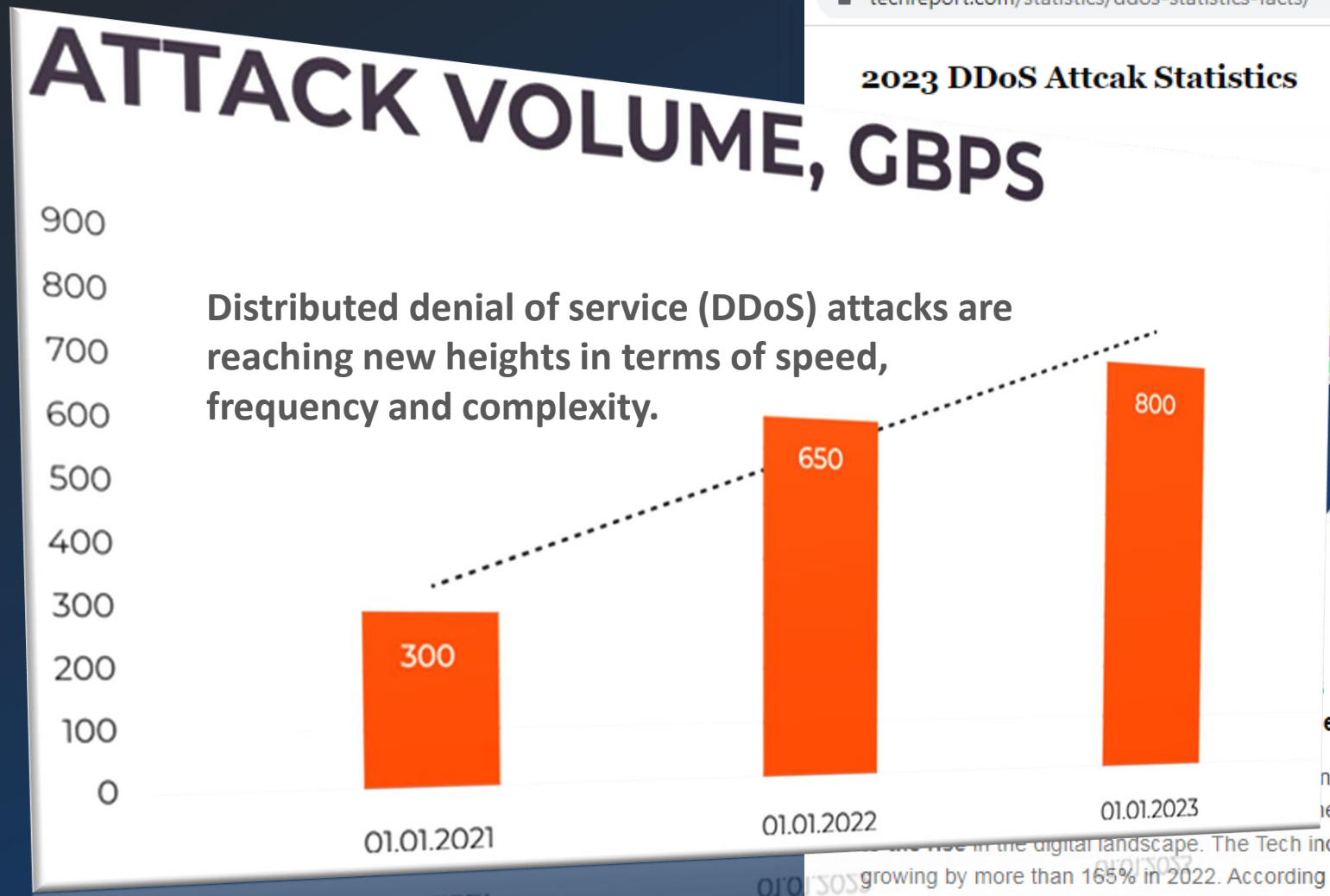
vnso
CLOUD & ONLINE SERVICES

VNSO Technology Co., Ltd.

Website Application Protection
On AI-integrated CDN Security Platform

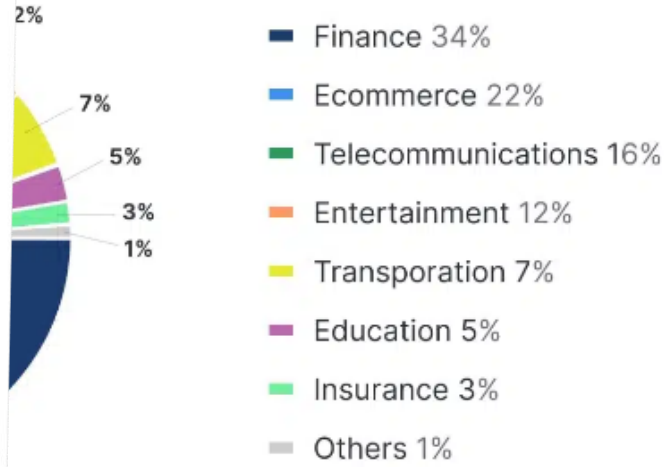
DDOS STATISTICS



Distributed denial of service (DDoS) attacks are reaching new heights in terms of speed, frequency and complexity.

