GCORE

eBPF in modern networks

FRNOG 41 Meeting, Paris 2025

PCI DSS COMPLIANT

MADE IN LUXEMBOURG

GUINNESS WORLD RECORDS

Meet you presenter

Andrey Slastenov

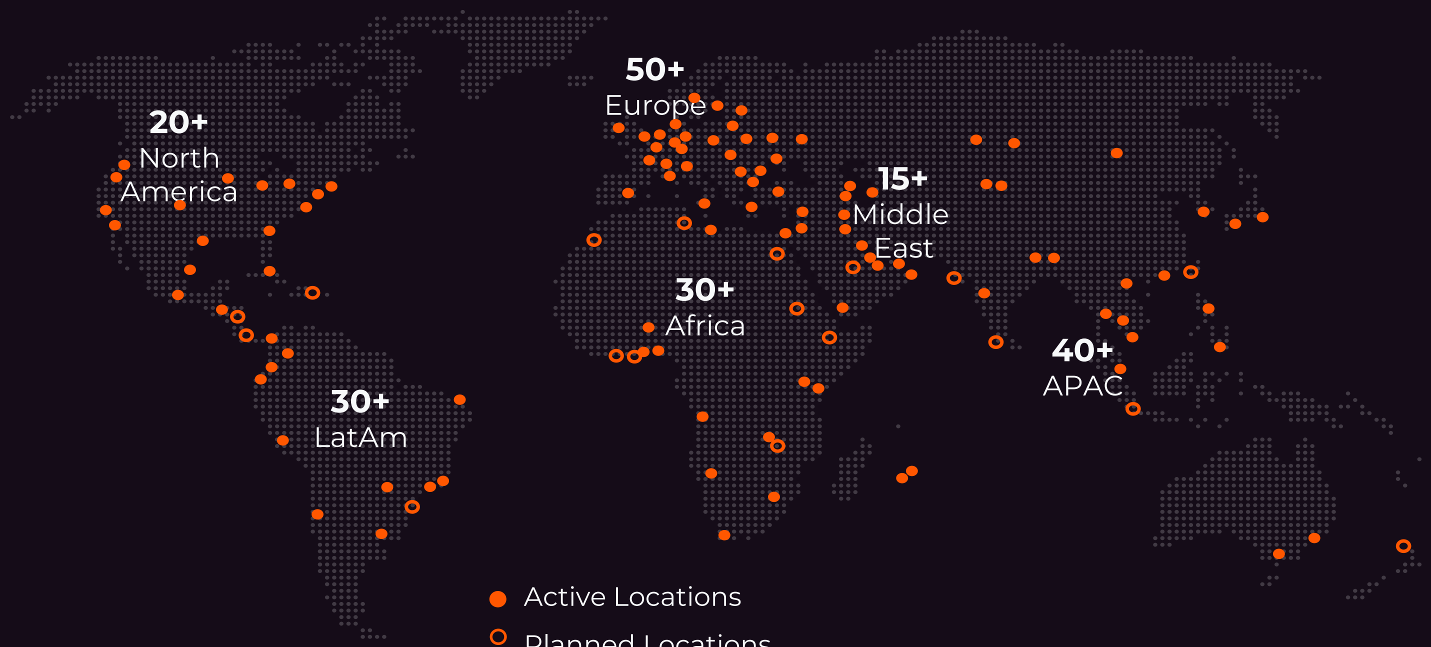
- Security Product Manager at Gcore
- 25 years in telecom industry and security
- A wide range of experiences: routing, MPLS, forensic investigations, conducting security trainings, working on DDoS protection product
- CCIE #19983

