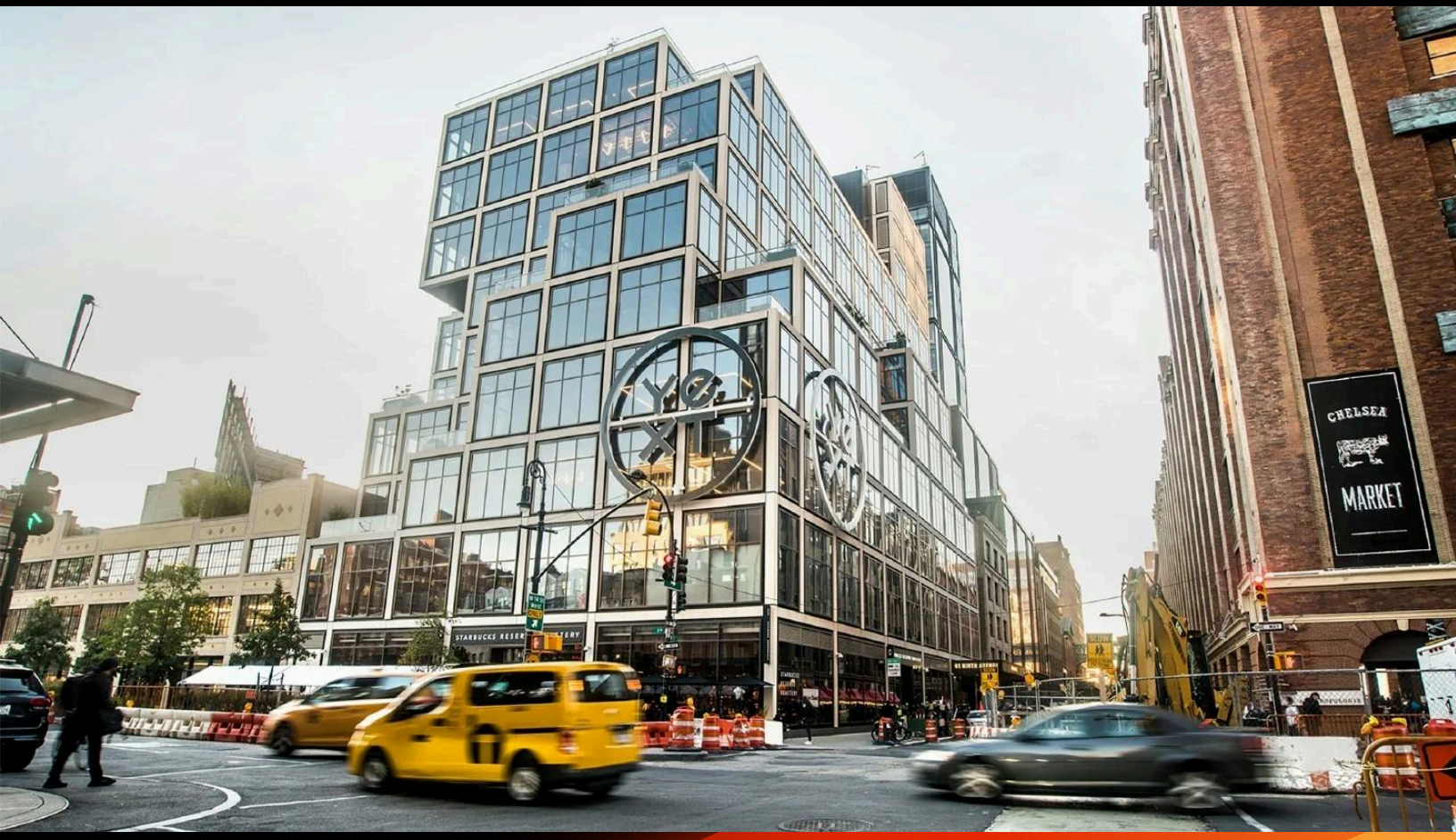
wallarm



CASE STUDY

Yext Secures Its Digital Experience Platform with Wallarm API Security

From Unknown Attack Surface to Millions of Blocked Attacks — and 60% Savings in Bug Bounty Costs

wallarm

Overview

Yext operates a Digital Experience Platform (DXP) that helps brands manage and distribute critical business data across search engines, maps, apps, and other digital channels. APIs are foundational to their platform because their business model is built on sharing and distributing structured data at scale. The reliance on APIs for Yext makes API security a clear business priority.

