GCORE

Protecting Infrastructure

Protecting servers and web applications: their differences and a comprehensive approach for protection

PCI DSS COMPLIANT

MADE IN LUXEMBOURG

GUINNESS WORLD RECORDS

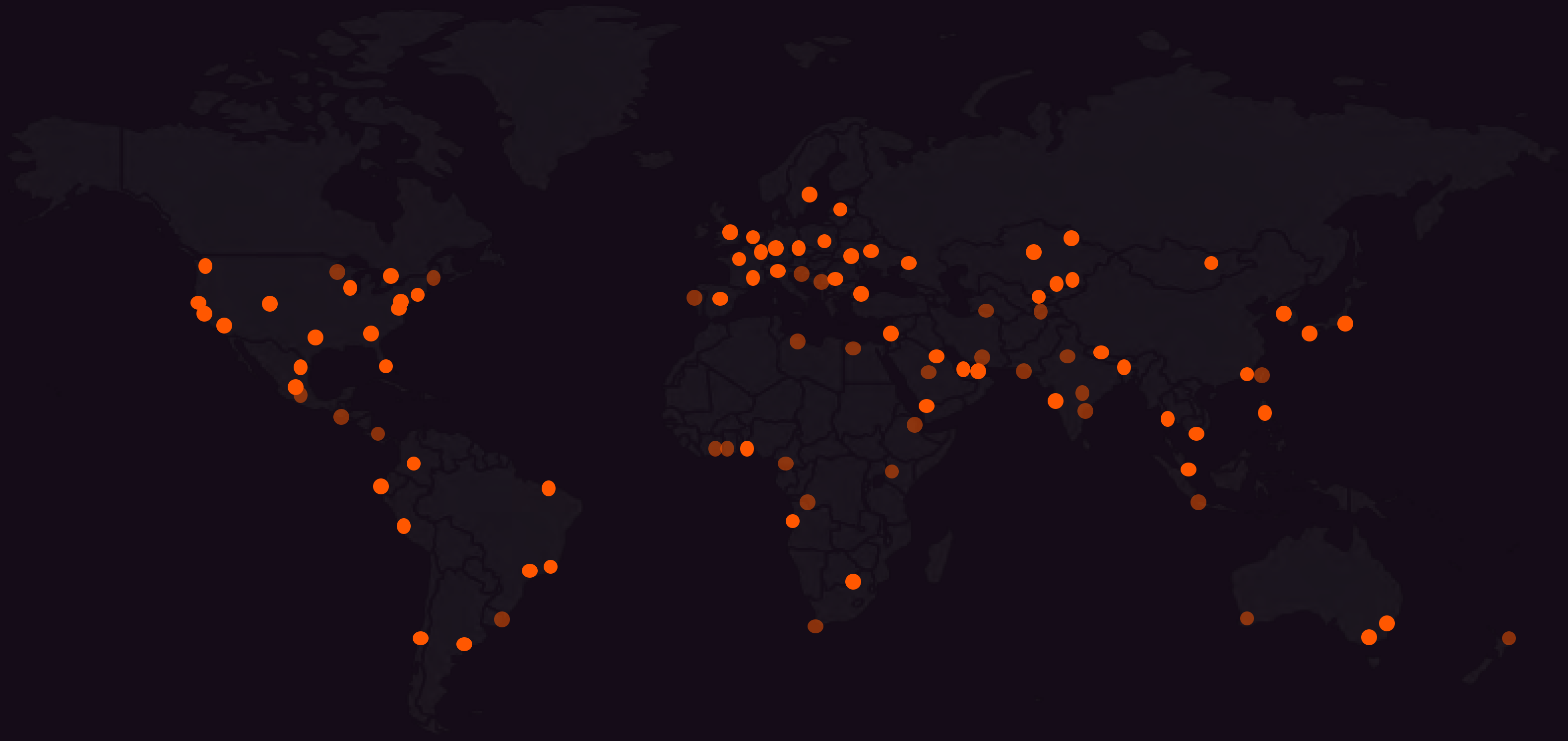
Agenda

1. Gcore's infrastructure
2. What does cybersecurity mean?
3. All about DDoS attacks
4. Protecting your infrastructure with Gcore

01

Gcore's Infrastructure

Gcore at a glance



- ✓ **180+**
  points of presence (PoPs)
- ✓ **50+**
  cloud locations
- ✓ **14,000+**
  peering partners
- ✓ **200+ Tbps**
  network capacity
- ✓ **30 ms**
  average response time worldwide
- ✓ **99.99%**
  SLA

02

What does cybersecurity mean?