01

Gcore’s Evolution and Challenges

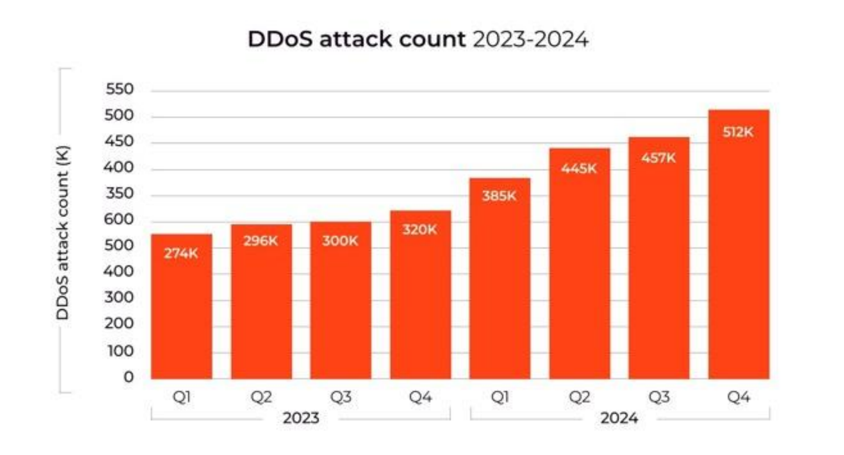
Gcore at glance

GCORE

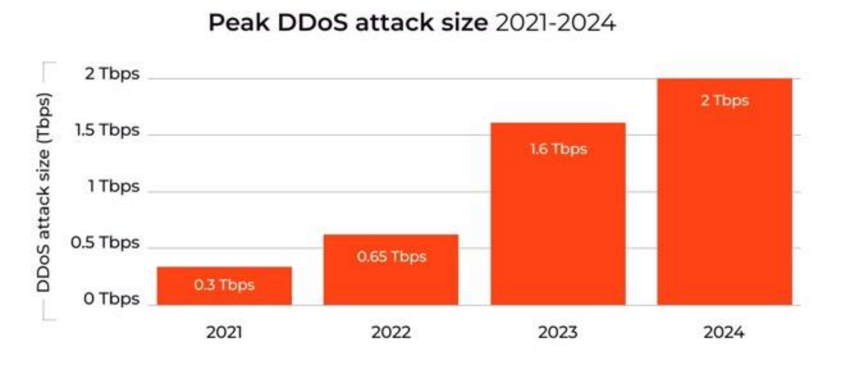


200+ Tbps	Total filtering capacity
180+	PoPs worldwide
14000+	Peering partners
10 Tbit/s	Protected peak load capacity
2 Tbps	Largest mitigated attack
500+	DDoS attacks mitigated daily
30+	Gcore data centers protected

