Case Study: E-commerce Information Technology

Distrelec Elevates Web Application Security with Radware WAF and Bot Management

Customer

Distrelec

Industry

E-commerce
Information Technology

Problems Faced

- Web applications vulnerable to a number of common attacks
- Significant malicious bot traffic disrupting operations and more
- Need for a solution that provides protection without affecting legitimate users

Why Radware

- WAF blocked threats with machine learning and signature-based protections
- Bot Manager identified and classified bots, allowing only good bots access
- Policies managed bot traffic through rate limiting, CAPTCHA challenges and more

Overview

In today's digital landscape, web applications face escalating threats from cyberattacks, encompassing both web application assaults and malicious bot activities. Distrelec, a leading European distributor, specializes in technical components, automation, measurement technology, IT and accessories. With their expanding customer base and online footprint, they found themselves particularly vulnerable to web application threats. And because they rely so heavily on their online presence, even a brief disruption could have a major impact on sales and customer trust. Recognizing the need for robust protection, Distrelec turned to Radware, a top-tier provider of cybersecurity and application delivery solutions. Radware's web application firewall (WAF) and bot management solutions presented a comprehensive security approach. This case study delves into how Distrelec successfully integrated these offerings to fortify their web application security.

Challenges

Distrelec encountered several challenges related to web application security and bot management:

1. **Web Application Attacks —** The company's web applications were vulnerable to a range of attacks, including SQL injection, cross-site scripting (XSS) and other common web application vulnerabilities.
2. **Bot Traffic —** Distrelec faced a significant volume of malicious bot traffic that disrupted operations, scraped product data and attempted fraudulent activities, such as account takeovers and payment fraud.
3. **Solution —** Distrelec needed a solution that could provide continuous protection without affecting legitimate users' access.

Solution

Radware's WAF and Bot Management

Distrelec decided to implement Radware's WAF and bot management solutions to mitigate the identified challenges and strengthen their web application security. Here's how Radware addressed each issue:

1. Web Application Attacks

- **Advanced Attack Detection** — Radware's WAF employed advanced machine-learning algorithms and signature-based protections to detect and block web application attacks in real time.
- **Custom Rule Creation** — Distrelec created custom rules tailored to their specific web applications, ensuring precise protection against known and emerging threats.

2. Bot Traffic

- **Bot Detection and Mitigation** — Radware's Bot Manager accurately identifies and classifies bot traffic, differentiating between good bots (e.g., search engine crawlers) and malicious bots.
- **Bot Mitigation Policies** — Distrelec configured policies to manage bot traffic, including rate limiting, CAPTCHA challenges and blocking, ensuring that only legitimate users could access their site.

Results

After implementing Radware's WAF and bot management solutions, Distrelec experienced significant improvements:

1. **Enhanced Security** — The company's web applications were safeguarded against a wide range of attacks, significantly reducing the risk of data breaches and unauthorized access.
2. **Reduced Bot Traffic** — Malicious bot traffic was drastically reduced, preserving server resources, and preventing data scraping and fraudulent activities.
3. **Improved Performance** — The website's performance improved, resulting in higher customer satisfaction and increased revenue.
4. **Granular Control** — Distrelec had granular control over bot management policies, allowing them to balance security and user experience effectively.
5. **Cost Savings** — By reducing the load on their servers and minimizing the impact of attacks, Distrelec saved on infrastructure costs.

According to **Ben Scholey, CIO of Distrelec Group**,

> *Embarking on the WAF implementation journey was a breeze. Each configuration and deployment went well to create a resilient system. The support from Radware was brilliant and nothing was a problem for them. The solution integrated into our digital landscape to offer better protection, ensuring our digital assets are protected from potential threats."*

Conclusion

Radware provided Distrelec with powerful and flexible WAF and bot management solutions tailored to their specific needs. By effectively mitigating web application attacks and managing bot traffic, Distrelec achieved enhanced security, improved user experience and increased revenue.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.