What is cybersecurity?

Protecting and Monitoring

Networks

Endpoints

Applications

IAM

Infrastructure

Cyber threats are escalating faster than ever

7.9 Million

DDoS attacks in the first half of 2023, marking a 31% YoY increase. The maximum attack bandwidth reached 800 Gbps in 2023.

201 Million

Attempts made every second to overwhelm a server in one of the most sophisticated web attacks in 2023, setting a new record for the highest volume of attack requests.

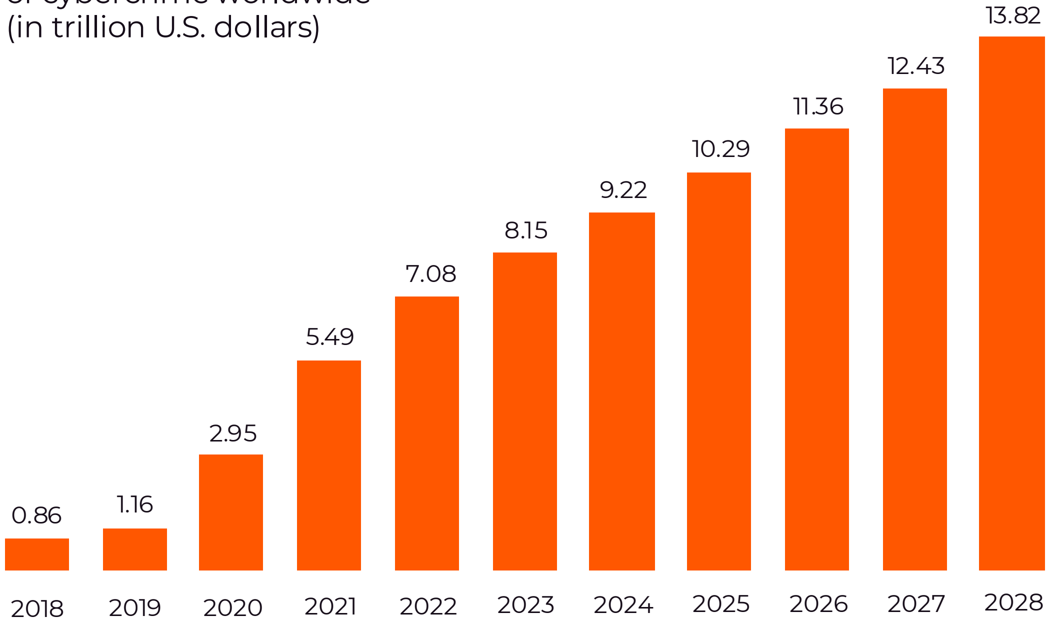
398 Million

Attempts made every second to overwhelm Google Cloud's infrastructure during the largest DDoS attack ever mitigated, peaking in 2022 and setting a new record for attack intensity.

GCORE

Cybercrime expected to skyrocket

Estimated annual cost
of cybercrime worldwide
(in trillion U.S. dollars)



As of Sep. 2023. Data shown is using current exchange rates.
Source: Statista Market Insights

statista

03

All about DDoS Attacks

DDoS attack types

⚠ Volumetric attacks

These attacks are designed to swamp the available bandwidth of their targets, ranging from individual clients to entire data centers. By using a mix of methods like UDP and ICMP flows, as well as amplification strategies, they can block legitimate users from accessing servers and applications.

- UDP flood
- ICMP flood
- IP/ICMP fragmentation
- IPSec flood
- Amplification attacks
- Ping of death

⚠ Connection attacks

Connection attacks exploit network devices or systems that track ongoing connections using finite resources or features. When these internal tables are flooded with excessive connections, new users are barred from making connections. In extreme situations, this overload can cause devices to crash, disrupting connections for all active users.

- SYN flood
- SYN+ACK flood
- ACK flood
- RST flood
- TCP attacks

⚠ Application attacks

These attacks can severely hamper server performance by flooding servers with complex requests, devouring all available CPU and memory resources.

