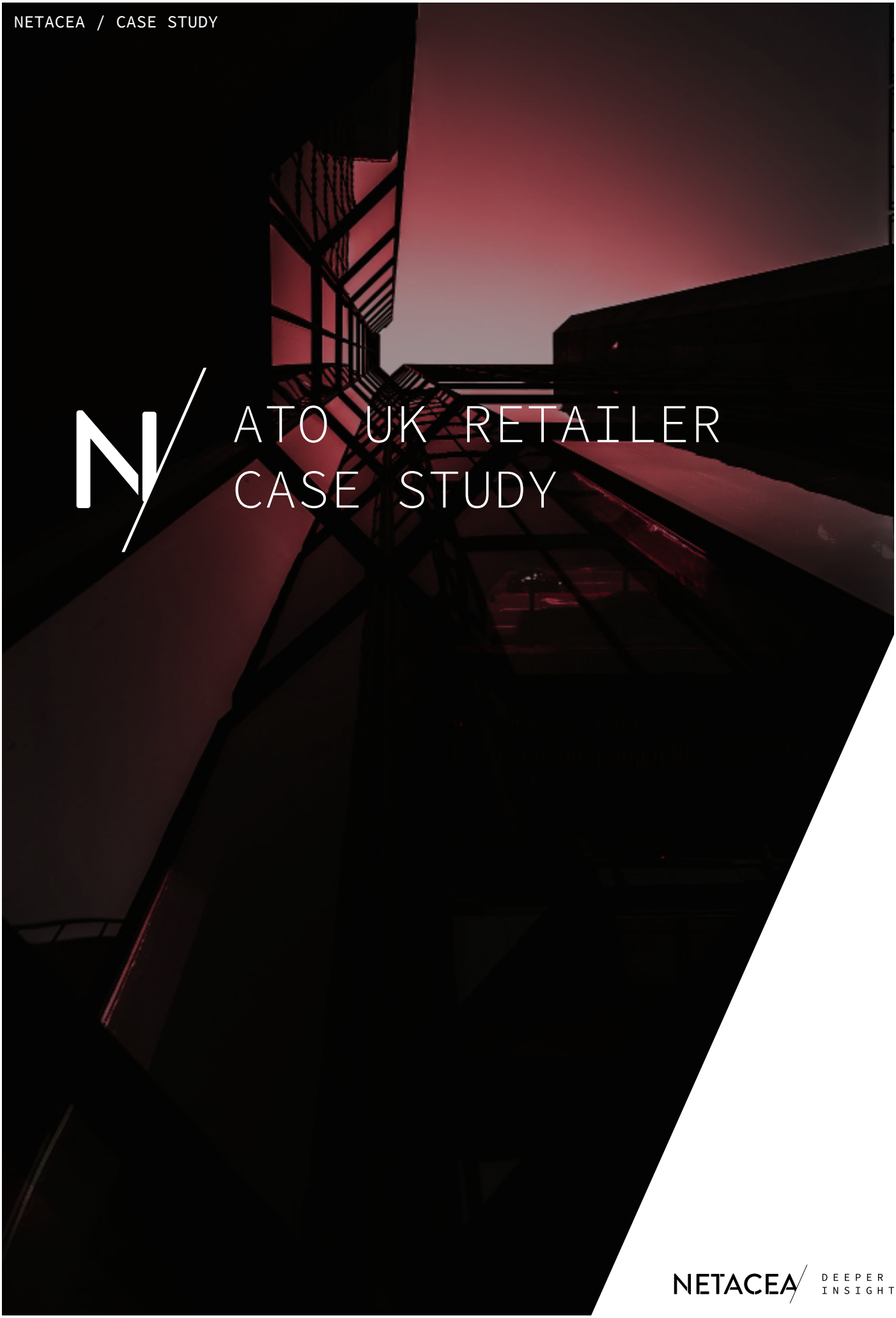

ATO UK RETAILER CASE STUDY

ATO UK RETAILER CASE STUDY

CUSTOMER PROFILE

- One of UK's fastest-growing lifestyle brands
- Operates over 500 stores across 5 continents
- Significant web presence
- Netacea Virtual Waiting Room customer for over 3 years
- Looked to Netacea to assist with managing and mitigating against automated traffic and attacks

RESULTS

- Ensured uptime and availability of customer website during a large-scale account takeover attack
- Rapid implementation of Netacea Bot Management during the attack
- Detection and mitigation of automated account-based attacks
- Continued customer engagement to help detect and prevent further attacks

CLIENT CHALLENGE

The customer has managed their intermittent traffic peaks effectively for several years using Netacea's Virtual Waiting Room product, however a large, unexpected surge in traffic gave the customer cause for concern, prompting them to ask Netacea to investigate.

"We were seeing traffic levels that far exceeded what we'd usually expect during an on-sale event. While we were confident the Netacea Virtual Waiting Room solution would ensure the site continued running under high volumes of traffic, we were concerned about the origin and intent of what else was happening and called on the team to assist us." – E-Commerce Manager

An initial investigation allowed Netacea to determine there was definitely suspicious activity and advised that the Netacea Bot Management solution be implemented. This solution was implemented within minutes and immediately began to reveal the profile of a very large, distributed bot attack, with the machine learning engine further identifying this as an account takeover and credential stuffing attack.

INSTANT ATTACK MITIGATION

This real time identification allowed Netacea to quickly apply appropriate mitigations, within just 6 minutes from initial deployment the machine learning based algorithms had already started blocking attacks from multiple geographical locations and datacentres.

Netacea continued to block the attack for a further two hours until it ceased. In line with typical attack patterns, after a short respite the attack was recommenced from more disparate locations, however all attempts in this second attack were unsuccessful, resulting in the bad actors retiring the attack.

"The Netacea team were incredible throughout the attack, and the days that followed. The speed they implemented and started mitigating was phenomenal, and the information that they we're able to provide us during the investigation with our hosting partner was invaluable." – E-Commerce Manager

GAIN VISIBILITY INTO AUTOMATED TRAFFIC

Most organisations lack clear visibility on the extent of bot activity, but this is a critical first step to be able to devise an effective defence strategy. Netacea provides visibility and insight into bot activity and intent on your website.

Audits are client driven and can focus on either bots in general, or, on key a problem area such as Account abuse, Ad fraud, Price scraping and/or content theft.

FAST FACTS

• $6.5 - $7 Billion lost per year to Account Takeover attacks.

- Forrester

• Successful ATO attacks increase 45% over 2017.

- PYMNTS

THE OUTCOME

Netacea provided the customer with constant analysis of the attack traffic during and after the event to surface as much intelligence as possible. This included the exact geographic locations, datacentres and IP addresses used during the attack. Instantly blocking connection requests from those locations significantly reduced the amount of attack traffic on the website, and soon after this action was complete the attack stopped. A further attack was unsuccessful in impacting the customer website. No further attempts have been seen from this attacker.

Implementation of a site wide Proof of Work to improve the detection of malicious bots on the customer's website.

Fingerprinting of the attack; both successful and non-successful attempts to login were analysed and this data was correlated with the customer's hosting partner.

PROVISION OF TWO MITIGATIONS:

- Captcha served on the login page – implemented in a way that allows it to be activated as a catchall should we see a similar attack in the future.
- Captcha served to a headless browser (as discovered by Netacea's Proof of Work) on the login page. Implemented to be activated on demand.

By blocking the attack in real time, the customer was able to prevent a GDPR data-breach disaster and the negative impact on brand and customer faith that also follows when the event is broadcast in national news.

ABOUT NETACEA

Netacea provide the world's most advanced, multi-tiered Bot Detection and Account Takeover solution which unlike JavaScript-based solutions which are vulnerable to manipulation, Netacea is built on behavioural machine learning.

Our adaptive architecture automatically pre-empts potential bad bot traffic and kicks in-line only when critical conversion or login paths are under threat, due to abnormal behaviour. The reputational analysis identifies malicious bots by using the shared intelligence database to check the digital provenance of the request.

We work in partnership with our enterprise customers to provide the best possible technology integration, allowing you to leverage our machine learning and data science to co-create and engineer the best custom build to meet your business goals.

Netacea's machine learning engine uses behavioural analysis to understand the intent of inbound web traffic. This engine enables Netacea to identify and categorise sophisticated bot behaviour that would typically evade detection, reduce false positives and protect against IP and User Agent rotation.