DATADOG | namify

CASE STUDY

Namify turns to Datadog to gain real-time visibility into critical production threats

ABOUT NAMIFY

Namify is a US manufacturer of identification and branding items. The company serves over 130,000 clients worldwide, including over 65 percent of the Fortune 500.

E-Commerce

150 Employees

Springville, Utah

"One of the most important things for us was to correlate all the information related to production. This visibility allowed us to solve the puzzle, and it was a game changer."

Marcus Flores
Director of Development
Namify

WHY DATADOG?

- Delivers correlated observability and security insights in a unified platform
- Offers automatic threat detection and clear prioritization to cut through alert noise
- Provides deep production visibility that helps developers quickly diagnose and remediate vulnerabilities

CHALLENGE

As Namify's product and user base grew, its existing tools lacked the visibility needed to detect and address emerging threats, prompting the need for a unified, developer-friendly security solution.

USE CASE

APM

App and API Protection

Log Management

KEY RESULTS

Immediate attack detection and mitigation

Identifies active SQL injection attempts

Rapid vulnerability remediation

Detailed alerts and context help isolate and patch exploitable components

Correlated visibility across production

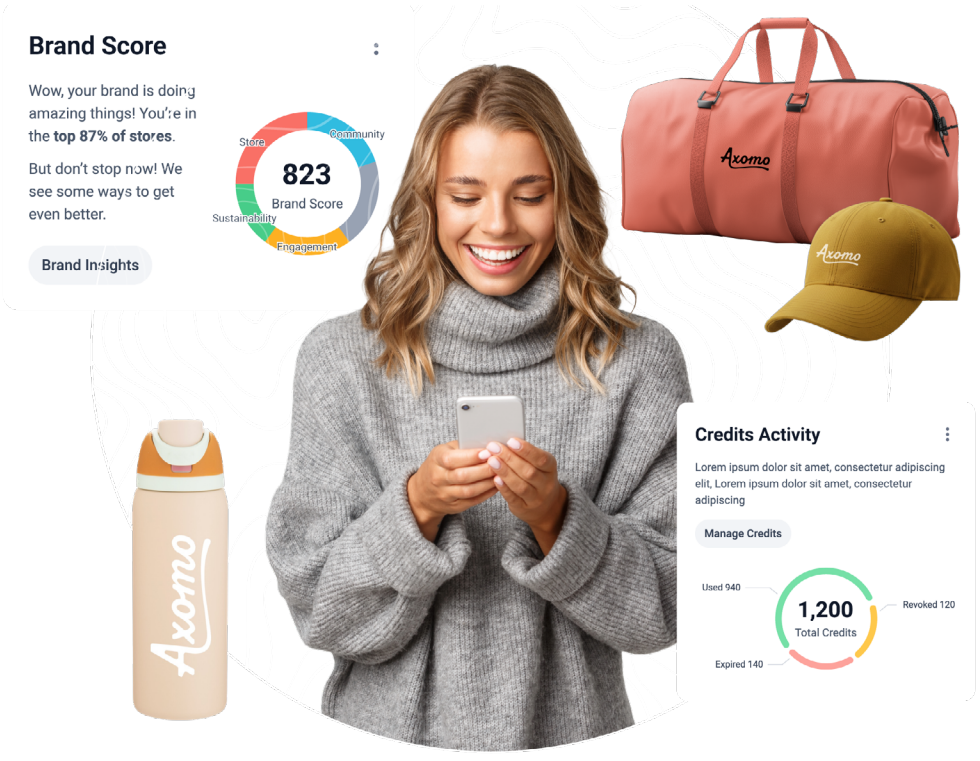
Unifying data and security events enables suspicious activity to be traced to specific services and code paths

Lack of visibility and correlation limits ability to detect emerging threats

Namify is a US manufacturer of identification and branding items that offers same-day services in graphic design, full-color printing, engraving, embroidery, and wide-format printing. The rapidly growing company serves hundreds of clients worldwide, including over 65 percent of the Fortune 500.

Namify initially focused on rapid product innovation, but as its product portfolio and user base expanded, its IT team realized their existing security tools lacked the visibility and correlation needed to detect and address emerging threats. Its existing toolset couldn't sufficiently correlate data across logs, traces, and application layers, which created blind spots in production. "We knew we had some vulnerabilities that we were unable to patch. In other words, we were not confident in our posture or our ability to see everything happening in production," says Marcus Flores, Director of Development at Namify. "The turning point was a few engineers reaching out because they had noticed something suspicious coming through logs and other metrics. We needed more visibility into our applications."

Namify needed to strengthen its application and API security to protect against emerging threats and improve confidence in its overall security posture. The company sought an all-in-one solution to not only detect threats in real time but also guide developers to fix the root causes before attacks became full-blown incidents.



Gaining end-to-end insight as threats evolve

Namify had been using Datadog for observability for a couple of years. As the company looked to improve its attack visibility in production, it again turned to Datadog.

By adding Datadog App and API Protection, Namify can now not only see security issues but also integrate and correlate them with traces and logs in one central location. By using Datadog's security products, Namify can rapidly block malicious attempts while giving engineers the breathing room they need to roll out fixes safely. The unified dashboard cuts through the background noise of automated scans, helping the team focus on genuine threats.

> "We knew we had some vulnerabilities that we were unable to patch. In other words, we were not confident in our posture or our ability to see everything happening in production."

Datadog App and API Protection came in handy recently when Namify began experiencing targeted SQL injection attacks. The attacker started a very large security scan (~100k attacks) and then attempted to exploit a vulnerability they identified. This meant that meaningful exploits were lost in the noise. “For this specific incident, we were not sure a bad actor was coming through,” says Flores. “We had an entire team threat-hunting. We did not know that components had been targeted. It could be the same person probing a different back door.”

Datadog quickly flagged the activity and generated a high-severity alert. After confirming that an attacker was probing different vulnerabilities, Namify relied on Datadog’s correlated traces to spot patterns and scope the potential impact. “Based on our logs and other tools, we already suspected something when the notifications and alerts came in, so the alerts did not catch us by surprise,” says Flores. “But we didn't know we could mitigate the effect and slow the attackers and have an edge to patch while still being protected. We needed a quick way to stop the attack while we tested and deployed the patch.”

Namify was able to surface the attacks and bring attention to the high-threat requests, ensuring that 100 percent of successful exploits were captured (less than half would have been captured by their legacy approach). This greatly simplified the investigation since they could see everything the attacker did. “One of the most important things for us was to correlate all the information related to production,” explains Flores. “This visibility allowed us to solve the puzzle, and it was a game changer.”

Datadog App and API Protection becomes foundational to Namify’s security

Datadog App and API Protection quickly identified active SQL injection attempts, even those hidden by obfuscation and automated scans. Clear alerts and rich context enabled Namify’s team to rapidly isolate and fix the vulnerable components. Datadog’s integrated approach to application security gives Namify the protection and clarity it needs to confidently scale its operations.

Looking ahead, Namify plans to continue growing across new cloud environments, confident that Datadog’s coverage extends seamlessly across providers. “We’re very happy that we can still use the same tool in our new cloud environment,” says Flores.

GET STARTED WITH A FREE TRIAL TODAY >