Publication date:
19 Jan 2026
Author(s):
Rik Turner, Chief Analyst, Cybersecurity

Corero hones its enterprise focus, combining availability and resilience with DDoS

Omdia view

Summary

Corero Network Security, best known for its distributed denial-of-service (DDoS) mitigation technology, is broadening its marketing focus beyond its traditional service provider customers to target enterprises as well. Both its product portfolio and go-to-market strategy are expanding to reflect that widening remit.

Corero underpins multiple service provider DDoS services

Corero is no “new kid on the block” in DDoS mitigation, having been founded in the UK in 1991. Its shares have been traded on the AIM, the junior market of the London Stock Exchange, for many years and, since February 2024, on the OTCQB venture market in the US. The company reported revenue of $25m in 2024.

The vendor spent its first three decades focused on the service provider market, where telecoms operators and ISPs use its hardware appliances to offer DDoS mitigation services to their business customers. It presently has over 100 customers, the majority of which are in the service provider segment. Most of them are Tier 2 or Tier 3 ISPs, though it also has at least one Tier 1, namely GTT Communications.

However, over the last couple of years, Corero has been expanding its horizons, developing both its technology offerings and how it takes them to market with a view to selling both to enterprise customers. Of particular relevance in this context are large enterprises operating networks with multiple points of presence serving extensive workforces and customer bases. Once an organization reaches that size, its network operations team is effectively operating as a “mini telco,” making it an ideal target for Corero, given its service provider heritage.

The vendor has been striking alliances with major tech players over the last few years, with its partnerships with content delivery network (CDN) market leader Akamai and Juniper (the networking heavyweight acquired by HPE in mid-2025) among the most significant.

The deal with Akamai for hybrid DDoS mitigation

Corero's Akamai deal was announced by both vendors in September 2023 and is interesting for what it says about the evolution of the market for DDoS mitigation technology. Akamai has very much been the poster child for cloud-based DDoS mitigation delivered as a service since it ventured into that world. It did so in response to requests for help from major Wall Street banks and financial institutions coming under attack as part of Operation Ababil, a massive volumetric DDoS attack launched by the Qassam Cyber Fighters (QCF) in September and October 2012.

With its massive network capacity, Akamai was able to soak up the excess traffic thrown at those customers by the QCF, and the vendor not only recognized the business opportunity presented by DDoS mitigation services but also became the leading advocate for this cloud-based, "as-a-service" approach. This was in contrast to the on-premises boxes from the likes of Radware, F5, and Arbor that had prevailed in the market up until that point.

To be fair, Verizon Business had unveiled a cloud-based mitigation service as far back as 2010, but Akamai really became the face of this business model after Ababil, doubling down on DDoS service with its February 2024 acquisition of Prolexic, which brought a network of scrubbing centers to support another line of mitigation capabilities.

The cloud versus on-premises debate in DDoS mitigation

Given that, in the mid-2010s, so much business IT was migrating to the cloud, it seemed reasonable at that time to assume that all DDoS mitigation might eventually be delivered as a service in this way. Akamai was certainly vociferous in making that argument, particularly as the frequency and size of volumetric attacks ramped up, powered by the success of the fiber-to-the-home and fiber-to-the-curb initiatives in the 2000s.

The vendors of appliances to be deployed on an enterprise's premises countered, however, that an always-on service, routing an organization's entire internet traffic through a service provider such as a CDN, was expensive and added latency to its communications. Instead, they proposed a hybrid option, with on-premises infrastructure handling the attacks it could, detecting when a volumetric attack that would swamp its capabilities was starting, and rerouting traffic to a cloud service to escalate mitigation efforts.

This approach was more economical and reduced the latency impact of an always-on cloud service. However, it initially faced the challenge that the time between the detection of a volumetric attack starting and the rerouting actually kicking in could be several minutes, during which the victim could be driven offline, with potential damage done to the infrastructure. The proponents of always-on cloud services, meanwhile, made them less expensive in an effort to weaken the economic argument for the hybrid solution.

Corero was largely on the sidelines of this debate; while it produced DDoS mitigation boxes, it sold them to the providers of cloud-based mitigation services rather than to enterprises.

Hybrid looks like it is here to stay

A decade on from when the debate was raging, Omdia's data on the evolution of the DDoS mitigation market (see links in the ***Further reading*** section below) confirms that, far from withering in the face of the cloud-only onslaught, hybrid services have held their own, remaining a major part of the overall business. Indeed, if anything, the conditions for hybrid mitigation have improved in the intervening years.

On the one hand, tech vendors have significantly reduced the time required to switch from on-premises to cloud-based mitigation platforms, reaching a point where it is virtually instantaneous. On the other hand, many companies have been repatriating at least part of the infrastructure from the cloud back to their premises. This trend is driven by factors that include:

- The cost of data egress
- Regulations requiring data sovereignty
- The adoption of artificial intelligence (AI), where hosting some of that infrastructure yourself can prove much cheaper than relying on a cloud provider

The combination of these issues and the resulting repatriation trend have led Omdia over the years to respond to the bold claim that "the future is cloud" with the qualifier that "the foreseeable future is hybrid."

Burst attacks require on-premises mitigation

A further dimension worth noting is the evolution of new attack types, specifically the so-called "burst" DDoS attacks that arose around 2017. These short-burst or "pulse wave" attacks are designed to hit a target with a massive amount of traffic quickly, then switch to another target, often before returning at an indeterminable time. They challenge cloud-hosted applications that use autoscaling, causing rapid scale-ups and then redundant scale-downs when the burst is over.