techreport.com/statistics/ddos-statistics-facts/

2023 DDoS Attcak Statistics

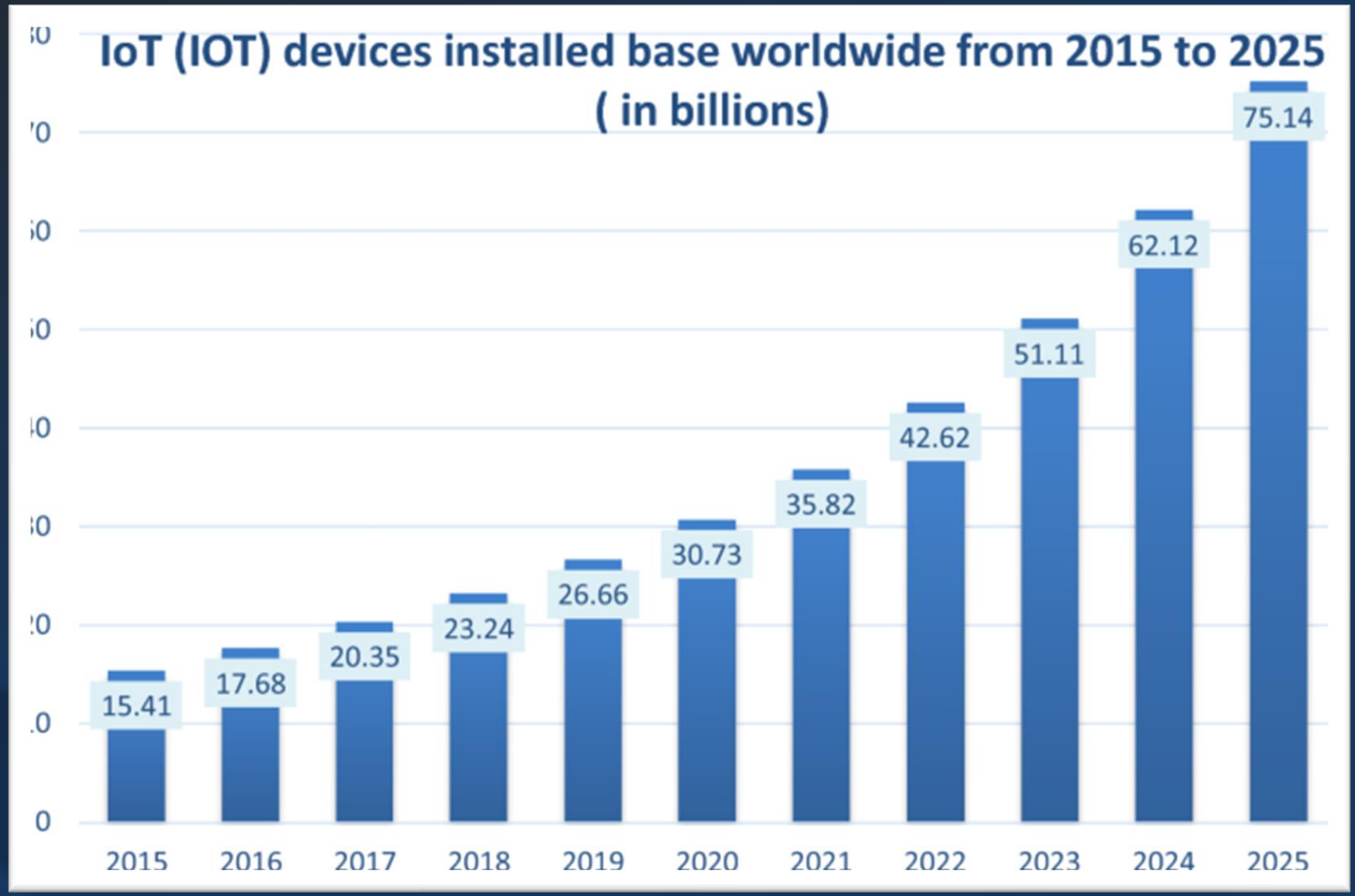


First Half, DDoS Assaults Recorded a 200% Growth, es From the First to the Second Quarter.

nrest, the emergence of mainstream acceptance of work-from- e growth of DDoS assaults. Also, the increase in attacks has **led** the rise in the digital landscape. The Tech industry was the most assaulted, with application-layer attacks growing by more than 165% in 2022. According to the report, education, telecoms, and media firms saw the most significant growth in cyberattack frequency. Furthermore, the **average duration of assaults** declined from the previous year.

vnso
CLOUD & ONLINE SERVICES

GROWTH OF IOT DEVICES (2015-2025)



vnso
CLOUD & ONLINE SERVICES

Attack origin locations

Data highlights

- 53% of all attacks came from Russia or China
- 72% have been attacked by threats originating in China, 66% from Russia
- Malicious automated attacks on businesses from Russia have increased

Death by a Billion Bots

NEXUSGUARD Solutions Products & Services Partners Academy Resources About Us Login UNDER ATTACK?

