

# HYBRID-CLOUD DATASHEET

## Adapting to Modern Challenges: Harnessing the Power of a Hybrid-Cloud DDoS Solution



### Meeting the challenge head-on

Keeping your business up and running is essential. But how do you do this in a modern digital age where bandwidth needs keep increasing, and attack methods become more severe? The answer is simple: you adapt with a Hybrid-Cloud approach. This strategy combines the instant response of on-premises solutions with the scalability and flexibility of cloud-based services, ensuring robust protection against the broadest range of DDoS attack types and intensities.



### So, how do we do it?

We've been defending our customers with a powerful software-based solution that is among the fastest at detecting and protecting against DDoS attacks. Now, by partnering with leading and trusted cloud service providers, we offer a single, turnkey solution that defends against even the largest attacks, those that exceed on-premises capacity.

**A Hybrid-Cloud solution helps you bridge the gap**—when traffic becomes excessive, it's rerouted to our cloud-based service, preventing your infrastructure from being overwhelmed. This strategy effectively mitigates threats and curbs network congestion, all while preserving the speed and availability of your applications and services. Our two-layer integration handles attacks efficiently, whether they're small and sophisticated or large and volumetric. Plus, our hardware-agnostic, software-based solution ensures consistent traffic visibility and filtering, **keeping your services available and secure.**



**Building on the necessity for robust defenses, it's crucial to recognize that the sophistication of DDoS attacks continues to evolve, presenting more complex challenges with their scale and severity. Given that the average attack duration is brief, real-time detection and blocking become indispensable for comprehensive protection, underscoring the value of a Hybrid-Cloud solution that is designed to meet these dynamic challenges head-on.**



## Benefits that make business sense



### Affordability

Keep costs low by prioritizing on-premises protection and routing traffic to the cloud only when necessary. A hybrid approach is far more cost-effective than a cloud-only solution, preventing business impacting downtime and utilizing cloud resources ONLY when needed.



### Adaptive & Scalable

Our solution dynamically adjusts to handle the various types of DDoS attacks, regardless of their size or complexity. Enjoy the low-latency response of an on-premises solution combined with the massive scalability of a cloud-based service.



### Minimal Touches

Reduce your IT workload with our automated protection, which cuts down on management tasks and streamlines resources with key traffic insights and robust support. This lets you and your team focus on what you do best.



### Flexible & Effective

Our solution simplifies deployment and daily management, including leveraging your existing network hardware, to ease the load on your teams. With no vendor lock-in, you can reduce initial investment and use our partner relationships to enhance protection across your entire network.



### Service Availability

A Hybrid-Cloud solution enhances your ability to protect your network, meet your SLAs, and keep your customers happy. With hybrid on-demand, cloud defense you're safe from even the biggest attacks.

