How Ucom Safeguarded Its Online Infrastructure and Achieved 100% Uptime with Qrator Labs AntiDDoS Solution

<1 second
average system reaction time to DDoS attacks

100%
malicious traffic filtered with zero false positives

6 Gbps
peak attack on August 28, 2025

0 downtime or service degradation since AntiDDoS deployment

QRATOR LABS
Cloud CyberSecurity. Smart.

Ucom is one of the largest telecommunications operators in Armenia, providing mobile communication, fixed broadband internet, television, and corporate IT solutions.

Founded in 2009, the company has become a key player in convergent services — combining mobile, fixed, and TV offerings — and delivers digital infrastructure to hundreds of thousands of subscribers across the country.

719,000+ mobile subscribers

142,000+ fixed broadband and TV subscribers

17,7% market share in Armenia's mobile base segment

Roaming in 160+ countries through 316 partner operators

Geography and audience: Ucom serves customers throughout

Armenia — from major cities to rural and mountainous regions with limited connectivity.

Infrastructure: a multi-service telecom platform powered by centralized data centers with redundancy and 24/7 SLA, international backbone channels, and traffic exchange points ensuring high availability and low latency.

Key business factor

For Ucom, uninterrupted operation of its network infrastructure and online services directly impacts customer satisfaction, trust, and revenue stability. Any degradation in availability or successful cyberattack could affect communication for thousands of corporate and residential clients across the country.

Technical challenge

Ucom needed to ensure resilience and high availability of its network resources — protecting business-critical services such as the customer portal, billing system, DNS zones, and API interfaces — against DDoS attacks while maintaining stable platform performance around the clock (24/7).

Key Features of Ucom

CONTENT AND TRAFFIC PROFILE

The company’s primary traffic sources include internet services, IPTV, streaming video content, mobile data, and enterprise-grade digital services such as corporate networks and cloud infrastructure.

AUDIENCE

Ucom serves subscribers across all regions of Armenia — from major cities like Yerevan, Gyumri, and Vanadzor to remote and mountainous areas where internet connectivity may be less stable. Users access services through both mobile and fixed-line connections.

BRAND AND MARKET PRESENCE

Ucom is one of the most recognized telecom brands in Armenia, holding a significant share of both mobile and fixed-line markets. The company has a strong position in delivering convergent services and enjoys high brand awareness among consumers nationwide.

CRITICAL IMPORTANCE OF AVAILABILITY

Ucom’s services — internet, television, and voice communications — are essential for daily life. Any network disruption, overload, or service degradation directly affects customer satisfaction, service quality, and brand reputation.

Challenge

Since 2020, Ucom has relied on Qrator Labs to protect its online resources, using the AntiDDoS service for the domains ucom.am and shop.ucom.am.

At the beginning of the collaboration, the operator was regularly facing a number of threats typical for large telecom platforms with high network activity and a large customer base.

KEY CHALLENGES INCLUDED

Heavy load on web portals and customer accounts during peak hours

A growing number of DDoS attacks targeting public web resources and API interfaces

---

Attempts to disable ucom.am and shop.ucom.am, especially during major promotions and customer campaigns

The need to maintain high service availability under any traffic conditions

For a telecom operator that provides nationwide internet and mobile services, service stability is mission-critical. Even brief disruptions in website or account functionality directly affect customer satisfaction, online payments, and overall trust in the brand.

Ucom's main objective was to ensure resilience and uninterrupted availability of its online resources, eliminate the risk of downtime caused by DDoS attacks, and maintain stable operation of all user services 24/7.

> "It is absolutely critical for us that users can connect services, make payments, and manage their accounts online without interruptions. Even during an attack, the website must remain accessible — for Ucom subscribers, it's a part of their everyday communication."
>
> — Alla Galoyan, Head of Mass Segment Fixed/FMC & B2B Marketing Division Ucom.

Solution

To ensure continuous service availability and protect its critical online infrastructure, Ucom implemented the Qrator Labs AntiDDoS solution for both ucom.am and shop.ucom.am.

The service was integrated at the network level, enabling automatic detection and mitigation of volumetric and protocol-based DDoS attacks in real time — without any disruption to legitimate user traffic.

The AntiDDoS system continuously analyzes all inbound network flows, identifying anomalies in volume, connection patterns, and protocol behavior. Suspicious traffic is rerouted through Qrator Labs distributed filtering network, where malicious packets are dropped before reaching the origin servers. Legitimate traffic, in turn, passes through unaffected, ensuring a seamless user experience.

Since the initial deployment, Qrator Labs has successfully mitigated dozens of DDoS incidents targeting Ucom's public resources.

A particularly notable case occurred on August 28, 2025, when the company experienced a large-scale Layer 3/Layer 4 attack combining UDP flood and SYN flood vectors.

The incoming malicious traffic peaked at approximately 6 Gbps — nearly 1,000 times higher than Ucom's typical baseline of ~6 Mbps on the affected service.

Despite the sudden spike, the AntiDDoS system reacted instantly — in under one second.

All illegitimate packets were 100% filtered, with zero false positives. The attack had no visible impact on the availability or performance of Ucom's web resources; customers continued to access services normally throughout the incident.

> “Even during the heaviest attacks, we didn’t notice any downtime or degradation. Qrator Labs’ filtering kicked in instantly — the system handled everything automatically.”
>
> — Alla Galoyan, Ucom.

By deploying Qrator Labs’ AntiDDoS protection, Ucom ensured 24/7 resilience of its online infrastructure, maintaining uninterrupted customer access and reinforcing the reliability expected from one of Armenia’s leading telecom providers.

Result

The comprehensive DDoS protection implemented by Qrator Labs allowed Ucom to significantly enhance the stability and resilience of its digital services within the first weeks of deployment.

Since 2020, both ucom.am and shop.ucom.am have operated continuously — without downtime, even during large-scale attacks.

Key outcomes

Full protection from DDoS attacks: every detected incident — including volumetric and protocol-level floods — has been automatically mitigated with 100% efficiency.

Zero false positives: legitimate users remain unaffected, even during active filtering phases

Instant mitigation: the system responds in under one second, ensuring that malicious traffic never reaches application servers.

Uninterrupted availability 24/7: both the main website and online shop stay online at all times, ensuring stable access for customers and partners across Armenia.

Operational efficiency: automation of DDoS response significantly reduced manual monitoring and emergency handling efforts, allowing Ucom's network team to focus on core infrastructure development.

Proven performance under real attack: on August 28, 2025, the platform withstood a 6 Gbps UDP + SYN flood, over 1,000× its usual 6 Mbps baseline load — fully filtered in under one second with zero service disruption.

Business continuity: no downtime or service interruptions reported since the introduction of Qrator Labs AntiDDoS protection in 2020.

"After implementing Qrator Labs' protection, we immediately saw that our key online systems remained stable and accessible even during high-intensity attacks. For a telecom operator, uptime means trust — and now we are confident that our services will stay online no matter what."

— Alla Galoyan, Ucom.

100% attack mitigation rate — all DDoS attempts successfully filtered

<1 second average response time for automatic mitigation

0% false positives — no legitimate user traffic affected

0 downtime incidents since deployment in 2020

6 peak attack volume successfully absorbed and filtered (August 28, 2025)

≈1,000× traffic surge neutralized without performance loss

24/7 continuous availability of both ucom.am and shop.ucom.am

QRATOR LABS
Cloud CyberSecurity. Smart.

mail@qrator.net