corero [THE DDoS PROTECTION SPECIALISTS] blue.

BLUE CASE STUDY _

French Telco Goes from DDoS Mitigation to DDoS Protection with Corero

> “Today, we no longer have any customer support tickets related to DDoS issues and we can more easily meet our service level agreements (SLAs).”
>
> **- Nicolas Turpault, Infrastructure Director at Blue S.A.**

French telecommunications company Blue S.A. was lucky: it experienced relatively few DDoS attacks (less than 10 a week) that typically lasted only a few minutes and didn’t saturate network links.

But Blue, in this sense, was like a well-trained athlete that had finally gone pro but now wanted to win the league. All companies, but especially telcos, want to get the point of reducing latency issues and downtime to almost zero.

“Our network is relatively clean because we serve only businesses and IT departments,” said Nicolas Turpault, Infrastructure Director at Blue. Still, Turpault explained, when a public IP on a low-speed connection was attacked, it would become unusable, resulting in client support requests and stress for the IT security team.

That’s when Blue turned to Corero.

The Challenge - Moving from Mitigation to Prevention

Founded in 2005, Blue (formerly Bretagne Télécom) is a cloud service provider with a wide range of high-performance solutions, including very high-speed internet networks, private networks, information systems outsourcing, cybersecurity, and more.

The company has a presence in eight interconnected data centers in France as well as its own ISO 27001-certified data center. With 5,000 managed servers and 10,000 cloud servers, Blue supports over 2,500 organizations in France.

Blue was seeking to not just mitigate but prevent DDoS attacks. They wanted to implement their own DDoS protection for all of their network links rather than assuming that their transit providers would provide adequate protection. The company also wanted simple implementation and reliable support and maintenance so it could be free to focus on its core business goals.

The Solution - Corero's SmartWall One DDoS Protection Platform

Blue assessed several DDoS mitigation solution providers and ultimately chose Corero SmartWall® One because of its leading DDoS protection capabilities.

Many DDoS solutions are exclusively reactive, meaning they only start working after a DDoS attack has done some damage. However, Corero's SmartWall One solution proactively prevents attacks before they can cause harm. Blue uses the Corero SmartWall One solution in inline mode, meaning SmartWall One quickly and automatically inspects all incoming internet traffic.

"Corero earned our business because it was simple to implement, and the support and maintenance contract ensured that almost everything is done by Corero," said Turpault.

And since Corero's DDoS protection is based on powerful algorithms for immediate threat detection and mitigation, Blue had to do very little configuration of its own.

"The default rules integrated into Corero are very practical and useful, effectively blocking the majority of DDoS attacks easily, without any particular configuration," Turpault said.

The Results - Effective Protection and Peace of Mind

Corero has produced two primary and very tangible results for Blue:

1. No more support tickets — Pre-Corero, a public IP on a low-speed connection would become unusable if a DDoS attack happened. Now, everything works — an outcome that has given Blue's security team significant peace of mind. "Today, we no longer have any customer support tickets related to DDoS issues, and we can more easily meet our service level agreements (SLAs)," Turpault said.

2. Better visibility into attacks — Turpault noted that one of the most useful features of the SmartWall One platform is its customizable dashboard, which offers forensic evidence before, during, and after attacks, including granular detail such as the types of DDoS attacks attempted and how and when they are blocked. By gaining visibility into the latest attacks and blocked traffic on their network, Blue now has a much better understanding of the DDoS threats it faces.

Corero SmartWall One Highlights

- Surgically and automatically removes DDoS attack traffic before it reaches critical systems, eliminating downtime and ensuring optimal performance and maximum availability.
- Protects against a wide range of DDoS attacks, from simple volumetric floods to sophisticated state exhaustion attacks, at Layers 3 through 7.
- Delivers line-rate, in-line DDoS attack protection from 1 Gbps to 100 Gbps per rack unit in a solution that scales to terabits per second of protected throughput.
- Provides comprehensive forensic-level analysis before, during, and after attacks.
- Ensures that legitimate traffic is not impacted by false positives.
- Inspects every inbound packet header and payload data, surgically removing DDoS packets without disrupting the delivery of legitimate network traffic.
- Dynamic tuning rapidly identifies and automatically protects against emerging DDoS threats.
- Detects and mitigates attack traffic in less than a second instead of the minutes or tens of minutes required by traditional DDoS protection solutions.