- L7 UDP flood
- L7 TCP flood
- Slowloris
- DNS cache poisoning
- HTTP
- HTTP get/post flood
- Game server attacks

Challenges of DDoS attacks

Real-time protection

- Low latency must be maintained
- Huge attacks occur during critical events
- Security and performance must be balanced

Network code design

- Protocol vulnerabilities
- Decentralized nature of the online games
- Encrypted network code

Evolving threats

- Increasingly complicated attack types
- Botnets are becoming more capable and creating higher volume attacks

High-performance infrastructure

- High bandwidth required for volumetric DDoS attacks
- Mitigation needs high-quality infrastructure with multiple locations

Web application and API protection (WAAP)

Web Application Firewall

Comprehensive protection against vulnerabilities including OWASP Top 10 threat and zero-day attacks.

Bot Management

Identification of legitimate users, good bots, and malicious bots to protect against automated attacks and fraud.

DDoS Protection

Adaptive and behavioral L7 DDoS protection against application-layer attacks of any size.

API Security

Enterprise-grade API discovery and protection to guard against security threats.

Two levels of DDoS protection: both critical for full security

DDoS Protection

Infrastructure DDoS Protection

Objective:
Protects the underlying network infrastructure, including servers, routers, and data centers.

Scope:
Defends against attacks that aim to exhaust network bandwidth or overwhelm the server's resources, affecting the entire network and its ability to handle legitimate traffic.

WAAP DDoS Protection

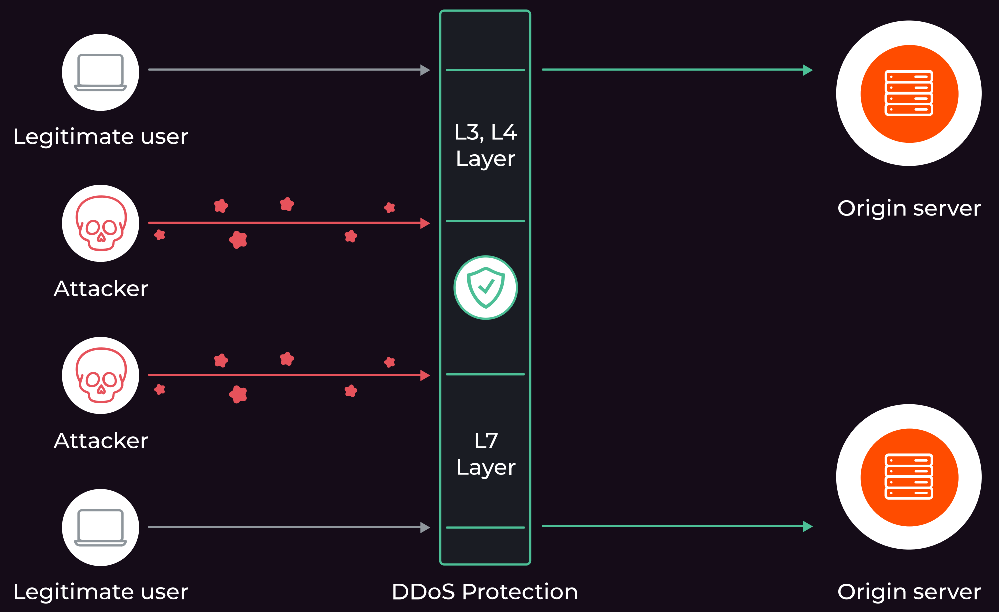
Web Application DDoS Protection

Objective:
Specifically protects web applications such as websites, APIs, and online services.

Focus:
Protects against attacks designed to overwhelm the application layer (Layer 7 of the OSI model), which can include HTTP flood attacks or attacks that exploit application vulnerabilities.

Even a minor DDoS attack can cripple your business

A DDoS attack (distributed denial-of-service) is a series of actions by an attacker designed to fully or partially disable a resource. As a result, users may be unable to access system resources (servers) provided, or their access will be hindered.



- Attackers target both the **L3/L4 (network) layer** and the **L7 (application) layer**.
- Without proper **DDoS protection**, these attacks can bypass defenses.
- Once through, the attacks can **overload the origin server**, disrupting service for legitimate users.

Unsecured businesses face severe consequences

Financial Losses

Direct theft:
Funds stolen from customer accounts.

