CEQUENCE

Case Study

Canada’s Largest Pizza Chain Moved from Reactive to Proactive API Protection with Cequence

Security Team Detects and Blocks Cyber-Campaigns That Target Their APIs

Canada’s largest and most iconic pizza chain has been in business for over 50 years. With over 750 locations across Canada and annual revenue of over $750 million dollars it is a premier fast food company delivering pizza to a market of over 38 million Canadians nationwide. World-wide, this pizza chain would land itself within the top ten pizza chains in terms of overall revenue.

This nationwide pizza-chain accepts orders via a mobile app, a 1-800 number, and brick and mortar stores. Pizza lovers across Canada can use a rewards program to redeem points and gain access to special promotions. All orders, regardless of the method, are routed to a cloud-deployed order fulfillment application for processing. This application leveraged application programming interfaces (APIs) to ensure an efficient and smooth experience for order requests and rewards processing.

Driven by the pandemic, 2020 saw a dramatic uptick in web and mobile traffic at this pizza chain, some of which were malicious. Threat actors were executing automated credential stuffing attacks impacting the web performance and the user experience. The security team would immediately respond by performing root-cause analysis to determine the severity and plan of action to repel the attacks. The team needed a security partner to help them move from being reactive to proactive.

The Results

Cequence Enables Proactive Protection to Automatically Detect and Block Cyber-Campaigns

After implementing the Cequence Unified API Protection solution, the company was more proactive in their security approach. They were now able to automatically detect and block cyber-campaigns that targeted their mission-critical pizza ordering and rewards program APIs.

They were able to do the following:

- **Ensure a positive user experience:** By proactively uncovering and blocking volumetric credential stuffing attacks, the website and mobile application performed as designed, giving hungry pizza lovers rapid access to their favorite pizza.
- **Stop potential fraud:** Blocking credential stuffing brought the added benefit of preventing account compromise and fraudulent purchases, often the secondary goal of a credential stuffing attack.

Customer Profile

Canada’s largest pizza chain with over 750 locations across Canada and annual revenue of over $750 million dollars.

Goals

- ✓ **Establish a partnership** where the pizza chain and API security solution vendor work proactively to uncover and repel attacks.
- ✓ **Use machine learning** to uncover and alert the team as credential stuffing and brute-force attacks happen.
- ✓ **Enable the pizza chain’s security analysts** to move from a reactive to proactive mode, ensuring they stayed ahead of their attackers.

- **Move to a proactive security partnership:** Machine learning models uncover malicious attack patterns, sending alerts to the team and displaying them graphically. The pizza chain's security team, working in collaboration with the Cequence threat management team can quickly respond to attacks before they impact the business.

What They Achieved

Today, Cequence is deployed in the pizza chain's Google Cloud environment, protecting their production web and mobile APIs from automated attacks, resulting in the following benefits:

- **Bandwidth Costs:** Malicious traffic caused by attackers was blocked, helping to reduce bandwidth costs for their cloud-deployed API application. On average, Cequence was able to slash cloud traffic bills by at least 25% within weeks of deployment.
- **Malicious Login Traffic:** Malicious traffic that targeted the application's login API endpoints were mitigated, directly blocking over 575,000 ATO attempted requests. At its peak, this malicious traffic represented over 80% of all login traffic.
- **Legitimate Access:** Prevented over 5,800 ATO attacks that targeted their user accounts, saving over $1.6m in potential account losses.[1]
- **Increased Productivity by 12.5%:** Their security analysts saved an hour a day, providing an improvement of 12.5% in increased productivity.

[1] Based on a $290 account loss per account Javelin Strategy & Research https://www.javelinstrategy.com/research/identity-fraud-digital-age