Yext needed comprehensive visibility into its API attack surface, proactive protection beyond a traditional WAF, and deployment flexibility that worked with complex infrastructure. After implementing Wallarm, Yext gained full API discovery and observability, blocked millions of attacks, avoided significant bug bounty payouts, and transitioned confidently from visibility to enforcement.

wallarm

About Yext

Yext is a Digital Experience Platform that helps brands amplify their impact by managing and distributing structured knowledge across digital ecosystems.

Operates a large-scale API-driven data distribution platform, supported by **1200+ employees** across **10 global offices**.

Supports **250+ API-based integrations** with platforms like **Amazon Alexa**, **Google**, **Salesforce**, **Shopify,** and **Zendesk** to keep business information synchronized across the web.

Yext's Analytics APIs (Reports API and Logs API) expose over **80 metrics** and **90 dimensions**, enabling programmatic extraction of both aggregated and event-level analytics for further analysis or embedding.

Deployment was really crucial for us. Our infrastructure is complex, and the flexibility and ease of the Wallarm deployment model was a huge part of why we decided to move forward.

Matthew Szymanski, Director of Information Security, Yext

wallarm

Challenge

Yext's Digital Experience Platform depends on APIs to distribute customer data across multiple channels. That business model inherently exposes them to a broad range of API attacks. Before implementing Wallarm, Yext faced several challenges:

Limited Visibility

- No complete inventory of exposed API endpoints
- Minimal monitoring and logging of API traffic
- Little understanding of real-world attack activity

Reactive Security Posture

- Heavily reliant on an active bug bounty program to identify vulnerabilities
- No proactive API-specific mitigation capabilities
- Traditional WAF (Cloudflare) only monitored routed traffic and was not designed for API security

Legacy Configuration Risks

- Lenient WAF rules that were difficult to modernize
- Regular expression–based rules that struggled to block complex attack types
- Shadow and unprotected API endpoints

The core business problem was simple, but critical: They needed to know what existed before they could protect it. Discovery, then observability, then policy enforcement.

wallarm

Solution

Yext evaluated API security vendors after recognizing elevated attack levels and limitations in their existing WAF.

Key evaluation criteria included:

- Clear API inventory and discover
- Intuitive platform navigation
- Actionable, consolidated security insights
- Business logic abuse detection
- Deployment flexibility (agent deployment was not an option)

Yext had prior experience evaluating other vendors and found usability and reporting lacking.

Wallarm stood out by:

- Providing full API Discovery across their environment
- Detecting threats that bypassed their traditional WAF
- Enabling business logic abuse detection
- Delivering flexible, infrastructure-friendly deployment
- Supporting a move from visibility to enforcement

Wallarm's ability to operate independently of traffic routing through a specific CDN was a key differentiator. It revealed shadow APIs and previously unseen threats. Beyond the platform itself, Yext valued Wallarm's proactive monitoring and white-glove support. A proactive outreach regarding unusual activity reinforced the partnership's value.

wallarm

Outcomes

After deploying Wallarm in front of production traffic, Yext saw immediate impact:

- 129,000 attacks blocked immediately post-deployment — over 100,000 of which would have bypassed their traditional WAF. More than 3 million attacks blocked in the last year.
- 60% of bug bounty traffic would have been stopped during POC, reducing payouts by a corresponding 60%.
- Full API attack surface visibility, enabling confident policy enforcement

The organization transitioned from uncertainty to enforcement, achieving its original objectives around discovery and observability.

Compliance and governance benefits also emerged:

- Improved readiness for customer security reviews
- Stronger responses during cyber insurance audits
- Alignment with evolving requirements such as NIS2
- Better positioning amid increased scrutiny from insurers where API breaches represent a growing portion of claims

> **We saw 129,000 attacks blocked. That's over 100,000 threats that would have completely bypassed our traditional WAF.**
>
> **Jake Jacobs-Smith, Product Security Manager, Yext**

wallarm

Ongoing Value

Yext continues to expand enforcement policies with confidence. Wallarm's proactive monitoring and customer success engagement provide incremental value beyond the technology itself.

What began as a discovery initiative evolved into a mature API security program with:

- **Continuous visibility**
- **Business logic abuse detection**
- **Proactive threat mitigation**
- **Governance and compliance support**

wallarm

BOOK A DEMO

www.wallarm.com
(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107