Fraud:
Unauthorized transactions and purchases.

Reputational Damage

Loss of trust:
Customers lose trust in the business.

Negative publicity:
Bad press from data breaches.

Legal Consequences

Fines and penalties:
Significant fines for non-compliance.

Lawsuits:
Customers may take legal action against the business.

Operational Disruptions

Business interruptions:
Disruption of normal operations.

Increased costs:
Expenses for breach mitigation.

Customer Impact

Identity theft:
Long-term effects of identity theft.

Emotional distress:
Stress from compromised data.

Competitive Disadvantage

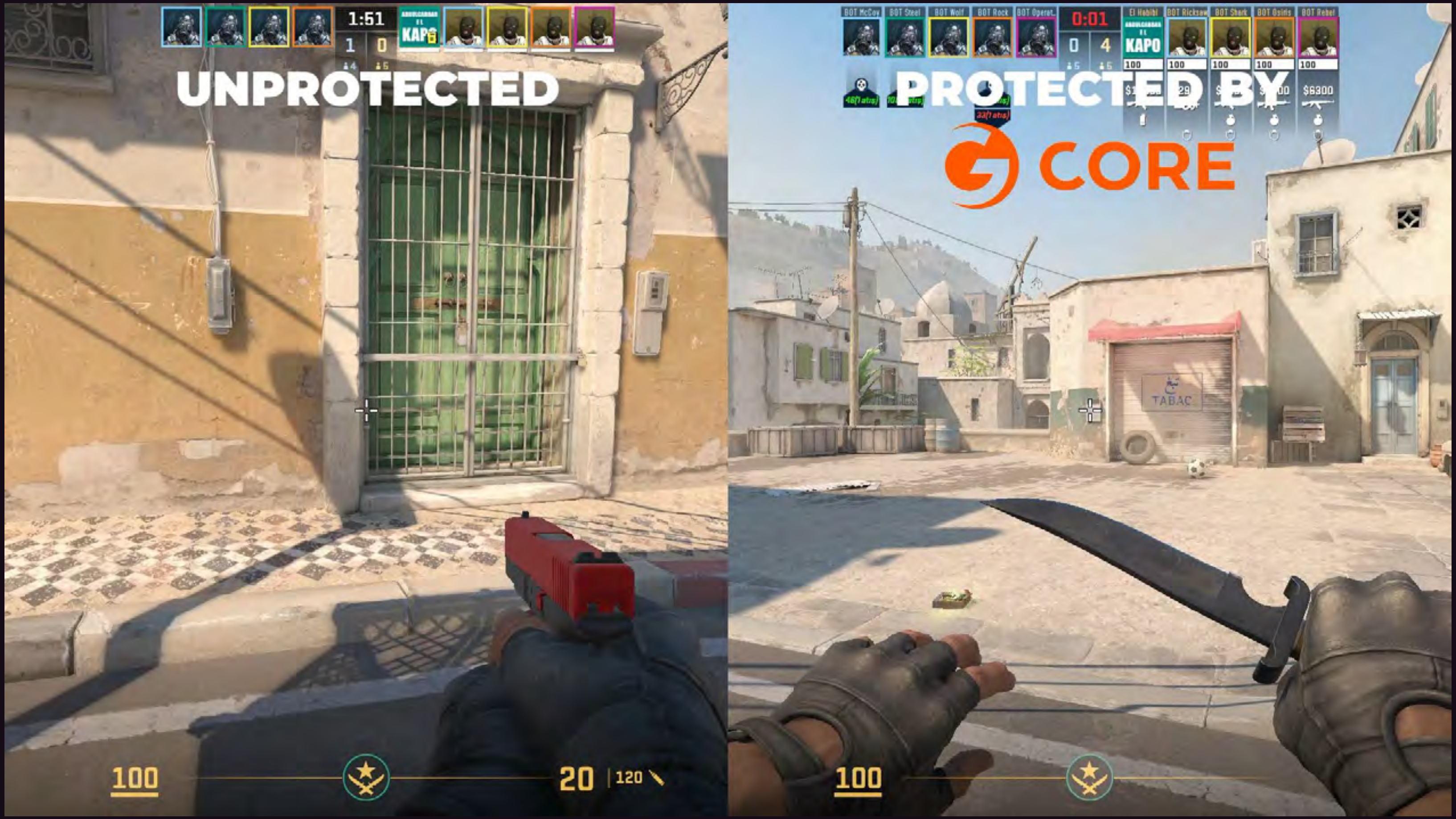
Loss of competitive edge:
Customers move to secure competitors.