DDoS attacks key trends and insights



DDoS attacks significant growth by 56% YoY



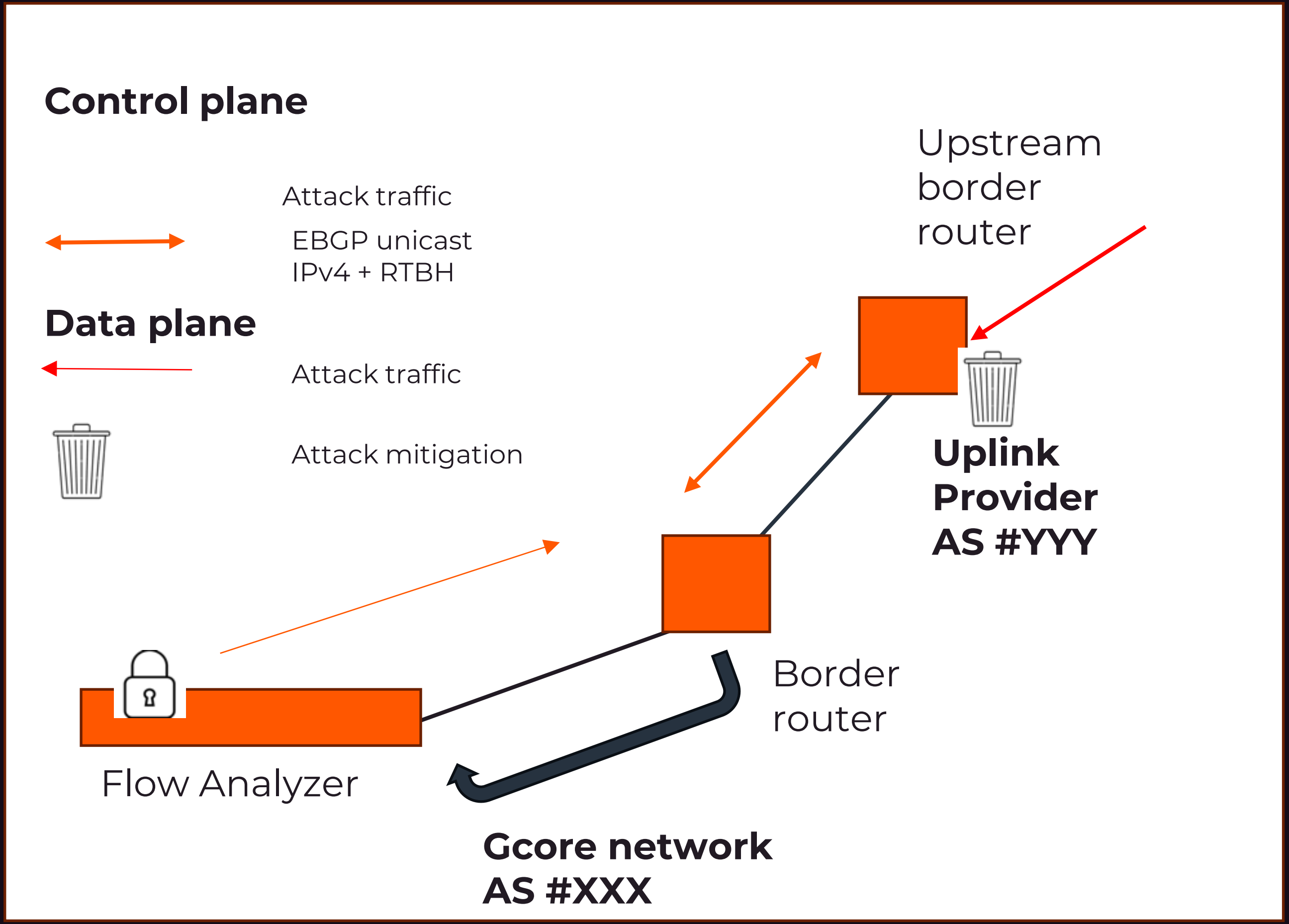
Attacks peak increased by 18%

GCORE

02

Shaping DDoS Solutions: From Basic to Proprietary

Local mitigation options: RTBH & Flow-spec



	RTBH	Flow-spec
Pros	Reduces the impact on your infrastructure by quickly dropping malicious traffic.	Allows you to rate-limit or block traffic targeting a specific host, offering more granular control.
Cons	Blocks all traffic on the attacked host, which can inadvertently cut off legitimate access.	It does not help when the attack targets the application layer, and it does not work efficiently on multi-vector attacks.

Both options should be supported by service providers.

