Residential Proxies: The Hidden Threat to Businesses

Ad Fraud & Click Fraud

- 40% of digital ad budgets lost
- Invalid traffic masquerades as real users
- Campaign effectiveness is severely compromised

Account Takeover (ATO)

- Thousands of accounts compromised monthly
- Financial losses from fraudulent transactions
- Customer trust severely impacted

Emerging Threats

- SMS pumping draining budgets & reputation
- Agentic AI requests bypassing defences
- Sophisticated automation at scale

Real Business Impact

$42B
Annual fraud losses

52,905
ISPs contaminated

238
Territories affected

Traditional Security is Blind

- **96%** of residential proxy traffic goes undetected

- **Only 15%** of organisations have any detection

- **Standard tools** can't differentiate from legitimate users

Sophisticated Attack Methods

- Phishing campaigns masking true location
- DDoS attacks blending with normal traffic
- Credential stuffing against major platforms
- Fraudsters faking their location

Agentic AI-Powered Attacks

- Automated attack orchestration
- Advanced adaptation beyond current limits

State-Sponsored Attacks

- Volt Typhoon (China) targeting critical infrastructure
- APT29/Earth Koshchei (Russia) conducting espionage
- Camaro Dragon (China) deploying router malware

The Threat is Accelerating

Recent High-Profile Attacks

- Okta credential stuffing campaign
- AUKUS infrastructure targeted
- European foreign affairs entities

Superior Protection with RST Cloud & Peakhour

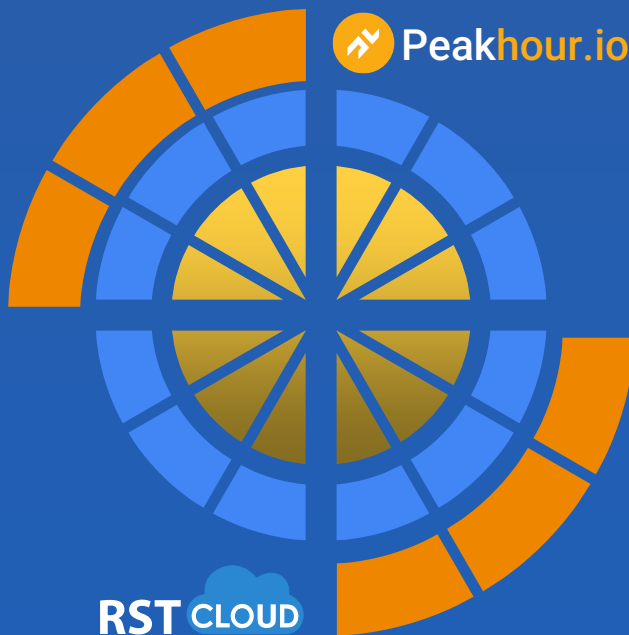✓ Advanced Threat Intel

✓ Continuous Monitoring

✓ Real-time Protection

Unique Advantages

Intel-driven scoring system
Advanced IP reputation
service

Proven Results

35% reduction in
fraud-related losses

Peakhour.io

RST CLOUD

Proprietary Detection

Network fingerprinting catches
96% more threats
Active scanning of the whole
Internet

Comprehensive Coverage

>14M observed residential proxy IPs
across 238 countries and territories