As a service or hosting provider, you understand the ongoing challenges of pricing pressure on your core offerings. To increase revenues and stand out from competitors, value-added services are important. Corero SmartWall One DDoS protection is an attractive value-add service that can also serve as an additional revenue stream. With our services, you won't have to worry about complex 'per-tenant' policies as it is easy to manage through our convenient SmartWall Service Portal.

The threat of DDoS attacks is not to be taken lightly, as they can harm your reputation, brand, and bottom line. With the rise of such attacks and their average costs exceeding $200,000 per incident, now is the right time to safeguard your infrastructure, while generating additional revenue by offering this protection as a service to your customers.

SmartWall One ensures you are protected across every external point of connection in your network. With a simple addition of our service portal, that protection becomes a valuable ‘protection-as-a-service’ revenue opportunity.
**Proactive DDoS Protection**

Our market-leading, innovative SmartWall One platform delivers fast, automatic protection from DDoS attacks in seconds, rather than the minutes taken by legacy solutions. It automatically and surgically removes DDoS attack traffic, ensuring that ‘good’ user traffic remains flowing with no interruption or downtime to your network traffic. Flexible deployment topologies include:

» In-line appliances  » Infrastructure-based  » In the cloud  » Scrubbing centers

Protection is available in cost-effective increments which scale to tens-of-terabits, supporting your growing bandwidth requirements. SmartWall One solutions are the highest performing in the industry and provide robust DDoS protection coverage at unprecedented scale, with low total cost of ownership.

**DDoS Protection Service Flexibility**

Our service portal is highly customizable and is designed to work with your requirements, whether you are experienced with DDoS or not. Service levels are fully flexible and can be set up according to the number of tiers that you offer and the types of subscriber being protected.

**Providers can configure the service to:**

» Onboard customers and assign DDoS protection service levels
» Set up alerts and reports for customers
» View attack dashboards for each customer

**Protected tenant customers can:**

» Log in to their own view to access DDoS attack reports and dashboards
» Clearly see when there is an attack and when their traffic is protected
» Get comprehensive views of attack information from easy-to-understand dashboards
“Corero has provided a robust solution that protects NRBN and its customers from the increasing threat of DDoS attacks.”

Glenn Hynes,
Director of Network Technology and Business Transformation,
Niagara Regional Broadband Network (NRBA)

Key Service Benefits

Simple Lifecycle Management
Easy to onboard, update, set service levels or remove tenants from the system, as well as set automatic attack alerts to demonstrate the value of your DDoS protection to unsubscribed tenants.

Automated Reporting
Scheduled email reports to every tenant, demonstrating the benefits of your DDoS protection service.

Easily Customizable
Login screens, service descriptions, terms of service, logos and password policies can all be modified to match your branding and service offering.

DDoS attack analysis dashboards for protected tenants
Technical Specifications

Service Visibility

Provider Login
Live and historical reporting on attack size and duration
Service overview and per-tenant views

Tenant Login
Live and historical reporting on attack size and duration
User management

Service Enablement

Service Policy
Configurable bandwidth-based service tiers

Alerting
Operator and per tenant configurable attack start, stop and service level notifications
Email or webhook (Slack/Teams) alerts

Physical Environment

Hypervisors
VM using Linux server (Redhat Enterprise 7+, Centos 7+, Ubuntu 16.04+, Debian 9.9) vCenter Server 6.5+ with ESX/ESXi 6.5+

System Requirements
Memory: minimum 16GB, recommended 32GB   Disk: 400GB

System Capacity
10,000 tenants