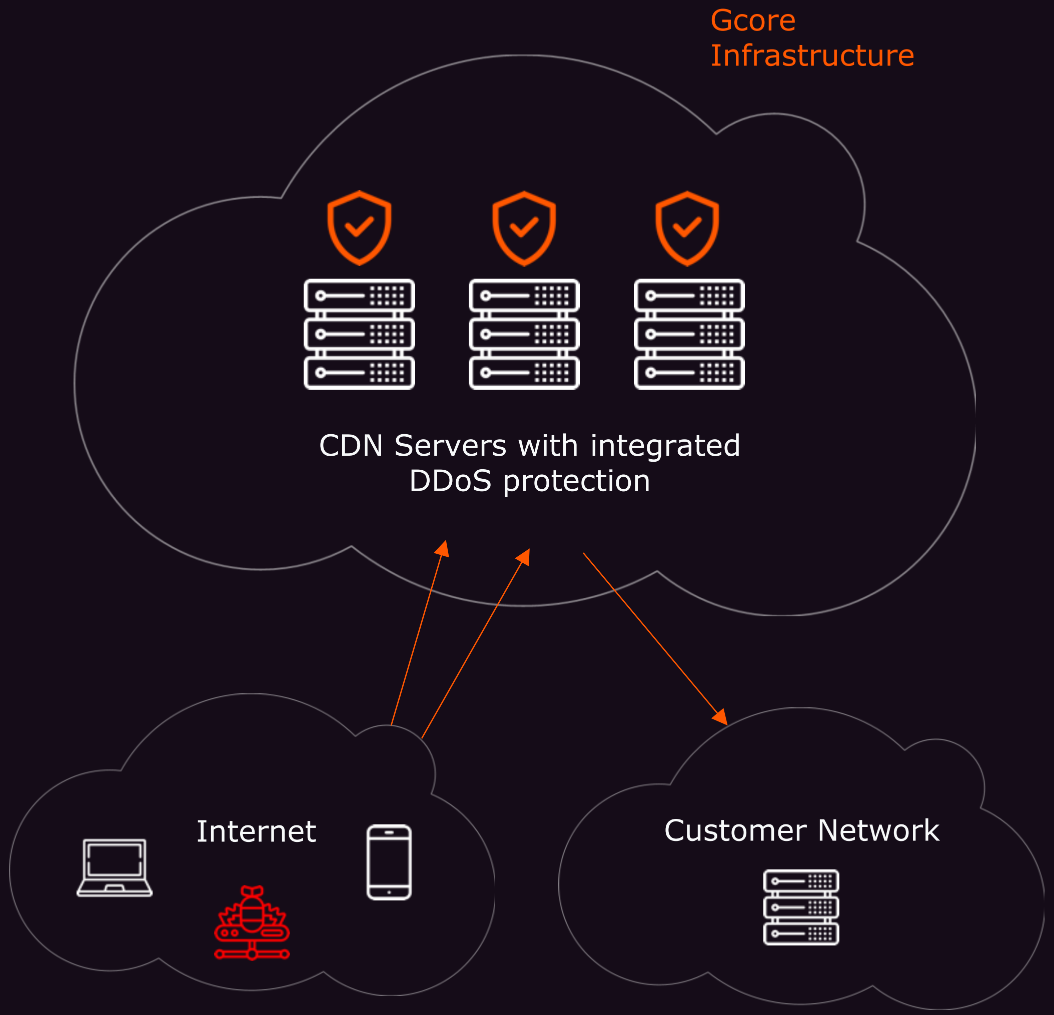
Distributed & resilient mitigation

Distributed servers,
each comes with DDoS protection

Heavy network applications
on the same nodes

Closer to client end-points
(and DDoS generators)

Scalable and Resilent



GCORE

03

Technical Choices: DPDK vs and eBPF

Native vs DPDK vs EBPF Filtering

Native Linux Filtering (e.g., iptables/nftables)	**DPDK**	**eBPF**
Pros: • Simple to use with familiar tools **Cons:** • Much slower (e.g., 1-2 Mpps) due to full network stack processing and context switching.	**Pros:** • Extremely high performance **Cons:** • Requires dedicated CPU cores pegged at 100%, reducing resource efficiency. • Complex setup	**Pros:** • High performance • Integrated into the Linux kernel, easier to deploy alongside existing tools **Cons:** • Slower than DPDK • Limited adoption at that moment

First eBPF Filtering Implementation & Results

Packet Size	Filtered		CPU	Line Rate		Efficiency
	Mpps	Gbps		Mpps	Gbps	
1500	31	383	12%	31	383	100%
512	85	349	52%	85	349	100%
256	144	294	92%	162	340	89%

- 3rd Gen Intel Xeon Scalable processors. Intel® Xeon® Gold processors deliver improved four socket performance, built-in workload acceleration and advanced security technologies for cloud and network workloads.
- 100GbE Intel Ethernet 800 Series Network Adapters. These offer innovative and versatile capabilities that optimize high-performance server workloads with support for up to 100GbE for bandwidth-intensive workloads.
- 2 x Intel Xeon 6348 + 4 x 100Gbps x Intel E810

04

Advanced Filtering Innovations

Enhancing Flexibility with Hyperscan

- **Packet Parsers**
  - Manually written filters
  - Programing work

- **Regular expressions (regex)**
  - Less time to create filters
  - Flexible approach
  - Efficient packet processing

➢ Usage: **Reaction to attacks**

Block DDoS attacks by identified pattern

➢ Usage: **Application-Level Protection**

Application traffic have a strict structure that can be described using regular expressions

Regex + eBPF Performance

Scenario 1. REGEX enable, not match on the pattern, verdict XDP_DROP

Packet Size	Filtered		CPU	Line Rate		Efficiency
	Mpps	Gbps		Mpps	Gbps	
1500	31	383	25%	31	383	100%
512	85	349	65%	85	349	100%
256	118	242	95%	162	340	73%