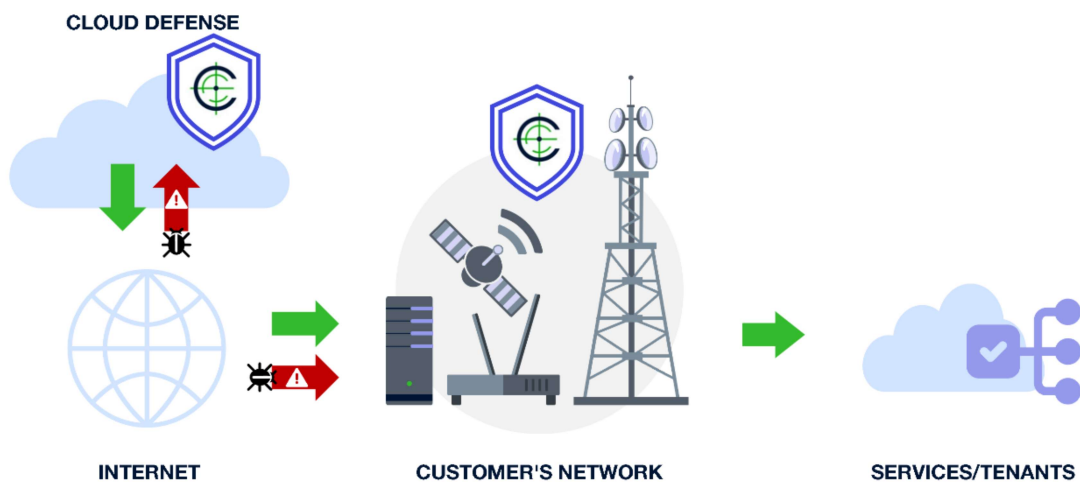


### First-Class Support

We understand how critical it is to keep your services up and running. Our knowledgeable support staff are available 24/7, ensuring your problem is solved by the first agent who answers your call, without bouncing you around.

## A closer look at how it works

Check out the chart below to see how traffic is managed with our Hybrid-Cloud solution.



Scrubbing Capacity	20Tbps of Dedicated Capacity
Scrubbing Centers	36, Globally Distributed
Redirection Method	BGP, Signaled automatically from on-premises defense



### Centralized management and analytics

Our robust analytics delivers comprehensive visibility into DDoS attacks with easy-to-read dashboards delivering actionable intelligence.



### Monitor in Real-Time

Information is presented in real-time or historical charts and dashboards.



### Optimize Protection

Gather traffic information to help you fine-tune policies.



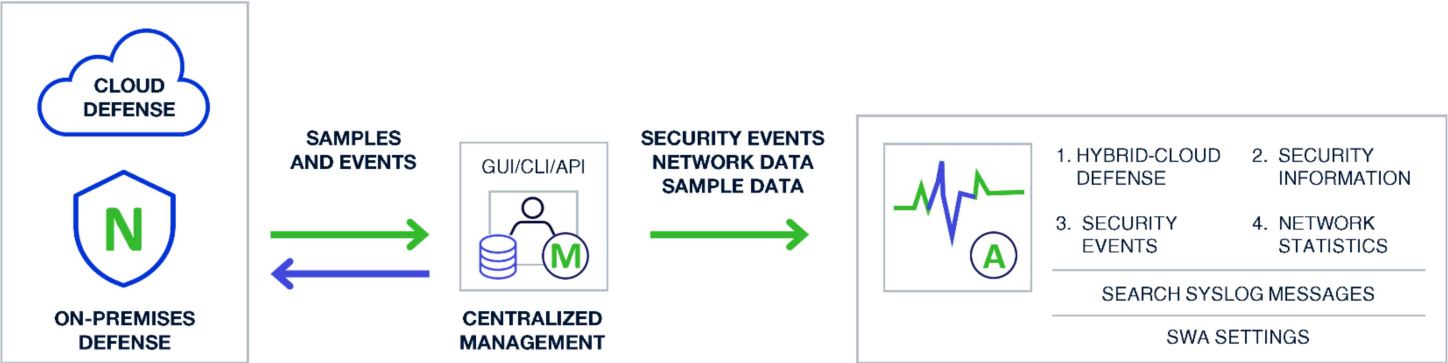
### Analyze Attacks

Drill down into blocked and allowed traffic seen an attack.



### Enhance Threat Intelligence

All events are securely stored, indexed in our web-based application, and made accessible for analytics externally to other security tools via syslog, enhancing integration and visibility.



N Network Defense Device | M Provider Service Management | A Analytics



## Underneath the hood

### Volumetric DDoS

- TCP Flood
- UDP Flood
- UDP Fragmentation
- SYN Flood
- ICMP Floods

### Reflection DDoS

- NTP Monlist
- SSDP/UPnP
- SNMP Inbound
- Chargen
- DNS
- Connectionless LDAP (CLDAP)
- Memcached
- Portmapper
- Netbios
- RIP

### Resource Exhaustion

- Malformed and Truncated Packets (e.g. UDP Bombs)
- IP Fragmentation/Segmentation AETs
- Invalid TCP Segment IDs
- Bad checksums and illegal flags in TCP/UDP frames
- Invalid TCP/UDP port numbers
- Use of reserved IP addresses

