corero [NETWORK SECURITY] tierpoint

TierPoint

CASE STUDY

TierPoint Tackles DDoS Threats with Corero Network Security's Adaptive and Cost-Effective Protection

TierPoint, a leading provider of hybrid IT solutions with a nationwide footprint, delivers secure, connected data center and cloud services that untangle complexity and provide tailored solutions. Since 2010, TierPoint has specialized in scalable, cost-effective IT infrastructure, supporting thousands of clients—from small businesses to Fortune 500 enterprises—through over 40 data centers in 20 U.S. markets and a coast-to-coast network of multi-tenant cloud pods. Their comprehensive portfolio includes cloud, colocation, disaster recovery, and managed IT services, all backed by a strong focus on security, compliance, and expert support. TierPoint helps organizations drive performance, manage risk, and stay focused on their core business.

The Challenge

TierPoint had grown increasingly frustrated with their existing DDoS protection solution, which failed to deliver the level of service availability required to meet their clients' expectations. Frequent disruptions and slow mitigation times were taking a toll on their ability to provide uninterrupted services, jeopardizing customer trust.

The situation had become so pressing that TierPoint began exploring the development of their own in-house DDoS protection solution. However, the potential time and resources required for such an initiative would have diverted attention from more critical business priorities, such as enhancing their core service offerings and driving growth.

4 Key Reasons TierPoint Chose Corero

1. Enhanced Defense with Existing Tech
2. Real-Time Protection
3. Collaborative Partnership
4. Significant Cost Savings

> “Our customers rely on us to keep their businesses running smoothly,” said Paul Mazzucco, Chief Information Security Officer at TierPoint. “We couldn’t afford to waste time on solutions that didn’t work, but building our own system would have been a massive distraction from our strategic goals.

Why TierPoint Chose Corero's Adaptive DDoS Protection Solutions

Before making their decision, TierPoint rigorously tested Corero appliances against its existing solution and was impressed by the exceptional performance. The results were so compelling that they decided to switch to Corero even while still under contract with their current vendor. Additionally, Corero's ability to integrate directly with TierPoint's Juniper routers was a game-changer, enabling a "protective mesh" that fortified their defenses without requiring additional hardware investments. The solution's superior performance and cost-efficiency made the decision clear.

"Corero's solutions not only protect our infrastructure but also enhance our existing tech stack," Mazzucco explained. "The Juniper integration allows us to deliver robust defense while saving on costs and reducing operational complexity."

Significant Reduction in Mitigation Time

One of the most impactful benefits TierPoint experienced was the dramatic reduction in mitigation time during DDoS attacks.

> "Our time to mitigation for DDoS attacks went from six minutes with previous solutions to 18 seconds with Corero," said Mazzucco. "This ensures that our customers experience uninterrupted services, even during attacks."

The Value of True Partnership

For TierPoint, working with Corero has been more than just adopting a new technology; it's about building a trusted partnership. Corero's collaborative approach and deep expertise have been invaluable in addressing TierPoint's unique challenges.

> "Working with Corero feels like a true collaboration," Mazzucco said. "My team and I can openly share ideas and discuss ways to enhance the efficacy of our protection. Corero's willingness to listen and adapt fosters a partnership where we're constantly improving together for the greater good."

The Benefits

Since implementing Corero's adaptive DDoS protection, TierPoint has realized key benefits, including:

- **Enhanced Defense Through Existing Infrastructure:** Seamless integration with Juniper routers delivers comprehensive protection without adding new appliances.
- **Operational Efficiency:** Real-time threat detection and mitigation reduce the workload for TierPoint's security teams, allowing them to focus on strategic initiatives.
- **Ongoing Collaboration for Continuous Improvement:** The partnership with Corero allows TierPoint to continuously refine and enhance its protection strategy. The collaborative nature of the relationship ensures TierPoint stays ahead of evolving threats, driving greater value for their clients.
- **Cost Savings:** Avoiding the need for additional hardware and maximizing existing infrastructure has significantly lowered operational expenses.

> Corero's solutions help us deliver a level of protection that would otherwise require a far larger investment," said Mazzucco. "This efficiency strengthens our business and our ability to serve clients at the highest level."

Moving Forward

With Corero as a trusted partner, TierPoint is confident in its ability to stay ahead of evolving threats.

> Corero's commitment to innovation and their collaborative approach give us a strategic advantage," Mazzucco concluded. "They've helped us turn a complex challenge into a competitive differentiator."

Corero DDoS Protection Solutions Highlights

- Inspects every inbound packet header and payload data, surgically removing DDoS packets without disrupting the delivery of legitimate network traffic.
- Surgically and automatically removes DDoS attack traffic before it reaches critical systems, eliminating downtime and ensuring optimal performance and maximum availability.
- Mitigates the impact of 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 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.
- Quickly defends against new and complex DDoS attacks by using Smart-Rules that adapt in real-time, ensuring continuous protection without downtime.
- Detects and mitigates attack traffic in real time instead of the minutes or tens of minutes required by traditional DDoS protection solutions.