Decreased loyalty:
Preference for better security practices.

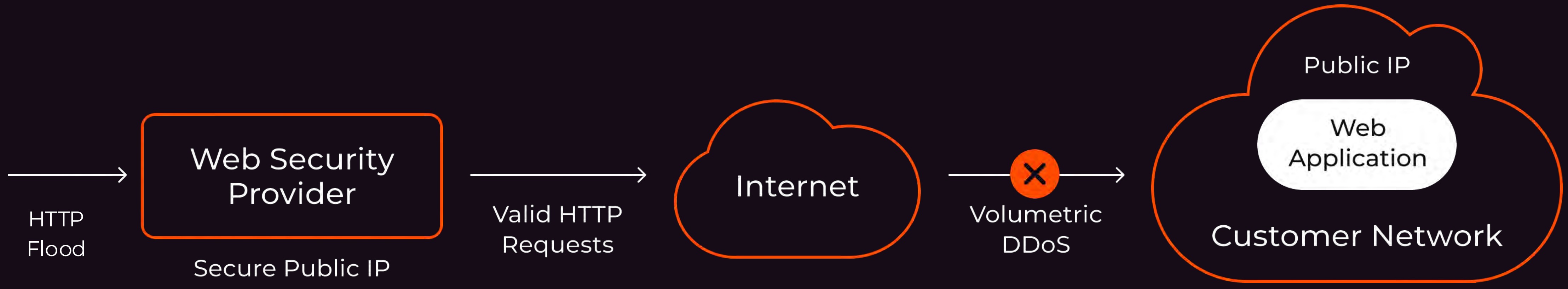
04

Protecting your infrastructure with Gcore

What gamers experience during an attack



Combining web and infrastructure protection is essential



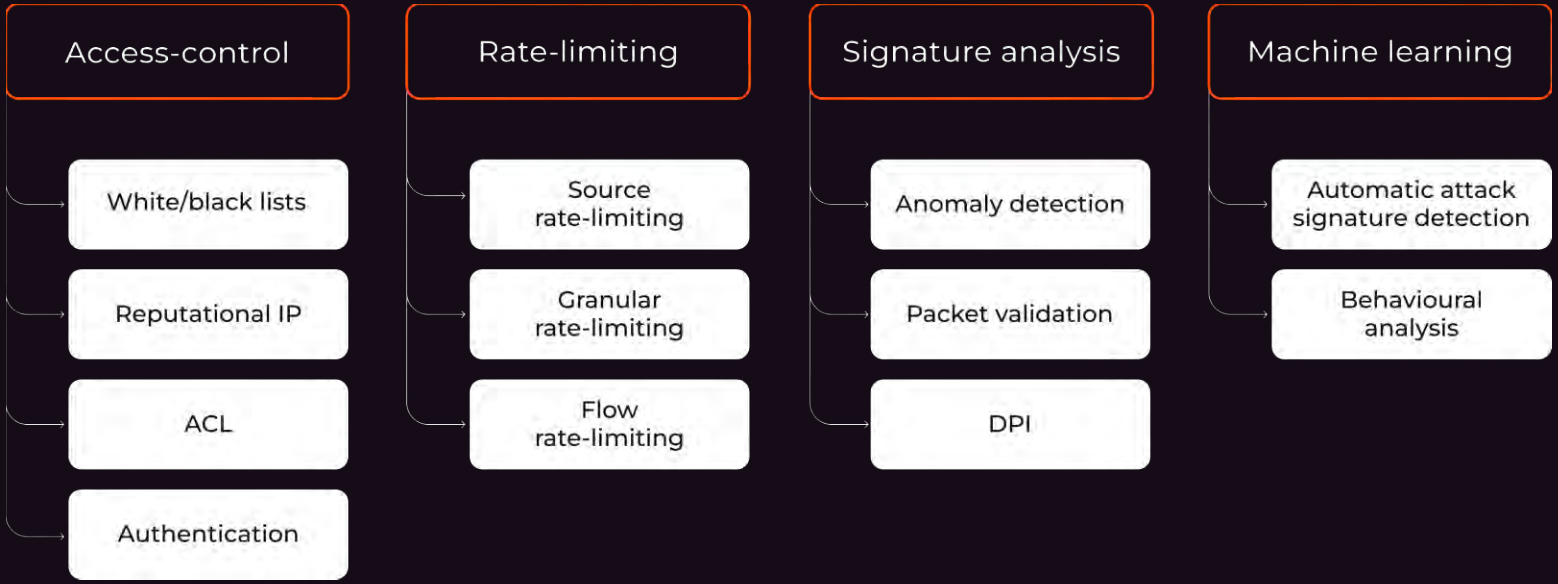
Single layer risks

- Limited defense:
  Web protection alone leaves infrastructure vulnerable to attacks.
- Exposure:
  Public IP remains exposed, creating security gaps.

Combined security benefits

- Comprehensive coverage:
  Protects both application and network layers.
- Increased resilience:
  Enhances overall security and reliability.

Gcore provides advanced, multi-layered DDoS defense



- Comprehensive protection
- Real-time detection
- Automated responses
- Scalable solutions
- Global coverage

Superior DDoS defense with Gcore CDN at its heart

Unified security solution

As a leading CDN and hosting provider, Gcore integrates CDN, DDoS protection, and web security for **optimal performance and protection**.