Scenario 2. REGEX enable, match on the pattern, verdict XDP_TX

Packet Size	Filtered		CPU	Line Rate		Efficiency
	Mpps	Gbps		Mpps	Gbps	
1500	31	383	12%	31	383	100%
512	85	349	52%	85	349	100%
256	94	194	94%	162	340	58%

Source Code

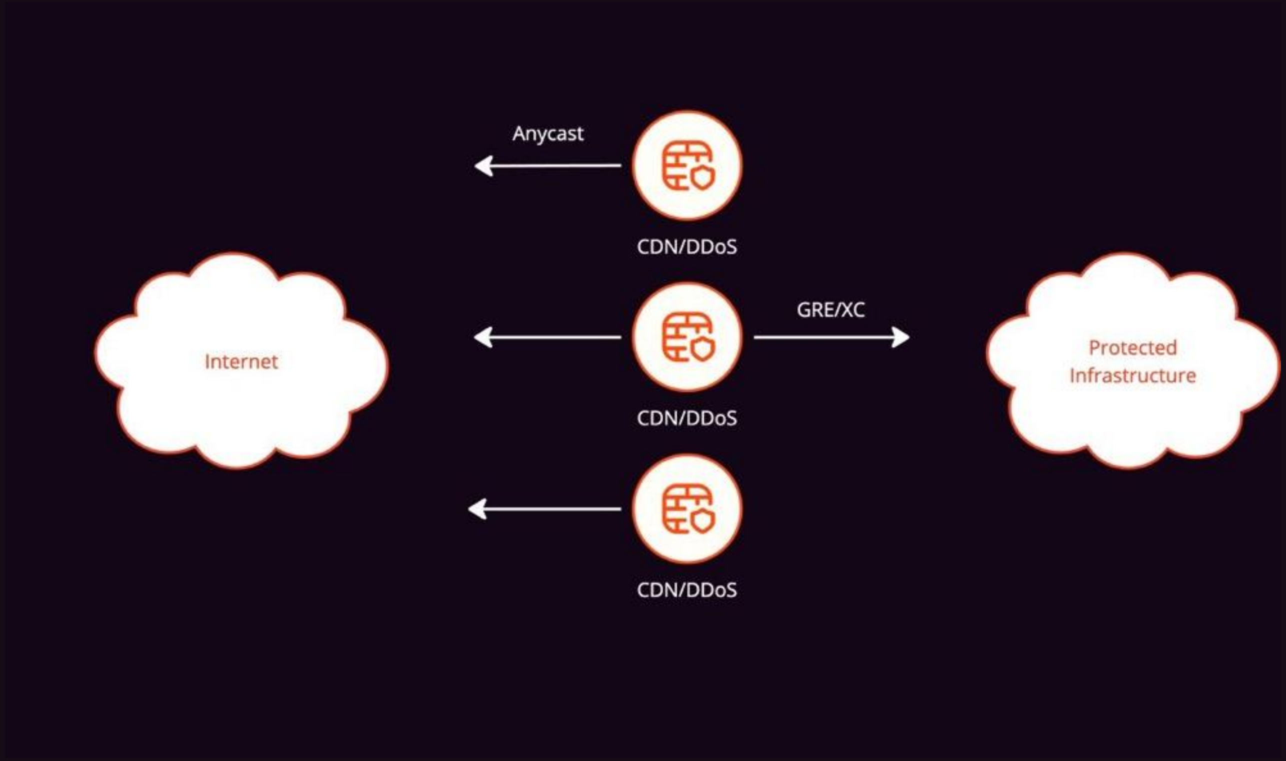
https://github.com/G-Core/linux-regex-module

Anycast/GRE Super Transit

GRE is unidirectional

With eBPF, we can easily add a GRE header

We can spoof the source IP address of tunnel



GCORE

05

Wrap-up

Wrap-up

Scalability for Modern DDoS: Protecting against today’s attacks requires handling millions of packets per second and terabits of traffic through a distributed approach.

Tech-Driven Evolution: Early mitigation challenges paved the way for advanced filtering, using eBPF, Hyperscan, and vendor-neutral strategies for flexibility and speed.