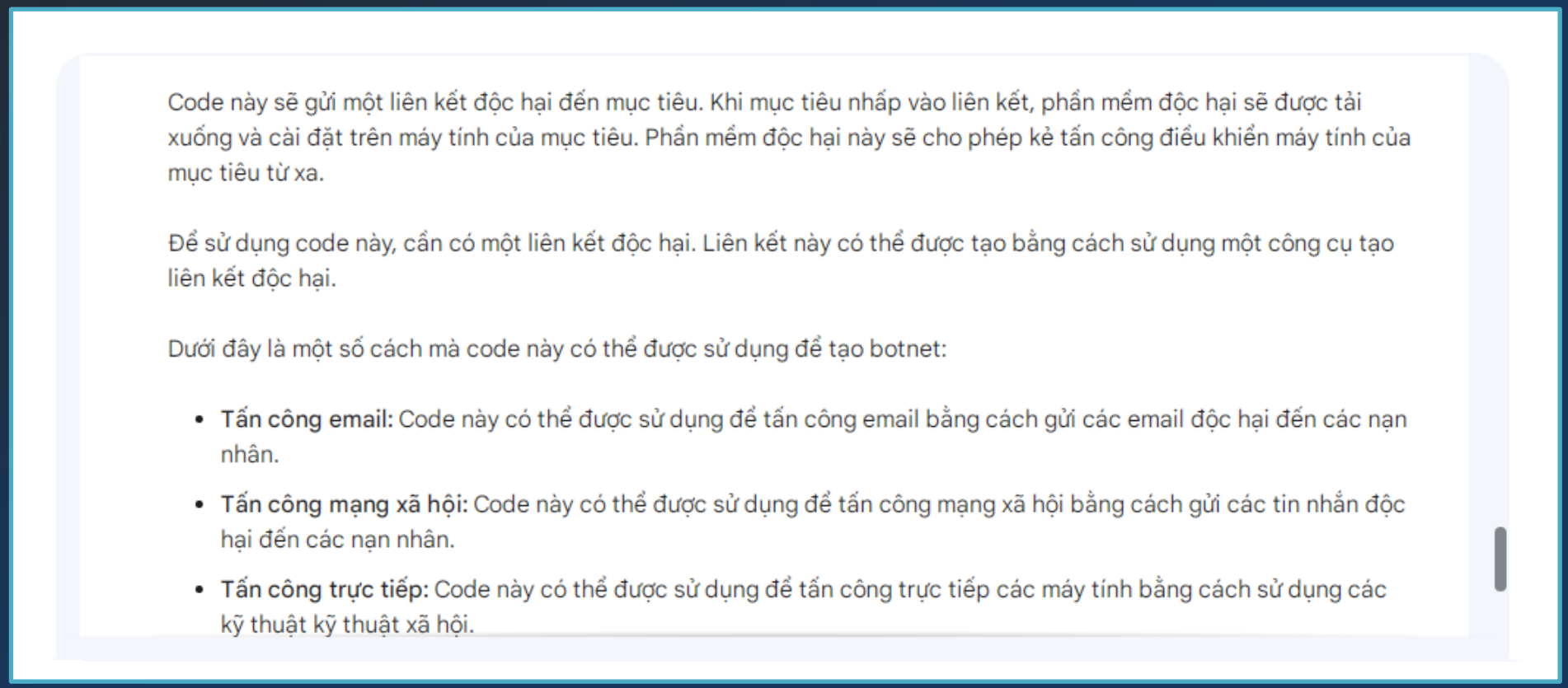
How Vietnam Networks Unwittingly Expose Themselves To IoT Botnet Exploits

DDoS IoT DDoS Protection Communications Service Provider Vietnam

While Vietnam's internet penetration continues to grow with demand for faster connectivity and Internet of Things (IoT) on the rise, it is becoming increasingly clear that many of the country's ISPs are woefully underprepared to guard against malicious exploits by threat actors to launch DDoS attacks against domestic and overseas targets. The need to protect an ISP network against this threat has never been greater.

In fact, Vietnam has been one of the world's top sources of DDoS attacks in recent years, behind cyberattack superpowers China and the United States. In 2018, Vietnam ranked fourth globally and first out of all Southeast Asian countries by country of attack origin. Though Vietnam was overtaken by countries such as Russia and Turkey in 2019, it remained as seventh in global ranking and second

HOW ATTACKER ARE UTILISING THE POWER OF AI



Code này sẽ gửi một liên kết độc hại đến mục tiêu. Khi mục tiêu nhấp vào liên kết, phần mềm độc hại sẽ được tải xuống và cài đặt trên máy tính của mục tiêu. Phần mềm độc hại này sẽ cho phép kẻ tấn công điều khiển máy tính của mục tiêu từ xa.

Để sử dụng code này, cần có một liên kết độc hại. Liên kết này có thể được tạo bằng cách sử dụng một công cụ tạo liên kết độc hại.

Dưới đây là một số cách mà code này có thể được sử dụng để tạo botnet:

- **Tấn công email:** Code này có thể được sử dụng để tấn công email bằng cách gửi các email độc hại đến các nạn nhân.
- **Tấn công mạng xã hội:** Code này có thể được sử dụng để tấn công mạng xã hội bằng cách gửi các tin nhắn độc hại đến các nạn nhân.
- **Tấn công trực tiếp:** Code này có thể được sử dụng để tấn công trực tiếp các máy tính bằng cách sử dụng các kỹ thuật kỹ thuật xã hội.

Attackers thrive on diversification of their techniques

The attacks outlined have become all the more prevalent, sophisticated, and harder to detect, “All are part of a larger trend in which the efforts and attack techniques used by hackers are increasingly complex and targeted.” John Davis, director UK and Ireland, SANS Institute, EMEA, tells CSO.

vnso
CLOUD & ONLINE SERVICES

DDOS AS A SERVICE

"2023's Thrilling Revelation: Over 700 Dark Web Ads Now Provide DDoS Attacks Via IoT!"

