CEQUENCE

Case Study

# Victoria's Secret Shuts Down Automated Attacks with Cequence

VICTORIA'S SECRET

Victoria's Secret has a large number of brick-and-mortar stores as well as a growing online e-commerce business which has expanded their attack surface and increased the number of cyberattacks targeting their business. While Victoria's Secret had a content delivery network (CDN) and web application firewall (WAF) in place, automated bot attacks were still plaguing their applications and APIs. Automated bot attacks take many forms and are often hard to detect because their traffic may appear to be legitimate users. That led them to Cequence and its unique ability to identify, track, and mitigate automated attacks that masquerade as legitimate traffic.

## Anatomy of a Thwarted Bot Attack

E-commerce companies often rely on reward or loyalty programs to incentivize customer engagement. However, reward programs are also frequent targets for cybercriminals. In one case at Victoria's Secret, attackers created throwaway accounts and purchased items to accrue reward points. They would then spend the reward points on merchandise and then return all the merchandise for cash. By automating the account creation process, attackers could essentially generate free money that could be spent at Victoria's Secret, costing the company money with no legitimate customer engagement. Cequence was able to identify that the attacks had similarities (such as the IP addresses they were coming from, or the type of browser being used, or a combination of such identifiers) and could then block them, eliminating the threats.

## Cequence Protects Victoria's Secret Against

- **Reward code fraud**
- **Credit card stuffing**
- **Account takeover (ATO)**
- **Fake account creation**

## CUSTOMER PROFILE

Victoria's Secret is the largest lingerie retailer in the United States with annual revenue of over US $6 billion. The company is headquartered in Reynoldsburg, Ohio and has over 900 locations around the world and a significant online presence.

## IN 2024,

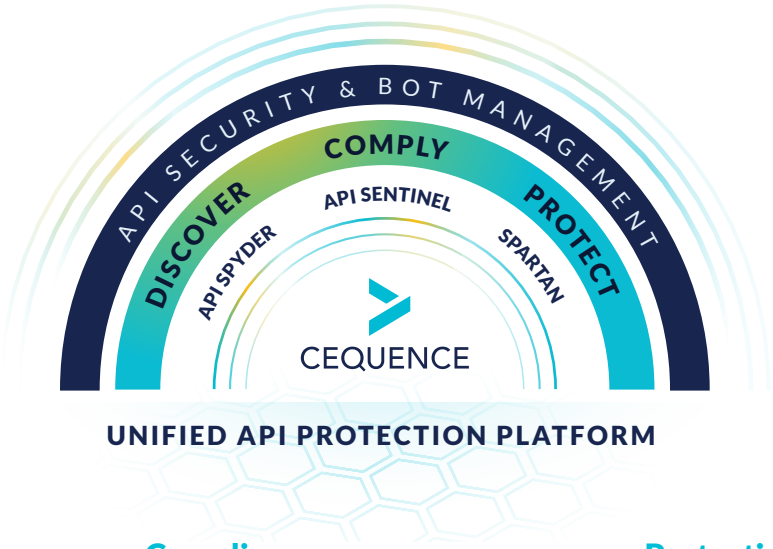
**15%**
of traffic identified as malicious and mitigated

**150M**
user accounts protected from account takeover

**$200K**
per month saved by mitigating a single account takeover event

## The Cequence Solution

Victoria's Secret started out with Cequence Spartan for bot protection but soon deployed the complete Cequence Unified API Protection platform to secure their applications and APIs from data breaches, automated attacks, and fraud.




### Discovery
**with API Spyder**

A SaaS-based discovery tool that provides an attacker's view into an organization's public-facing resources to identify external API hosts, unauthorized hosting providers, and API-specific security issues.

### Compliance
**with API Sentinel**

Discovers, monitors, and tests APIs, assessing a broad range of risks that can lead to compliance or governance issues, data loss, and business disruption.

### Protection
**with Spartan**

Protects web, mobile, and API applications from the full range of bot attacks to prevent data loss, theft, and fraud, eliminating harmful business impacts such as downtime, brand damage, skewed sales analytics, and increased infrastructure costs.

## A Successful Partnership

E-commerce attacks continue to increase in number and sophistication, and enterprises must employ a solution that is able to identify existing and new threats, track them as they morph to avoid detection, and then mitigate them. The Cequence platform enables Victoria's Secret to protect their customers and their business from cyberattacks and focus on their core business.

## About Cequence

Cequence, a pioneer in API security and bot management, is the only solution that delivers Unified API Protection (UAP), uniting discovery, compliance, and protection across all internal, external, and third-party APIs to defend organizations against attacks, business logic abuse, and fraud. The flexible deployment model supports SaaS, on-premises, and hybrid installations, and APIs can be onboarded in less than 15 minutes without requiring any app instrumentation, SDK, or JavaScript integration. Cequence solutions scale to handle the most demanding government, Fortune and Global 500 organizations, securing more than 8 billion daily API interactions and protecting more than 3 billion user accounts. To learn more, visit **www.cequence.ai**.

CEQUENCE

5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai