VERIFIED THREAT

Your Store Wizards

Case Study September 2025

Ecommerce | 50-100 Employees | Location: CA, USA

Deployment and Approach

Rapid Setup: "It was a simple cloud based automated setup that stopped 98% of the problem immediately."

Comprehensive Coverage:

VerifiedThreat scanned across all the cloud and on-prem infrastructure to identify and remediate incoming threats that other platforms couldn't detect or pick up.

Actionable Reporting:

Bittke and his team can visit the VerifiedThreat dashboard and get real-time status on any unusual traffic hitting their API.

"Finally, we can see what we're up against."

Prioritisation:

Risks were ranked by exploitability and relevance, enabling the security team to focus on what mattered most.

Zero False Alerts

Every alert was verified with evidence. A full vulnerability exposure and log details are available to deep dive.

Search Magic Ecommerce API Service.

It was the run-up to the incredibly busy Black Friday season and Your Store Wizards' developer Brett Bittke realized something strange was happening to his company's popular search enhancement application, Search Magic.

For ecommerce sites, a tool like Search Magic makes a huge difference to sales by accelerating the speed at which consumers can find products. Suggested products appear automagically as users type in the search box, spelling errors are corrected, while the application can even resolve unusual synonyms or words to the correct product.

Now, after many years of flawless performance, the application had slowed to a crawl for its 200 customers as it experienced what looked like a denial-of-service (DoS) attack on the tool's API.

"We were getting traffic coming in from large numbers of mobile phones in different locations with all sorts of IP addresses. It was a constant pain that at times was knocking down our servers,"

says Your Store Wizards developer, Brett Bittke. The company responded by increasing the number of servers but throwing horsepower at the problem made no difference. The rogue traffic simply scaled to consume those additional resources as well, costing the company in additional hosting and CPU resources, configuration and server maintenance.

It looked like a DoS but the fact that the traffic was emanating from what appeared to be legitimate mobile phone user agents was a clue they'd met a new enemy that has grown in recent times from occasional nuisance to major business hazard – price scraping and product surveillance bots.

Today's ecommerce sites are afflicted by all manner of bots with different purposes, but price scrapers are among the most troublesome. Their aim is to monitor a competitor's prices on a 24x7 basis with a view to understanding their economic model in detail.
Normally, price scrapers can be blocked by a few tweaks to the WAF which is why more sophisticated bots have started using large numbers of residential IPs - genuine home PCs and mobiles - to make blocking difficult or impossible without risking false positives.

Realtime AI Remediation

VerifiedThreat layers across existing defence setups, scales out autonomously and combines verified vulnerability testing with instant AI remediation.

Security Standards

Support for ISO 270001, SOC 2 & NIST Frameworks takes the pain out of manually recording incident and logging risk data, and automatically maps to each relevant control.

Attack Vector Chaining

Attackers can exploit weakly segmented domains to move laterally and escalate privileges. VerifiedThreat stops the attacks at the reconnaissance stage - before they can cause damage. This dramatically reduces the reconnaissance stage attacks by 70-90% and prevents more serious attack escalation in the future based on exploiting the weak defences.

Benefits

Typically customers see an immediate decrease in reconnaissance activity which leads to 30-40% decrease in unexpected server maintenance and overhead.

Benefits can be measured by setting up custom tags for each major risk area, department or risk owner, and can be reported on an enterprise-wide basis to give complete 360° visibility using custom KPIs that can be tailored to meaningful business impact.

The traffic slowing Search Magic was to an API, which because it is always automated makes distinguishing legitimate traffic from rogue especially difficult. The traditional WAF approach struggles to defend against this type of threat, while user CAPTCHAS won't work at all.

Why Verified Threat?

The company selected VerifiedThreat to provide constant vigilance and support for new attack threats and techniques. Ecommerce services are constantly subject to novel attacks. "We were using Cloudflare's general bot protection, but this wasn't working," comments Bittke. "We couldn't risk blocking users, or we might end up blocking real customers." The alternative was to subscribe to Cloudflare's enterprise bot service, but this way out of their price range.

Results

- **The Search Magic API** quickly became available to the company's customers again and the developers were able to return expensive server capacity to its normal level.
- **Significant Cost Savings:** VerifiedThreat reduced the overall API hosting and processing costs considerably, and reduced server maintenance costs by 70%.
- **Partner Confidence:** The 200 customers that actively consume the pricing API data received higher quality of service and greater confidence.
- **Operational Efficiency**: This specific threat resulted in some downtime and forced the team into support and remediation. VerifiedThreat was able to pinpoint the issue and solve the problem quickly, saving valuable time and resources..
- **OnGoing Threat Protection:** Critically, VerifiedThreat offers on-going protection and constantly checks for new vulnerabilities.

Impact

By using VerifiedThreat, Your Store Wizards had the following impact:

- **Technical**: Continual threat detection, combined with threat verification and automated remediation proved to be a game changer in terms of service delivery and rapid deployment..
- **Business:** Reduced costs, better use of resources across the new cloud microservices and legacy infrastructure, and stronger assurance to its customers and senior leadership team..

Verified Threat uncovered existing risks but also counters new threat types. If there's a new threat now, Bittke and his team get verified alerts on the new threat, so they can investigate.

"Finally, we can see what we're up against."

Brett Bittke Your Store Wizards.

Please reach out to our sales team and book in a demo to see the platform

www.verifiedthreat.com