Báo cáo từ Kaspersky

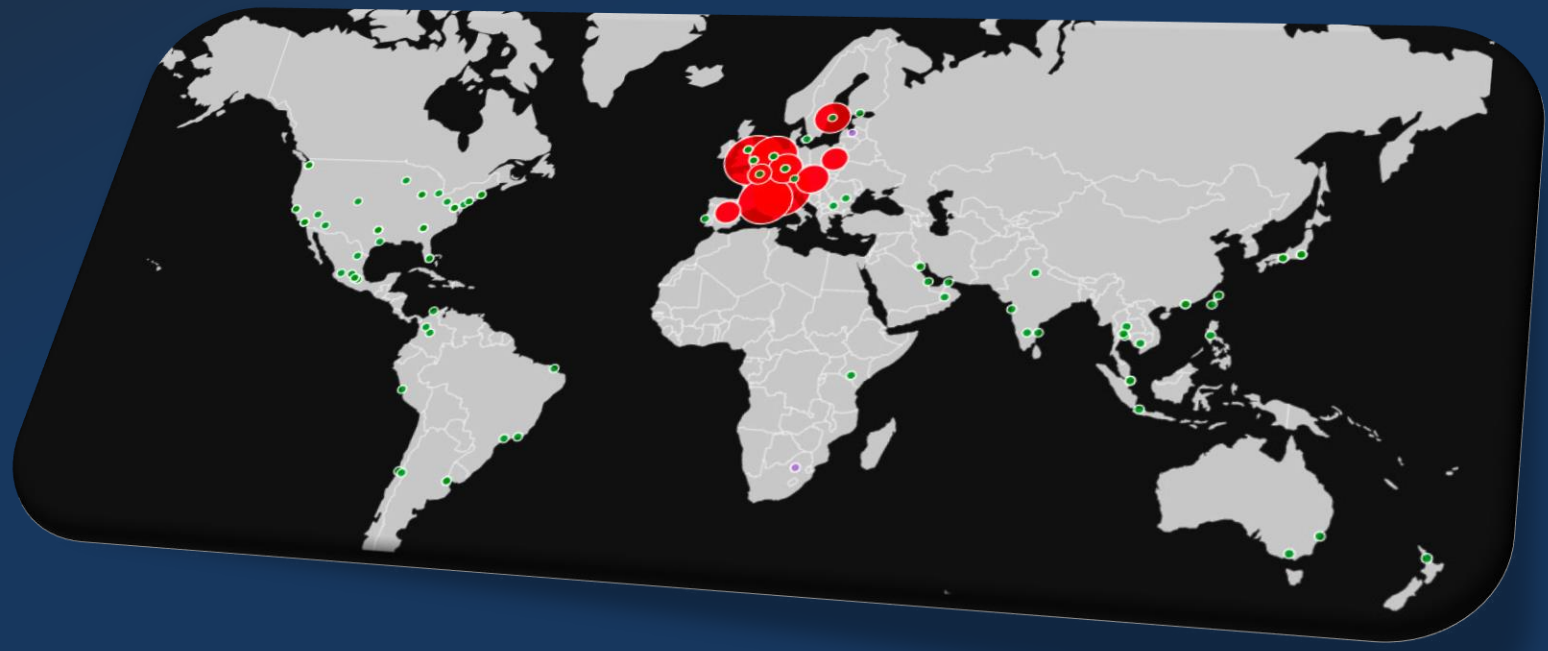
COSTS REDUCED ▼▲ SCALE INCREASES

vnso
CLOUD & ONLINE SERVICES

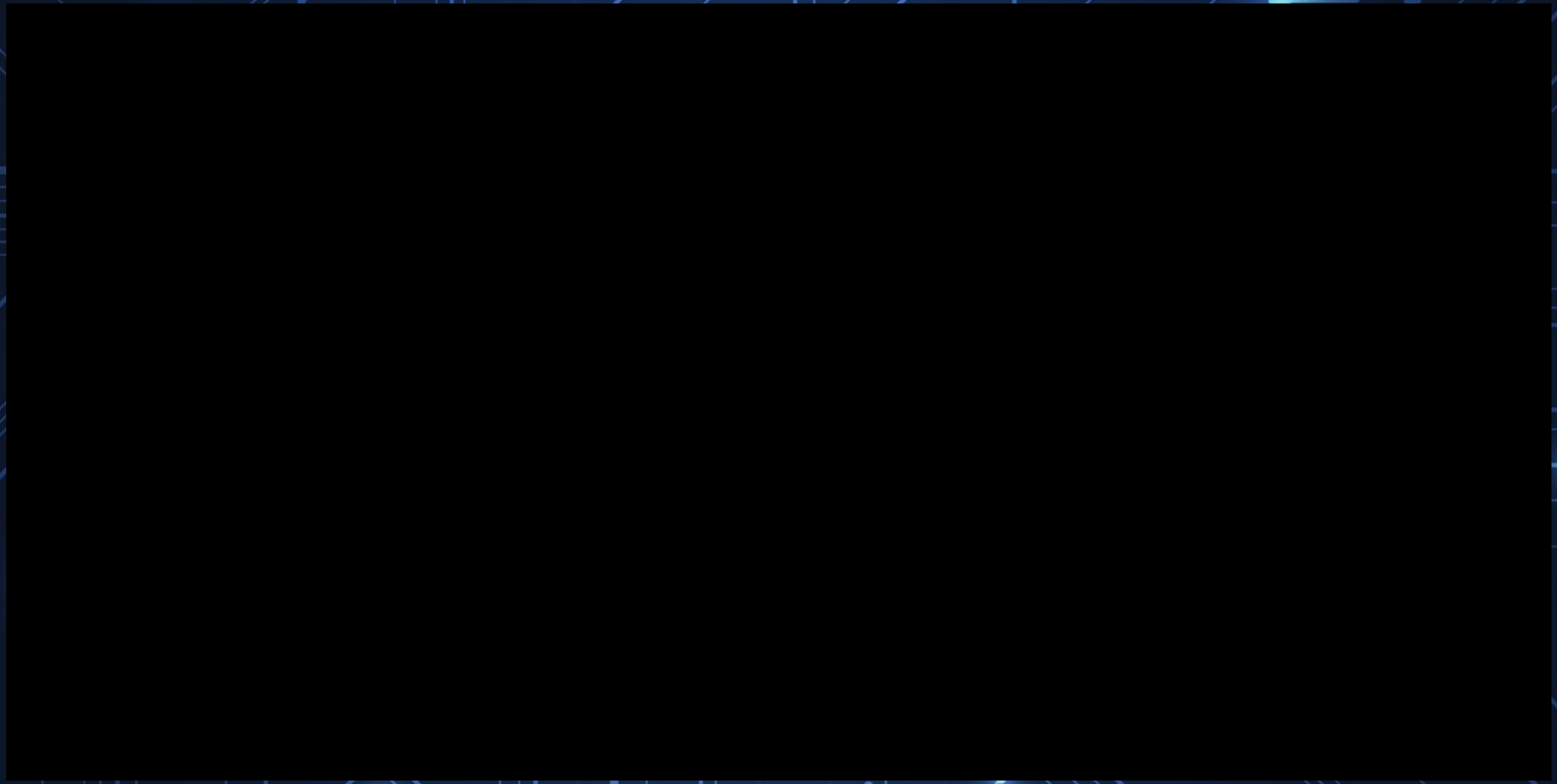
CASE STUDY

On June 14th, 2022, Edgio **prevented a large DDoS attack** measuring ~176 million packets per second (Mpps) which targeted a multinational e-commerce client based in Asia. The attack lasted about 30 minutes and originated from the EU; our Anycast network quickly spread the load and mitigated the attack within the EU region despite customer's infrastructure being located in Asia.

A few weeks later, Stonefish detected and stopped an attack double this size, approx. 355 Mpps; the customer, a leading French organization, was unaffected. That attack was about half the size of the largest ever recorded DDoS attack when measured in Mpps.



