HORSE

Holistic, omnipresent, resilient services for future 6G wireless and computing ecosystems

Consortium

cnit · Atos · Telefónica · ERICSSON · Technische Universität Braunschweig · HELLENIC REPUBLIC National and Kapodistrian University of Athens · Suite5 We Deliver Intelligence · UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH · MARTEL innovate · efacec · HOLO-LIGHT · ZORTENET · Sphynx Technology Solutions · EIGHTBELLS Independent Research & Consultancy

horse-6g.eu

6GSNS

Co-funded by the European Union

HORSE

Holistic, omnipresent, resilient services for future 6G wireless and computing ecosystems

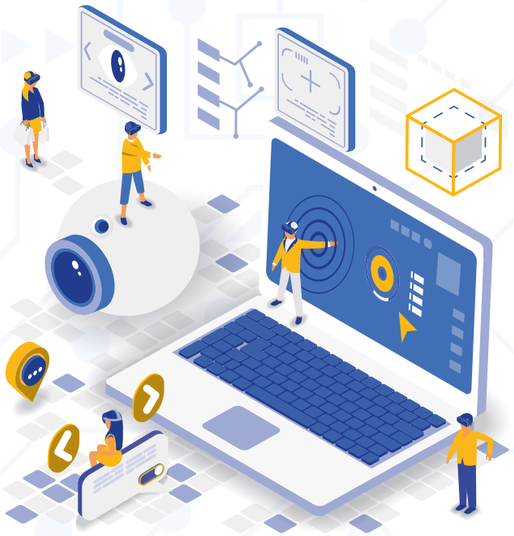
Exploring 6G Security

Real-time Threats and Mitigation in AR Server/Client Interactions

horse-6g.eu

Remote rendering to power XR industrial

Witness a live multi-user XR session where remote users interact with shared 3D CAD models in real time and communicate visually through avatars.



What sets this apart?

The HORSE platform actively predicts, identifies, and mitigates cyber-attacks in real-time, ensuring smooth interaction, low latency, and a seamless user experience.

Without HORSE, the same session is riddled with random avatar glitches and disruptive delays, clearly demonstrating the importance of resilient 6G infrastructure.

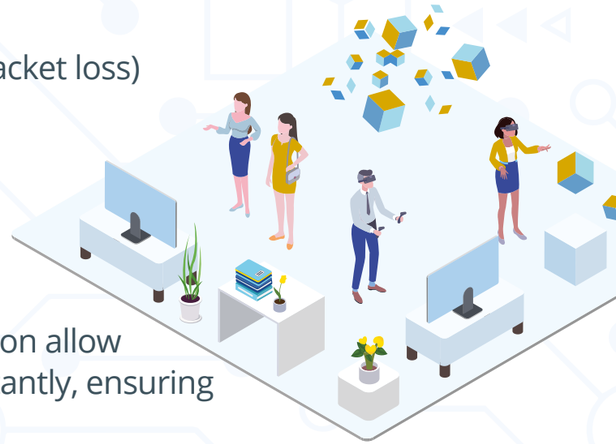
Transforming network resilience into immersive reality

HORSE validates end-to-end security and resilience in XR environments

Witness a live multi-user XR session where remote users interact with shared 3D CAD models in real time and communicate visually through avatars.

Without HORSE

Simulated attacks (e.g., latency spikes, packet loss) cause avatar jitter, delays, and scene inconsistencies resulting in a degraded user experience.



With HORSE

Real-time monitoring and threat prediction allow HORSE to detect and mitigate issues instantly, ensuring smooth, uninterrupted XR performance.

How?

- **Smart Monitoring:** Logs every NEF API request to detect suspicious activity early.
- **Intelligent Pre-processing:** Organizes requests by IP to identify patterns in the noise.
- **DEME Engine:** Analyses activity over time, flagging abnormal request spikes.
- **Swift Firewall Action:** Instantly blocks suspicious IPs before damage is done.