- Integrated CDN infrastructure
- Comprehensive web security
- Multi-layered DDoS defense

Efficient traffic handling

Our infrastructure handles 80-85% outbound and 15-20% inbound traffic, leveraging this imbalance to **strengthen DDoS defense**.

- High outbound traffic optimization
- Ample inbound capacity for DDoS mitigation
- Scalable bandwidth management

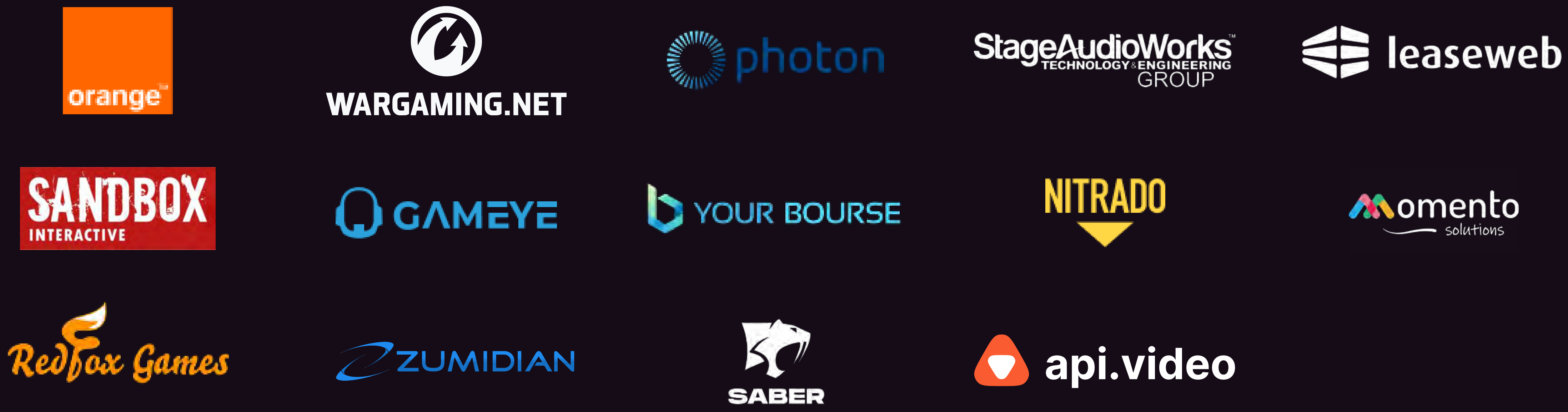
Robust DDoS defense

Designed to handle the heavy incoming traffic typical of DDoS attacks, our infrastructure is robust and reliable, providing a **consistent service**.

- High-capacity traffic filtering
- Real-time attack mitigation
- Automated threat response

Trusted by

We are trusted by some of the world's largest companies across media and entertainment, gaming, technology, telecommunications, financial services, and retail.



GCORE

Thank you!

Stay safe with Gcore

gcore.com