CASE STUDY

CLOUVIDER IMPROVES CUSTOMER ACQUISITION AND RETENTION WITH CORERO'S AUTOMATED DDoS PROTECTION

Clouvider prides itself on offering high-end quality and features at a competitive price, with a fully redundant infrastructure, 100% power and network SLA as standard.

Clouvider is a global cloud infrastructure provider of Web Hosting, Cloud Hosting, Dedicated Servers, Connectivity, Private Cloud, and Managed Services to a pan-European and US audience of resellers, as well as small to medium-sized business customers.

Clouvider uses the latest enterprise Supermicro hardware with Intel Coffee Lake processors, delivered via a redundant Juniper MPLS network infrastructure that is spread over multiple datacenters (in the US, UK, Netherlands, and Germany).

> Corero Smartwall at a glance

- Surgically removes DDoS attack traffic automatically, before it reaches critical systems, ensuring optimal performance and maximum availability.
- Delivers line-rate, in-line distributed denial of service attack protection, from 1Gbps to 100Gbps per rack unit, in a solution that scales to Terabits per second of protected throughput.
- Prevents the impact of attacks ranging from simple volumetric floods, to sophisticated state exhaustion attacks, at layers 3 to 7.
- Delivers comprehensive visibility for analysis and forensics, before, during and after attacks.

>the challenge

Clouvider realized the need to improve its DDoS mitigation in 2019, having experienced multiple attacks of very high volume that saturated their transit links. This was after starting off trying to use just the BGP FlowSpec DDoS filtering capability built into the traffic analysis platform deployed on their network edge.

Although this solution has detected and blocked attacks using the most common volumetric vectors, before they passed into the company's core network, it has a very limited ability to mitigate more sophisticated attacks, including those coming from spoofed IP addresses, such as is common with IoT botnet-based attacks.

>the solution

After careful consideration, Clouvider chose to deploy the in-line, real-time, always-on Corero SmartWall Threat defense System (TDS), with SecureWatch® analytics technology. This has enabled them to fully protect their customers against DDoS cyberattacks, including the most complex and sophisticated attack vectors. The new dual-stage mitigation approach, combined with their 2.9+Tbit/s total network capacity, allows Clouvider to provide comprehensive mitigation of any attacks that their customers may face.

They started by researching the available DDoS solutions, narrowing down their choice to, and conducting a Proof of Concept trial with, Corero. Ultimately, they chose the Corero SmartWall solution because *"it deals with tracking traffic patterns, out of the box,"* said Dominik Nowacki, Managing Director for Clouvider. *"The proof of concept went surprisingly smoothly,"* he said, and as soon as Clouvider installed the first Corero SmartWall appliance, one of their game server customers started getting attacked. It would turn out to be *"an excellent test for the new Corero solution,"* said Nowacki. They started routing traffic through the Corero appliance, and soon got hit with an extremely sophisticated attack. Nowacki and his team contacted the Corero Security Operations Center (SOC), who immediately analyzed the attack and were able to fine-tune the automatic mitigation to better distinguish the legitimate customers from the DDoS traffic, and surgically block the bad packets at the appliance level.

> *Nowacki said, "We thought it would be a simple fix, but it required an extremely custom mitigation. However, the Corero SOC team did it very quickly; they were very engaging and did much more than we expected them to do. We thought they would say, 'that's too custom, we need to charge you extra money.' Instead, Corero's SOC team went to extra effort, even buying the game, so they could understand the packets and write specific protocol-based rules around the traffic. We were extremely, positively surprised; that experience cemented the relationship and we'll never look at another solution again."*

>Value-added Offering

With all of its products, Clouvider includes complimentary best effort DDoS protection that provides coverage for the majority of customer accounts; additional protection and mitigation levels can be arranged on request, if a customer has a disproportionate level or volume of attacks.

> *"Our philosophy is to be customer-friendly, fair and reasonable, happy to help," said Nowicki.*

- No need to blackhole or null route traffic
- No blocking of legitimate customer traffic
- Maximum levels of service availability are maintained for customers, even in the face of a DDoS event
- DDoS attacks are automatically mitigated locally at each of their multiple locations across Europe, the UK and the US
- Reduced support requests by 90%
- Increased customer retention
- Increased customer acquisition
- Improved customer satisfaction
- Improved brand reputation
- A competitive advantage over other service providers

>the results for Clouvider

Corero has improved Clouvider's business on two fronts: they're better able to retain existing customers, and they can more easily acquire new customers. It's a competitive differentiator for Clouvider; *"We definitely stopped losing customers; we can retain customers now because we offer top-notch DDoS protection. And, we're also gaining new customers because they had previous experience with Corero's solution and were satisfied with it."*

Because Corero automatically mitigates 99+% of bad traffic, Nowicki says *"I no longer have to respond to alarms saying that we have an attack in progress, or that one of our security analysts can't identify the pattern to then apply the appropriate manual mitigation."* Clouvider's support team members are also happy with the Corero solution because they spend significantly less time working on attack mitigation, due to the automated functionality of the Network Threat Defense appliance that is part of the SmartWall solution. They've seen a 90% reduction in the number of support tickets for attack outages.

Instead of frequent customer support tickets that say *"my server is down,"* they now receive only sporadic support requests in the customer portal regarding inquiries into triggered mitigations. *"Formerly we received 'server down' requests at least once per week; it is now to the point where I have to think hard to remember the cases I had to deal with,"* said Nowicki.
He added, *"We now have more positive interactions with our customers because, rather than telling us that they're under attack, they're reaching out to us for additional details about the attacks that have been mitigated."*

>the benefits

> *"By having in-house filtering appliances in each of our PoP locations, there is no backhauling or impact to latency during any attack filtering, offering a unique competitive edge over multiple other providers that use external appliances and filtering technologies," said Nowicki.*

Nowicki's team uses the Corero SecureWatch® Analytics application to observe DDoS attack traffic targeting their network, which gives them a single-pane view across their entire network. First and second line support teams can see where attacks are attempted, and escalate support if necessary; this saves the time they would otherwise spend reviewing all the logs themselves. SecureWatch Analytics is integrated with Clouvider's API to deliver a broader single-pane view of other customer services, including; ordering, billing, and technical support.

Their customers receive reports, in PDF format, that summarize the effectiveness of the DDoS mitigation and show the size, duration and type of attacks that were mitigated. *"Our customers greatly appreciate this proof of protection, and this is also a great benefit to us, because the customer can see the value in the excellent service we're providing,"* said Nowicki.