Flexible, Scalable DDoS Protection

Your customers demand quick, smooth and continuous digital experiences. However, the threat from evolving cyberattacks, like distributed denial-of-service (DDoS) attacks, makes maintaining service availability challenging. Even for well-resourced teams, comprehending the variety of protection options against these attacks can be overwhelming. It’s an even tougher challenge when dealing with tight timelines, limited budgets and not enough staff.

The Corero SmartWall One Platform

These are the reasons why we’ve designed our SmartWall One DDoS protection platform around the principles of modularity and flexibility. We believe that a DDoS solution shouldn’t just be effective. It should be tailored to your unique needs, fitting seamlessly into your existing network infrastructure, offering a simple approach to enhancing your security posture. What sets SmartWall One apart is its ability to adapt.

Whether you’re just starting to build your DDoS defenses or looking to strengthen an established system, SmartWall One is ready to meet you where you are now and grow with your business. This platform aims to serve as a partner in your DDoS journey, providing the support you need today and preparing for the challenges you may face tomorrow.
Detect

DDoS detection is the first step to achieving full DDoS protection. Our approach utilizes packet header and payload inspection to detect malicious traffic, as well as aggregated traffic monitoring to identify known and previously unknown attack traffic patterns.

Mitigate

The goal of DDoS mitigation is to lessen the impact of an attack. SmartWall One intelligently and responsively employs the correct mitigation method to defend against the attack while protecting operations.

Protect

DDoS protection represents the final, ongoing stage in the DDoS defense journey. While detection focuses on identifying a DDoS attack and mitigation is about reducing its impact, protection is all about implementing intelligent, automatic countermeasures that accurately separate DDoS traffic from good traffic to maintain service availability.

DDoS Protection that Pays for Itself

DDoS protection-as-a-service (DDPaaS) is a service model that enables you to provide your customers with robust defenses against DDoS attacks. You can offer continuous monitoring and threat intelligence updates, helping your customers stay abreast of emerging DDoS attack trends. With the automated nature of SmartWall One and the backing of our industry experts, we reduce the burden for you to offer a DDoS protection-as-a-service. This not only enhances their security posture but also elevates their trust in your services. By offering DDPaaS, you position yourself as a proactive service provider that goes beyond providing internet services and ensures that your customers’ network infrastructure is secure, resilient, and trustworthy.

SecureWatch Managed Services

We understand that businesses like yours face unique challenges. Balancing the demands of providing top-tier services with the realities of limited budgets, staffing, and resources is no small feat. That’s why we’ve tailored our optional SecureWatch Managed Services to address these very challenges.

SecureWatch Managed Services represent a comprehensive set of services designed to optimize configuration, monitor network activity, and respond effectively to mitigation needs. Handled by our seasoned security operations center team, this service operates around the clock to ensure you’re always protected.

What makes SecureWatch stand out is that we take the time to understand your security policy requirements and business objectives. Consequently, each SecureWatch service plan is tailored to the specific needs of each SmartWall One customer. With SecureWatch, you’re not just enlisting a managed service, you’re enhancing a partnership that respects your unique requirements and business goals.

"GARR values the automated, hands-off efficiency of the Corero solution, which frees up staff to work on other tasks. Thanks to the Corero solution, we operate more efficiently. So, we estimate that we’re saving about 20% in terms of staff time dedicated to network security. It’s clear that no human, or even a team of ten security analysts, could react quickly enough to manage these sophisticated DDoS attacks."

- Massimo Carboni, CTO of GARR