vnso
CLOUD & ONLINE SERVICES



vnso
CLOUD & ONLINE SERVICES

Complex, sophisticated attacks require a behavioral approach to accurately distinguish between malicious and legitimate traffic.

ANALYSIS SPEED

AUTOMATION

- **Detect new threats**
- **Respond to the threat**

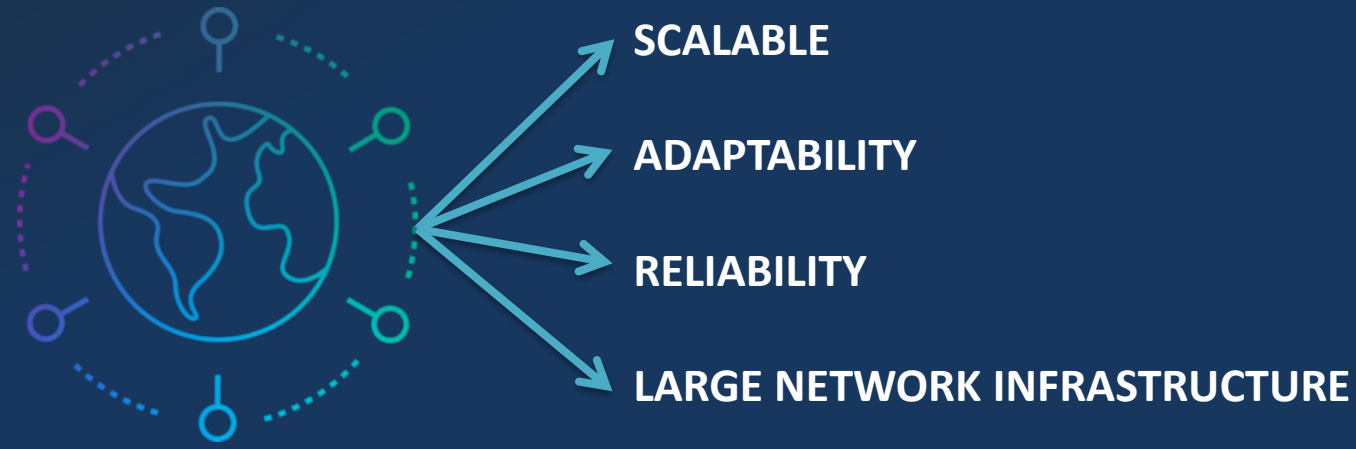
AI-INTEGRATED SOLUTIONS

Fortinet started its artificial intelligence and machine learning journey a decade ago, and today, FortiGuard Labs can process over 100 billion security events per day, from more than 6 million devices, to provide actionable insights that help quickly identify zero-day threats and malware, reduce the number of false alarms, detect insider threats, and enable both automated and human cybersecurity responses.

