

CyberDAM. DDoS Protection Service for MSSPs

Differentiate yourself with the fastest DDoS mitigation SLA

The CyberDAM-DDoS protection solution lets you expand your offering with enterprise-grade DDoS mitigation services - quickly, at no risk, and with zero capital investment. It brings together best-in-class technology, DDoS experts, and an SLA commitment for the best attack detection, notification and mitigation response times.

CyberDAM-DDoS protects against volumetric attacks, which attempt flooding the network and cause extensive service disruption for legitimate users, as well as handles application-layer attacks, which target server computing resources and can be more difficult to mitigate.

Offered as a white label, outsource service, CyberDAM-DDoS is based on a robust cloud infrastructure that can mitigate attacks reaching hundreds of Gbps, which cannot be handled by DDoS protection appliances installed at the perimeter of datacenters or by an ISP service. CyberDAM-DDoS includes:

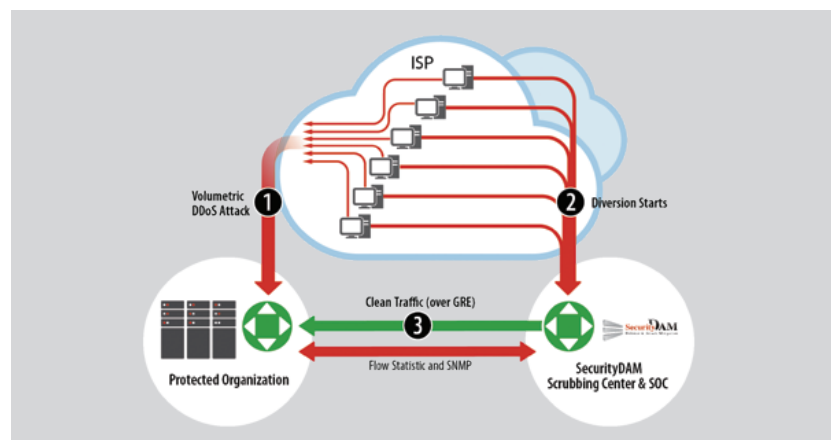
- On-demand or always-on cloud DDoS protection
- Global network of scrubbing centers with over 2Tbps of mitigation capacity
- Web-based DDoS management portal
- End-customer self-service portal
- 24/7 Security Operation Center (SOC)

Cloud Mitigation: On-Demand or Always-On

CyberDAM-DDoS lets you offer monitoring, detection and mitigation of DDoS attacks, regardless of your customer location, number of services or protected assets/networks, ISP connections or network configuration. It is offered in two modes: On-Demand and Always-On.

On-Demand service constantly monitors customers' protected assets to identify the emergence of volumetric DDoS attacks, using one or more of the following methods:

- Analyzing NetFlow records and SNMP queries
- Communicating with a dedicated DDoS protection appliance such as Radware's DefensePro, thereby creating a hybrid DDoS protection service
- Monitoring the availability and response time of customers' internet-facing services



Once a volumetric attack is detected, traffic is re-directed through our global network of scrubbing centers, using BGP routing advertising or DNS changes, depending on the network configuration. Traffic diversion may also be triggered via a request on the service portal, by communicating directly with the SOC, or using the SecurityDAM API.

The Always-on service routes traffic through our scrubbing centers at all times to automatically detect and mitigates both volumetric and application level DDoS attacks.

Scrubbing Centers Global Network

Located at main internet intersections, our global network of scrubbing centers provides a mitigation capacity of over 2Tbps. It enables filtering data and passing only legitimate traffic to a customer's data center using GRE tunnels or proxy servers.

Each center can absorb the largest volumetric attacks and handle redirected customer traffic, while ensuring the highest availability and adding only minimal latency.



Scrubbing centers are designed in full resilient mesh topology, based on N+1 redundancy on all networking (routers, switches, load balancers) and mitigation elements, as well as GRE tunnels to end-customer data centers. This ensures continuous operation of each scrubbing center during maintenance and/or element failure.

To provide high capacity and availability at all times, as well as flexibility in customer diversion options, our scrubbing centers are connected to the Internet through multiple Tier1 carriers for internet connectivity and backup each other.

DDoS Service Management Platform

A web-based portal – the SecurityDAM Control Center (SDCC) – lets you easily manage all DDoS protection operations. Using intuitive dashboards, you can:

- View alerts and monitor traffic for multiple customers
- Monitor and audit mitigation activities
- Manage subscriptions with multi-role customer options
- Provision services and manage accounts

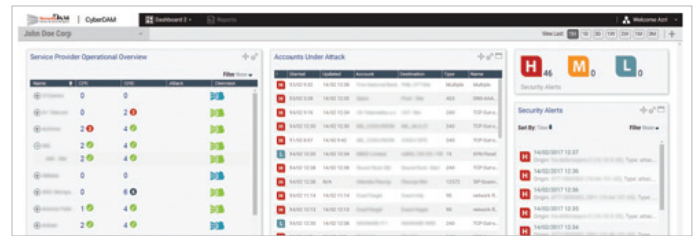
Benefits

- **DDoS Protection Services with Zero Capital Expenditure (Capex)**, leveraging SecurityDAM's cloud infrastructure
- **Over 2Tbps of Mitigation Capacity** through a global network of scrubbing centers
- **Flexible Deployment Options** including on-demand or always-on DDoS protection
- **Easy Management** of DDoS services via a dedicated MSSP and customer portals

About SecurityDAM

SecurityDAM is a leading provider of best-in-class cloud-based security solutions, helping organizations gain the highest possible level of security. The CyberDAM robust solutions suite, addressing cyber security challenges such as Distributed Denial of Service (DDoS) attacks and network/application Vulnerability Assessment. Using our multi-tenant management platform, global network of scrubbing centers and SOC services—we offer unmatched protection solutions for network and services. Founded by a team of security experts, SecurityDAM is a member of the RAD group.

For more information, visit www.securitydam.com



End Customer Portal

A web-based portal provides end customers with insight into the service status, provisioning and past performance. The portal can be branded with your name and logo and provides customers with:

- Real-time view of protected assets, incident info, traffic, - and mitigation stats
- Analysis of attack data including vectors, sources and destinations
- Reports covering historical data, trends and forensic analysis
- Self-provisioning of protected assets and users



DDoS Security Operation Center

SecurityDAM's Security Operation Center (SOC) is staffed 24/7 with top DDoS security experts to provide the fastest and most efficient response to DDoS attacks and any ongoing issues. The SOC provides:

- Provisioning of new customers, customer support and help desk.
- 24/7 monitoring of customers' protected assets, with immediate awareness and response to attacks.
- Quick analysis of attacks and execution of any necessary DDoS prevention methods.
- Analysis of zero-day attacks and setup of new signatures for successful mitigation.

- **24/7 DDoS SOC** with an emergency response team
- **SSL Traffic Attack Detection** supporting the detection and mitigation of DDoS traffic in SSL sessions, while maintaining the connection integrity.
- **Quick Onboarding** with a dedicated professional services team – tailoring our service to your, or your customer's specific environment including integrating with OSS/BSS systems
- **ISO 27001 Certified**

