule maintenance, freeing engineering teams to focus on strategic initiatives
- Significant reduction in false positives, preventing disruption to legitimate user traffic
- Stable, scalable protection for over a decade, with the platform evolving alongside their infrastructure and threat landscape

Instead of constantly managing signatures and exceptions, the team now relies on automated learning and detection to maintain protection with minimal intervention.

Ongoing Value

Over more than ten years of use, Wallarm has become a foundational component of Bayt's security architecture.

The platform continues to deliver value through:

Low-latency protection that operates invisibly to users

Seamless scalability alongside growing traffic volumes

Continuous automated detection without constant management

Wallarm's support team also plays an important role in maintaining the environment. Direct communication channels allow the Bayt team to resolve technical questions quickly and escalate complex issues to engineering experts when necessary.

This collaboration has enabled Wallarm to function as an extension of the internal DevOps and security teams.

"The silence in terms of false positives and traffic disruptions is the clearest indicator of the solution's effectiveness."

wallarm

About Wallarm

Wallarm is the unified platform for API Discovery, API Protection, API Security Testing, and AI application security. Wallarm helps organizations secure APIs, AI agents, and modern applications across cloud-native and hybrid environments without slowing innovation.

Schedule a Demo

Website Blog X (Twitter) LinkedIn YouTube

Explore Product