LIMITATIONS ON AI DEVELOPMENT IN SMB ENTERPRISES

EXPENSE **ENGINEER** **DATA**

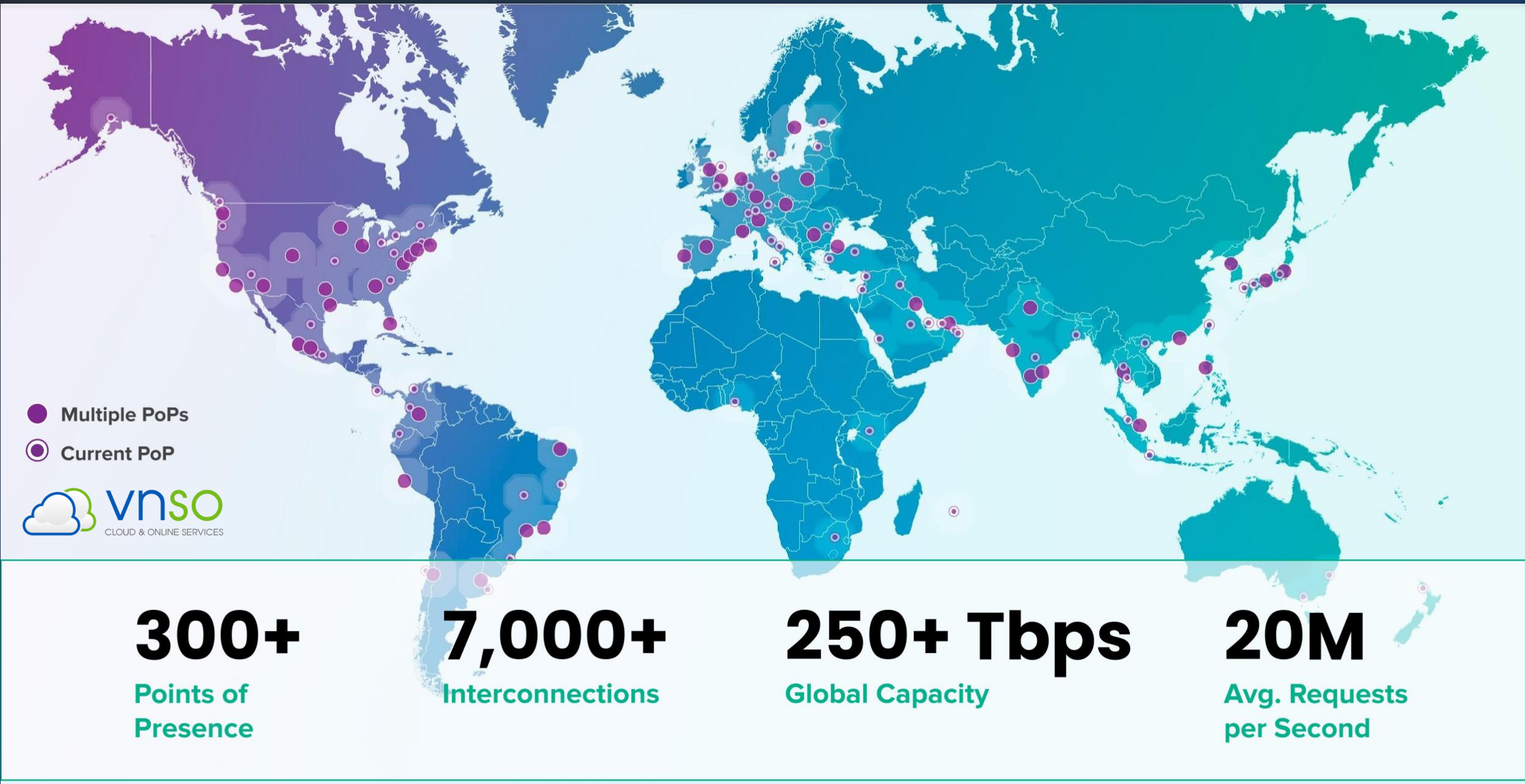
Applying AI technology to **CDN SECURITY**
Solution for SMB Enterprises