Global Optimization: Anycast, GRE tunneling, tackle unidirectional traffic and ensure efficient load balancing across networks.

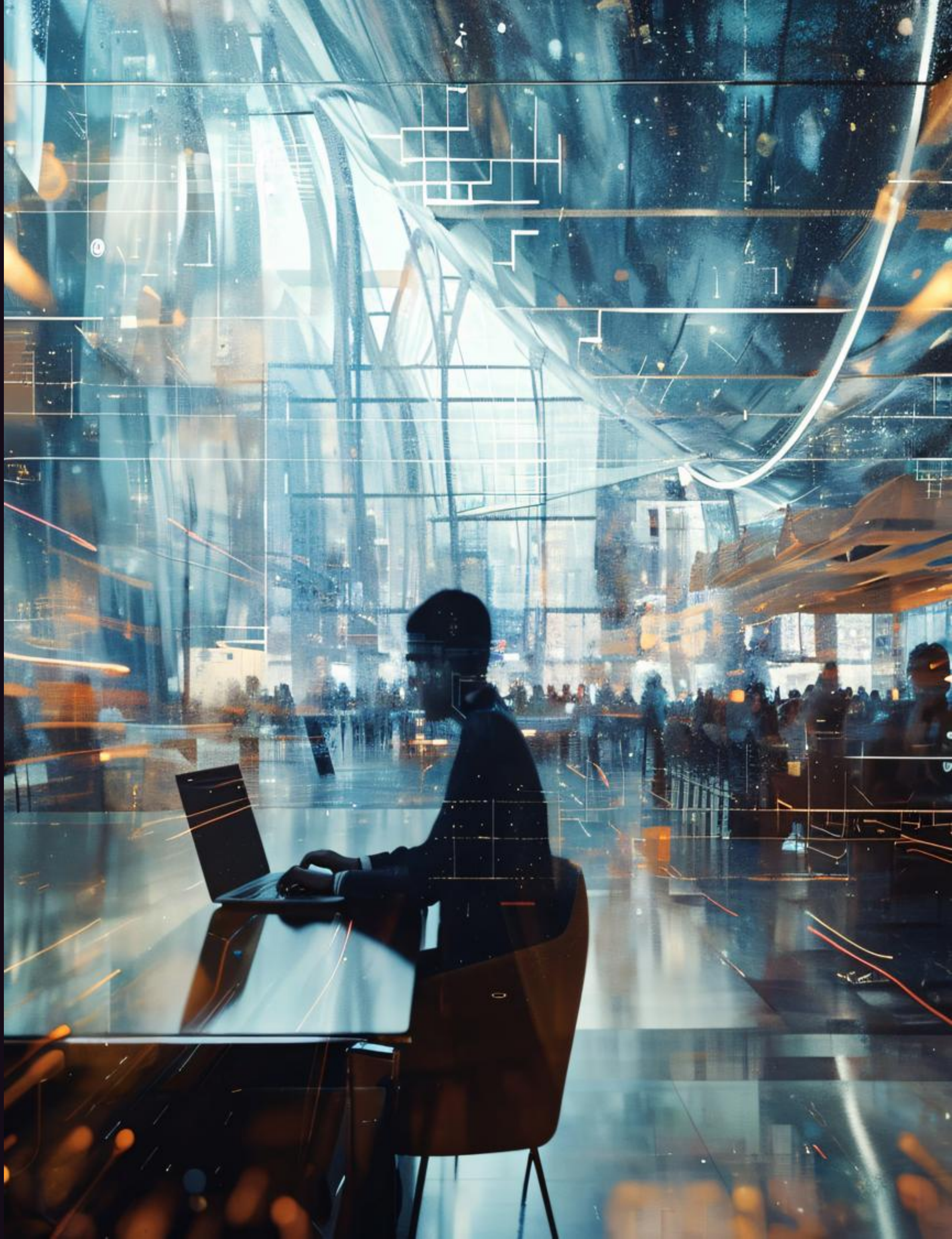
The future of DDoS protection

Increasing sophistication of detection methods

AI integration

Focus on available capacity

Distributed architecture



GCORE

GCORE

Thank you

Stay safe with Gcore

andrey.slastenov@gcore.com

gcore.com