

WHITE PAPER



PROTECT YOUR APIS DURING PEAK SEASON

Comprehensive Guide for E-commerce



INTRODUCTION

Why API Security Is Essential During Peak Season

During **Black Friday** and the **holiday season**, e-commerce platforms experience a significant surge in traffic and transactions, making **APIs a primary target for cyberattacks**. **APIs, or Application Programming Interfaces**, are the backbone of digital operations, connecting critical services and enabling the key functionalities of a website or e-commerce platform.

However, this also exposes e-commerce businesses to substantial risks, as **unsecured APIs can become entry points for cyberattacks**.

In 2023

60%

of **organizations** reported at least one **API-related breach** in the past two years

[Learn more](#)



Data breaches



Financial losses



Reputational damage

API-related breaches often lead to **data leaks, financial losses and harm to a company's reputation.**

In this white paper, we will explore the **main threats to APIs** during the **peak season** and provide practical recommendations to protect them, ensuring the continuity of your operations.



THE MOST COMMON API THREATS DURING BLACK FRIDAY

During peak season, cyberattacks become more frequent and sophisticated



DDoS ATTACKS

Distributed Denial of Service (DDoS) attacks aim to overload APIs with massive requests, causing downtime or slowdowns. This can lead to lost sales and frustrated customers.



INSUFFICIENT AUTHENTICATION AND AUTHORIZATION

Businesses must provide regular updates on security measures and detailed reports on potential vulnerabilities.



DATA THEFT

There is an obligation to clearly inform users about risks and the implemented protection measures.



MALICIOUS CODE INJECTIONS

Attacks such as SQL Injection and XSS exploit API vulnerabilities to inject malicious code, compromising data security and system integrity.



THE IMPACT OF API ATTACKS

Data, Reputation, and Revenue Losses

API breaches have significant consequences that go beyond the immediate loss of data. **52% of organizations** reported **financial damages** following **API breaches**, with many also experiencing a **decline in trust** from customers and business partners. The most common consequences include:



SALES LOSS DURING BLACK FRIDAY

Every minute of downtime can cost thousands of euros in lost sales, especially during peak holiday moments.



REPUTATIONAL DAMAGE

Breaches involving sensitive data can erode customer trust, leading to long-term customer loss.



FINES AND LEGAL PENALTIES

In cases of data breaches, companies may face heavy fines for non-compliance with data protection regulations, such as GDPR.

BEST PRACTICES TO PROTECT APIS DURING PEAK SEASON

Here are some of the best strategies to safeguard your APIs during the holiday period:

Input Validation

Set limits on the number of requests a single API can handle to reduce the risk of overload and prevent DDoS attacks.



Crowdtesting APIs

Engage a global network of testers to simulate real-world attack scenarios and identify hidden vulnerabilities before hackers can exploit them. Crowdtesting provides comprehensive insights into your operational weaknesses.



Rate Limiting

Set limits on the number of requests that can be made to a single API to minimize overload risks and prevent DDoS attacks.



Continuous Monitoring

Implement real-time monitoring solutions to detect anomalies or active attacks. This allows for swift intervention when threats arise.



Strong Authentication

Use advanced authentication protocols like OAuth and two-factor authentication (2FA). Ensure that only authorized users can access your APIs, protecting sensitive data.





THE ROLE OF CROWDTESTING IN API SECURITY

Test Your E-commerce in Real Conditions to Uncover Hidden Vulnerabilities

Crowdtesting is an effective strategy for **testing API security** in real-world conditions. During events like **Black Friday**, where **increased traffic** can expose **security flaws**, crowdtesting helps identify hidden vulnerabilities and evaluate the effectiveness of defenses against large-scale attacks.



SIMULATING LARGE-SCALE ATTACKS

Globally distributed testers simulate DDoS attacks, data theft, and malicious authentications to assess the resilience of APIs.



IDENTIFYING HIDDEN VULNERABILITIES

By testing APIs under real-world conditions, you can uncover weaknesses that traditional internal tests might miss.



PREVENTING COSTLY DOWNTIME

Minimize the risk of downtime or slowdowns, ensuring your APIs perform optimally during peak periods.



PROTECT YOUR E-COMMERCE AND APIS DURING BLACK FRIDAY

APIs are critical to the success of e-commerce operations, but their security cannot be overlooked.

With **increased risks** during **peak season**, it's essential to take proactive measures to prevent attacks and ensure operational continuity.

Download our comprehensive guide now and discover how UNGUESS can help you effectively test and secure your APIs!

Don't wait any longer

Protect your people and your business now!

Learn more about **UNGUESS Security**.

[BOOK A DEMO](#)