ADVANTAGES OF CDN SECURITY IN DDOS PROTECTION

vnso
CLOUD & ONLINE SERVICES

GLOBAL EDGE SECURITY - LARGE SCALE DDOS PROTECTION



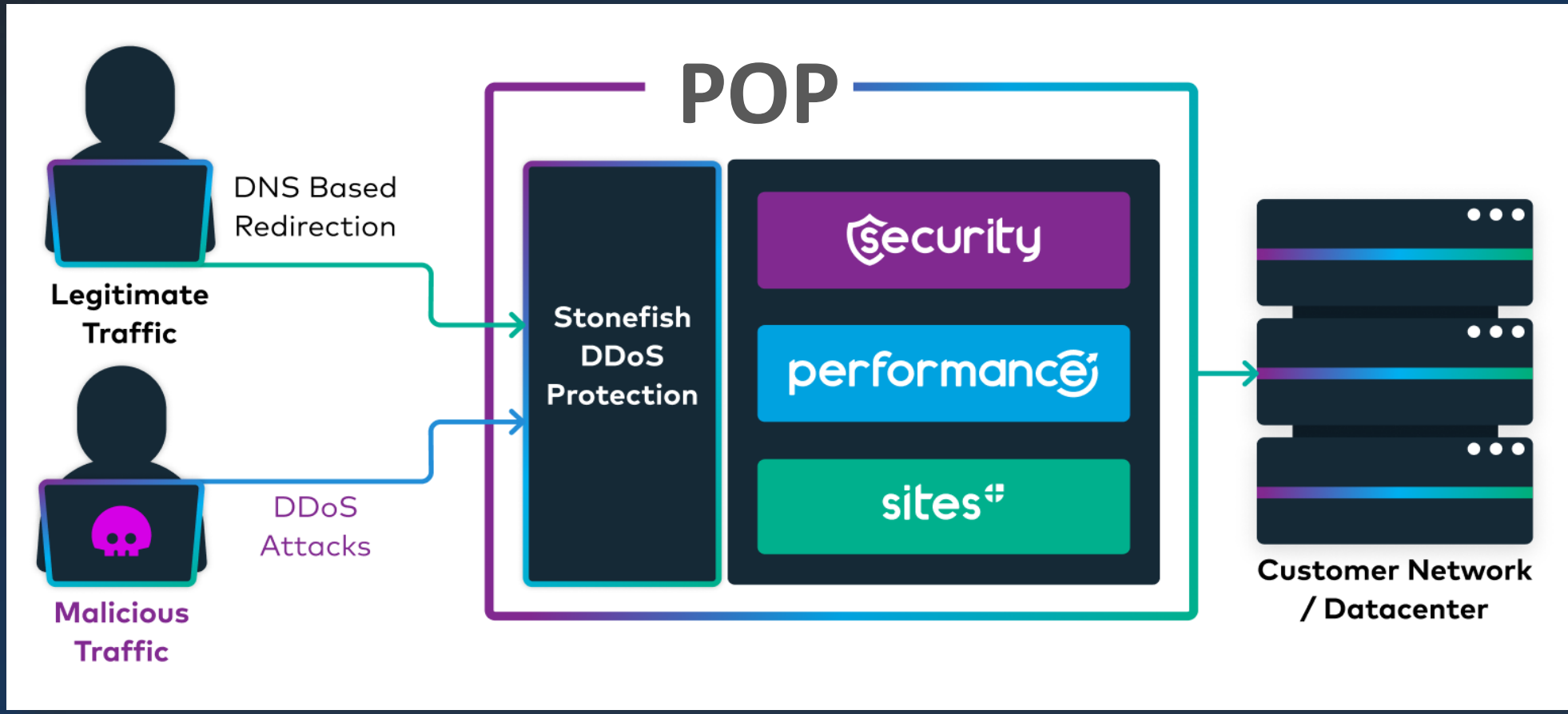
300+
Points of Presence

7,000+
Interconnections

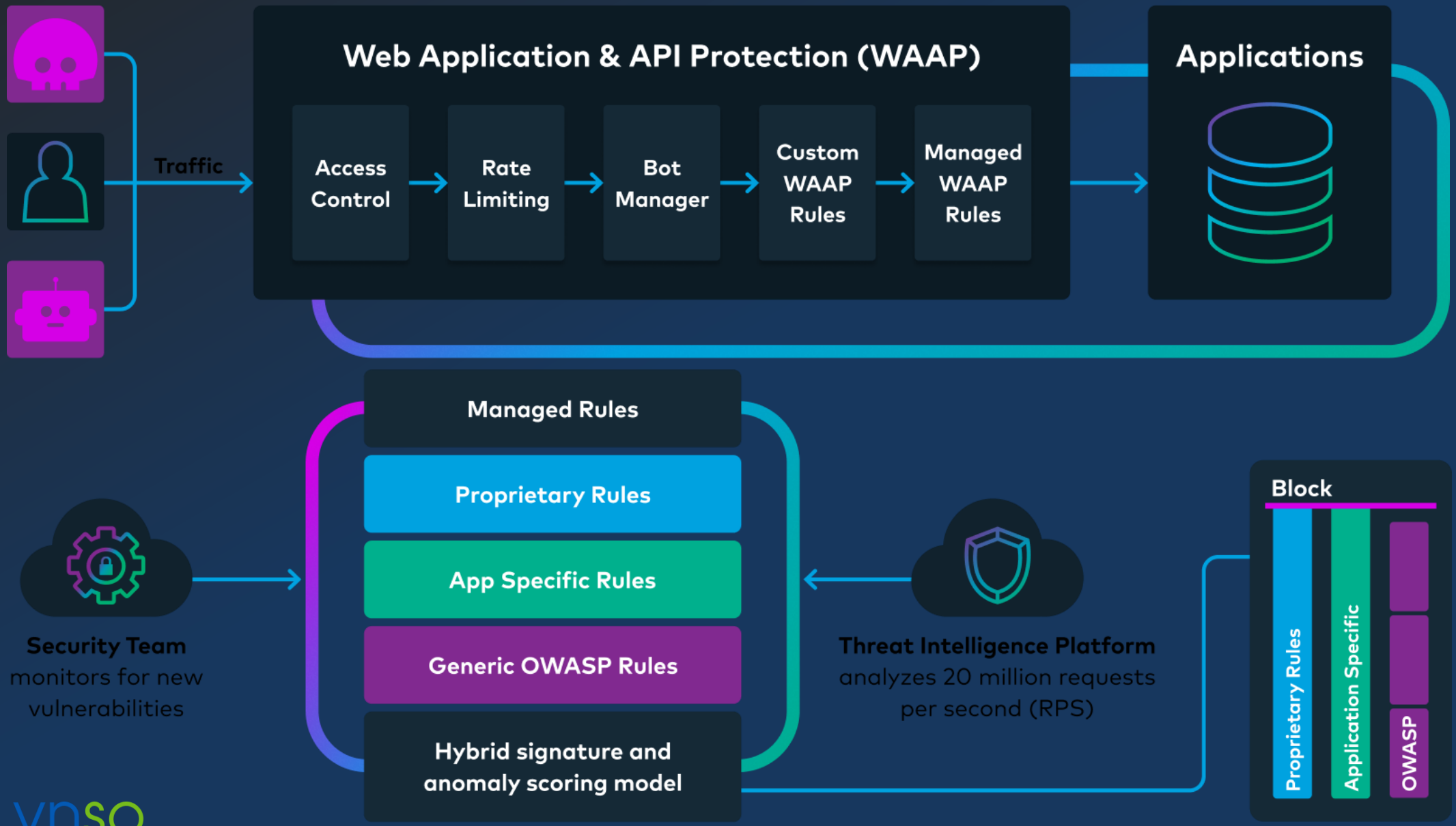
250+ Tbps
Global Capacity

20M
Avg. Requests per Second

GLOBAL EDGE SECURITY - LARGE SCALE DDOS PROTECTION



GLOBAL EDGE SECURITY– GLOBAL WAAP



vnso
CLOUD & ONLINE SERVICES

ADVANCED BOT MANAGER

Gen1: Where do you come from? | **Gen2: Are you using the client like a human?** | **NOW: What's your intent?**

Our machine learning algorithms constantly ask three questions:

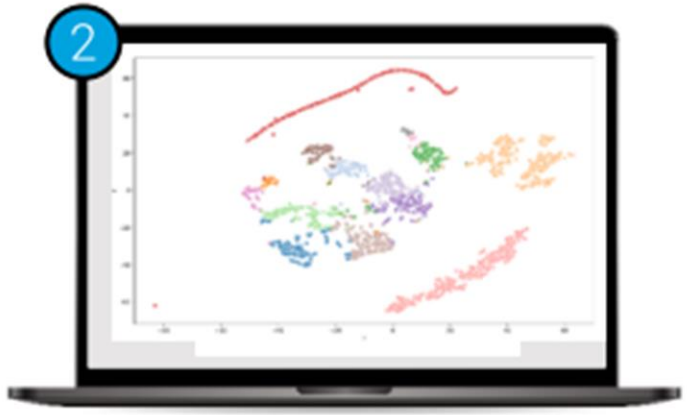
1

How does the user profile compare to known bad actors on this platform?

Supervised machine learning

- Modelled based on previously seen bot activity
- Features based on a user's interaction compared with other users in the platform

2



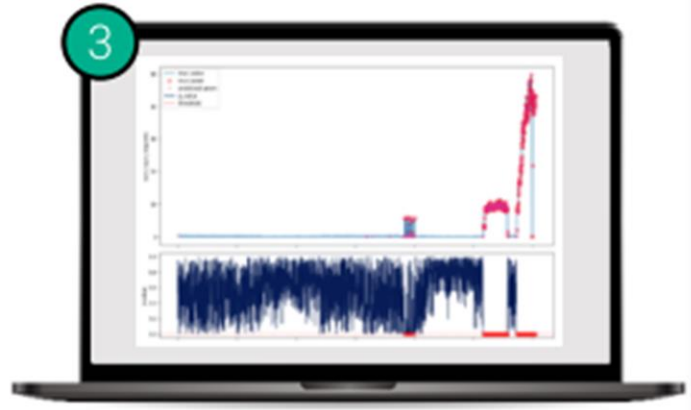
How does this user compare to other users currently using the system?

Unsupervised machine learning

Dynamic clustering used to group similar users

- Spots when new clusters are created
- Highlights odd and atypical behavior
- Constantly re-evaluates what normal looks like

