transparent edge

www.transparentedge.eu
comercial@transparentedge.eu
+ 34 91 091 64 19

KEEP YOUR SITE FAST AND SECURE

The European edge cybersecurity company

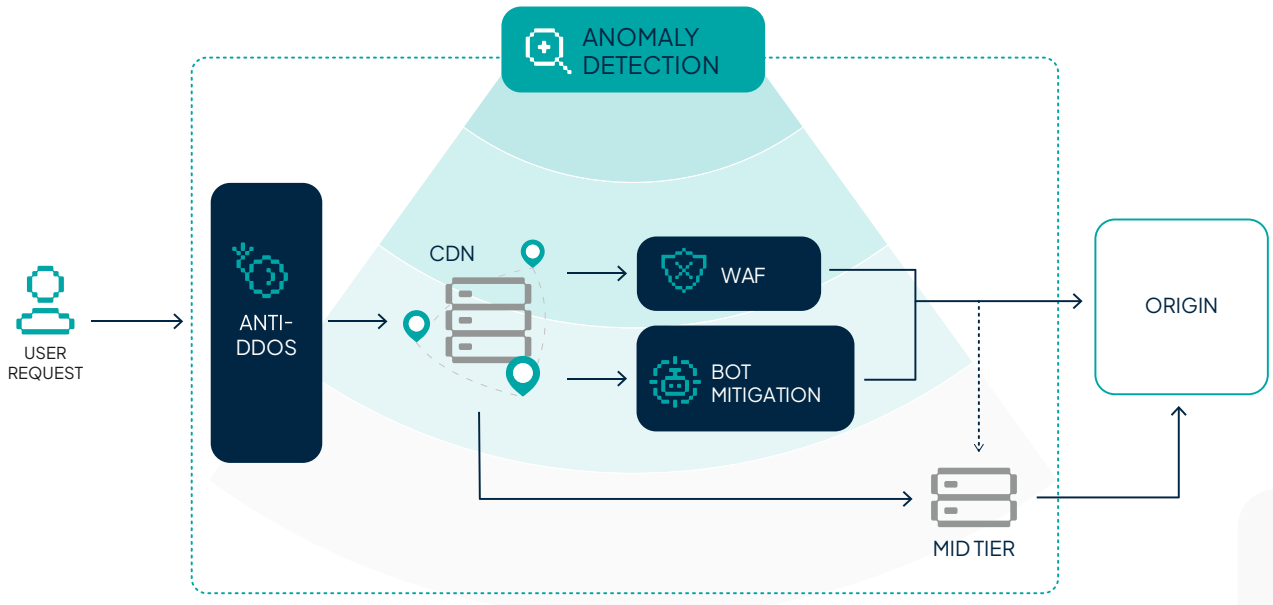
perimetrical

Comprehensive API and web protection at the edge

Websites and APIs have become essential technologies for business, making them prime targets for cyberattacks. Recent studies show a 25% to 30% increase in cyber incidents over the past year.

Today's threats are not only more frequent and sophisticated but evolve rapidly, introducing new layers of complexity to safeguarding digital assets. This trend is expected to accelerate, emphasizing the urgency of adopting robust security measures now.

Our comprehensive cybersecurity suite offers advanced multi-layer protection against the most significant multi-vector threats. Combining state-of-the-art detection and response technologies like WAF, Bot Mitigation, Anti-DDoS, and anomaly detection, our solutions ensure holistic security.



Simplified operations management

Transparent Edge's technology streamlines the administration of advanced cybersecurity functionalities through a unified dashboard. This simplifies the work of security teams, enabling them to efficiently analyze and manage extensive data across different platforms and providers.

With real-time visibility, precise controls, automated defenses, and instant threat response, Transparent Edge maximizes your security while reducing administrative tasks. This empowers your team to focus on strategic growth.

Real-time monitoring and advanced analytics

Leveraging advanced statistical models, Transparent Edge identifies anomalies to preemptively detect and neutralize threats like denial-of-service attacks or unauthorized web crawling.

Our solutions are continuously updated with the latest cybersecurity insights, thanks to a team with over 15 years of expertise managing high-performance content delivery platforms

ADDITIONAL BENEFITS OF PERIMETRICAL

EARLY RESPONSE

Our team is available 24/7 to provide efficient, real-time attack mitigation. No security tool is fully effective without expert backing.

AUTOMATION

Setting up anomaly reactions enables faster and more accurate identification of potential problems and frees up human resources by eliminating the need to constantly monitor systems. You will be able to automate different reactions to different scenarios

GRANULARITY

Tailor security rules to fit the specific needs of each site, ensuring minimal latency while maintaining the comprehensive visibility offered by our advanced analytics system.

VISIBILITY

With Perimetrical you can collect all the information required to report an incident to the State Security Forces and Corps, as required by the applicable regulations in terms of cybersecurity.

GDPR COMPLIANCE

As a European company, we strictly follow Regulation (EU) 2016/679, ensuring no user tracking or identification. We use advanced technology to identify malicious IPs without compromising user privacy.

OUR EDGE CYBERSECURITY SUITE

Dealing with hundreds of cyberattacks on a daily basis allows us to develop security features that include different technologies for efficient threat detection and mitigation. All of them are consolidated under Perimetrical, our advanced edge cybersecurity solution:

WAF

- Protection against SQL Injection, XSS, and CSRF
- Defense against advanced threats beyond the OWASP Top 10
- Account Takeover (ATO) prevention
- Support for multiple security levels
- Strict mode and detection-only mode
- Always up-to-date cipher suites
- Rate limit
- Custom signatures

BOT MITIGATION

- Low reputation IPs
- Low reputation Data Centers
- Low reputation ASNs
- Abuse lists
- VPNs
- TOR networks
- Anonymous proxy networks
- Bogon list

ANTI-DDOS

- At layers 3 and 4
  - → SSL, UDP, GRE-IP UDP, SYN, TCP RST, TCP CONNECT(), and TCP ACK negotiation flooding
  - → DNS amplification, NTP, CharGEN, Memcache, SSD, and SNMP
  - → SYN Tsunami
  - → Fragmentation and CLDAP attacks
  - → ARMS (ARD)
  - → Jenkins
  - → DNS Dropper
  - → CoAP
  - → WS-DD
  - → NetBIOS
- At layer 7
  - → Flooding of HTTP/S, login, creation, session and content requests
  - → Botnet detection
  - → Brute force attacks
  - → Slowlories

ANOMALY DETECTION

- Increase in bandwidth and/or requests (DDoS detection)
- Increase in requests per IP (identifies possible crawlers and scrapers)
- Decrease in cache effectiveness
- Increase in the number of 503 status codes
- Increase in origin response time
- Vulnerability scanner
- Detection of anomalous traffic by country