Of course, they also circumvent cloud-based mitigation, whether it be always-on or the ad hoc variant that is invoked from on-premises infrastructure, since they will often have stopped before any cloud-based response takes place. They are used not only to bamboozle cloud-based mitigation services but also to carry out reconnaissance on a victim's infrastructure, enabling the attackers to come back at a later date with a better-informed strategy.

Local rather than cloud-based mitigation is called for here, and there are estimates that over 90% of network-layer attacks are under 500Mbps and most last for less than 10 minutes, which highlights how prevalent this "hit-and-run" tactic has become in the modern threat landscape.

What each side gets from the deal

Akamai has long been an evangelist for always-on, cloud-only DDoS mitigation, of course, so teaming up with Corero, a provider of on-premises boxes, should be seen as the CDN heavyweight adapting its messaging to a changed market reality. Meanwhile, Corero is enhancing its marketing directly into the enterprise segment; having previously served that segment indirectly (i.e., through its service provider customers), it now has access to Akamai customers that need an on-premises dimension for their DDoS mitigation. It is clear that market evolution formed the backdrop to the Corero–Akamai deal.

Akamai now offers services called Prolexic On-Prem and Prolexic Hybrid, both of which use Corero's hardware to complement its cloud-based capabilities. Meanwhile, Corero is marketing the hybrid offering as Corero SmartWall ONE Hybrid Cloud DDoS Protection, again with the customer operating and controlling the on-premises boxes and escalating to the cloud as necessary.

Corero DDoS mitigation delivered from Juniper routers

The relationship with Juniper dates further back; the two sides announced a technology alliance in 2016, which developed into a formal global partnership in September 2018. This entailed the integration of the software behind Corero's DDoS protection technology into Juniper's MX and PTX series routers, which are sold primarily to service providers, making them a cost-effective alternative to a "two-box" deployment. However, the vendors expanded their partnership in April 2025, with Juniper broadening the range of Corero products in its portfolio. These now include:

- The SmartWall ONE portfolio, which consists of hardware appliances and software deployed on commercial-off-the-shelf devices, enabling Juniper to sell DDoS mitigation technology into accounts not using its routers
- The Corero Observability & Resiliency Ecosystem (CORE) platform, a software as a service offering that Corero launched in October 2024

CORE is designed to unify visibility and defensive actions across various security infrastructures, sitting alongside Corero's DDoS protection products. Its initial capabilities include traffic analysis, zero-trust access control, and Layer 7 DDoS protection, also known as defense against application-layer attacks.

CORE is a particularly important part of Corero's strategy of expanding its marketing directly to enterprises. It draws telemetry from hardware-based and software-only Corero DDoS platforms, of course, but the idea is to ingest from other vendors' systems as well, broadening the range of security benefits Corero can offer enterprise customers. The company refers to CORE as a "multi-solution platform," indicating where it wants to take the product.

Addressing polymetric DDoS with AI

Another significant feature added to the SmartWall ONE family of products is designed to appeal to enterprises and Corero's more traditional customers in the managed security service provider space. This is the inclusion of AI algorithms to detect suspicious behavior hidden in encrypted traffic.

Encryption has become the norm on the web in recent times, with Google publishing statistics in April 2025 to suggest that some 98% of all internet traffic in the US was over HTTPS, while users were spending around 99% of their Chrome browsing time on encrypted pages. Globally, estimates suggest that between 95% and 98% of internet traffic is now encrypted.

This is beneficial, of course, for companies and individuals seeking to protect the privacy of their data. However, it is also a double-edged sword, in that threat actors also use encryption to cloak their activities, whether that be malicious requests coming in or exfiltrated data going out. A case in point is the rise of polymetric DDoS attacks, which employ a range of techniques at different network layers, particularly at Layer 7 (the application layer), using HTTPS to bypass standard, single-focus defense mechanisms and increase the likelihood of success.

The idea behind Corero's October 2025 announcement is that, rather than decrypting data or using static signatures to flag anomalies, AI models can be used to look at behavior and metadata to model normality. In other words, they study behaviors such as handshake timing, packet size distributions, and concurrency rates to determine what normal encrypted traffic looks like, then detect problems as they occur.

More channel news is coming

As it expands its remit beyond service providers into the enterprise segment, Corero is also developing its go-to-market strategy for this purpose. In the second half of 2025 alone, the company announced relationships with channel partners in the US, Pakistan, Brazil, Thailand, the UK, and Singapore, promising more activity on this front in 2026.

A market report establishes Corero's credentials

This expansion will likely also entail actions to raise its profile with enterprise buyers, both in tandem with these partners and on its own. In this context, a positive move is Corero's publication of an annual Threat Intelligence Report, detailing how the DDoS market is evolving across the globe and how threat actors' tactics are evolving. This is a valuable source of data for analysts and journalists, as well as a handy promotional tool.

The US telco Verizon has long used its annual Data Breach Investigations Report (DBIR) to showcase its expertise in cybersecurity, with the DBIR cited in the trade press and in countless presentations at conferences every year. Specifically in the DDoS market, the likes of NETSCOUT's Arbor security division, Akamai, and Cloudflare all provide useful market data and background color on how attacks are evolving. Omdia would encourage Corero to make more of its annual report and perhaps consider quarterly updates in blogs to bolster its brand awareness.

Appendix

Further reading

DDoS Prevention Technology Market Tracker – 1H25 Analysis (December 2025)

Author

Rik Turner, Chief Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com