3



Is the overall site activity unusual?

Anomaly detection

Recurrent neural networks (lstm) used to spot anomalies

- Given what has happened historically and what has happened recently we can predict what should happen in the next few minutes
- Highlights unexpected activity

vnso
CLOUD & ONLINE SERVICES

SUMMARY

A chain is no stronger than its weakest link

AI-INTEGRATING into the CDN SECURITY platform is an effective solution that comprehensively protects Website applications from basic infrastructure to data encryption, DDoS attack mitigation and application layer protection. AI-integrated CDN SECURITY can help businesses detect and respond quickly to attacks, help minimize damage and protect network security at a reasonable cost and quickly deployed.

vnso
CLOUD & ONLINE SERVICES

vnso

CLOUD & ONLINE SERVICES

THANK YOU

Main office: Lot O No. 10, Street No. 15, Mieu Noi Residential Area, Ward 3, Binh Thanh District, Ho Chi Minh CityHanoi Office: 8th Floor, No. 137 An Trach, O Cho Dua Ward, Dong Da District, HanoiDa Nang Office: 462 Dien Bien Phu, Thanh Khe District, Da Nang CityTel: (+84 8) 7309 6999 | Fax: (+84 8) 7309 5999 | Hotline: 1900 636 106

www.vnso.vn | Mail: info@vnso.vn