SMARTWALL®
SERVICE PORTAL

DDoS Protection as-a-Service

Service and Hosting Providers face ongoing pricing pressures on their core offerings. To increase revenues and differentiation from competitors, Providers are increasingly looking to value-add services. SmartWall® DDoS protection is an attractive value-add service, that requires no complex 'per-tenant' policies to be managed and is simple to deliver using the SmartWall Service Portal.

Providers and their tenant customers are inseparably linked by the damage that DDoS attacks can have on reputation, brand and revenue. With DDoS attacks on the rise and associated costs typically above $200,000 per incident, this is an ideal opportunity for Providers to protect their own infrastructure from these damaging attacks and generate incremental revenue by offering that protection as a service to tenant customers.

Corero’s SmartWall ensures Providers are protected across every external point of connection in their network. With a simple addition of the purpose-built SmartWall Service Portal to the solution, that protection becomes a valuable ‘protection-as-a-service’ revenue opportunity.

**A Value-Add Service Revenue Model**

Create a differentiated offering to retain existing customers and attract new ones

Deliver an enhanced service with automatically protected infrastructure, eliminating service outages and latency issues from DDoS attacks

Generate incremental revenue with premium DDoS protection as-a-service, providing attack visibility for protected customers and a rapid ROI on deployment and operating costs

---

Proactive DDoS Protection

Corero’s market-leading, innovative DDoS protection solutions deliver real-time mitigation of attacks in seconds, rather than the minutes taken by legacy solutions. They automatically and surgically remove DDoS attack traffic, ensuring that the 'good' user traffic remains flowing with no interruption or downtime.

Flexible deployment topologies include:

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

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

---

**Corero DDoS Protection delivered as-a-service, by adding the SmartWall Service Portal**

| N - Network Defense Device | M - Provider Service Management | P - Service Portal |
DDoS Protection Service Flexibility

The service portal is highly customizable and is designed to work with the Provider's requirements, whether they are experienced with DDoS or not. Service levels are flexible and can be set up according to the number of tiers being offered and 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
» Easy-to-understand dashboards give comprehensive views of attack information

"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 Benefits

**Simple Lifecycle Management**
Easily onboard, update, set service levels for, and remove tenants from the system. Providers can configure automatic alerts to enable proactive management of the service, increasing sign-ups of unsubscribed tenants and upselling existing tenants to a more comprehensive service.

**Easily Customizable**
Login screens, service descriptions, terms of service, logos and password policies can all be modified to match a provider’s branding and terms of service.

**Per Tenant Visibility**
Focused dashboards and real-time alerts enable providers and their tenants to understand the frequency, size and details of attacks and show the value they get from the service.

**Automated Reporting**
Scheduled email reports to every tenant, demonstrating the benefit they are receiving from the DDoS protection service.

**Attack Analysis Tools**
Live and historical attack traffic can be monitored and analyzed by packet rate and bandwidth. Detailed DDoS attack analysis includes visibility into:
- Top Source Addresses
- Ports, Protocols and Packet sizes
- Source Countries and Autonomous System Numbers (ASN)

**Easy Integration**
As well as enabling a comprehensive standalone solution for multi-tenant service enablement, a built-in programmatic interface ensures simple, but powerful, integration with existing customer lifecycle management and reporting tools.

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

**Management**

**Web-Based GUI**
HTTPS secured portal login
Fully customizable tenant login screen

**Secure Authentication**
Role-based access via LDAP

**Programmatic API**
JSON-based REST

**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

[corero.com](http://corero.com) | [info@corero.com](mailto:info@corero.com) | [info_uk@corero.com](mailto:info_uk@corero.com)