CONTINENT8 technologies

DDOS

secure8

SECURE | DDOS

Effective, scalable protection against DDoS

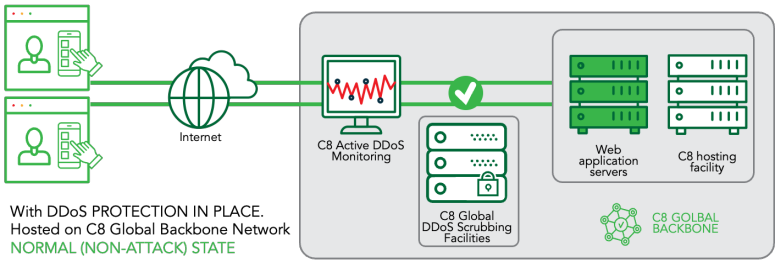
We've been protecting the world's most valuable information for over 20 years

The Continent 8 (C8) DDoS defence service is a mature, proven platform, built and developed over 17 years, using an optimised combination of technologies and our customised development layer. The key technology partners for our monitoring, detection and mitigation environments are A10 and Nokia.

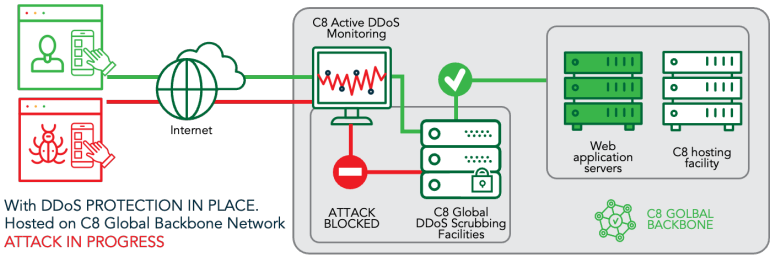
Typical time to mitigate a DDoS attack is 30-60 seconds

On-net protection

- On-net DDOS protection is for customers who are hosted within C8's data centres or utilise C8's IP bandwidth in third party locations.
- Customers can make use of C8 public IP address ranges or 'bring their own' Provider Independent ranges (subject to certain configuration criteria).
- On-Net mitigation of DDoS traffic is wholly under the control of C8 and will be achieved through automatic diversion using BGP route injection and dedicated VRF's.



- Ingress traffic is distributed around the edge of the C8 network at a point closest to the source.



- Real-time attack data can be seen by the customer in the C8 Portal, where custom whitelist configurations can also be created.

- Under DDoS attack conditions, traffic is diverted to the multi-node mitigation platform hosted within the C8 global backbone network. The platform selects to use the geographically closest scrubbing node to the source of the attack.
- In addition to scrubbing, network edge filtering can be achieved using BGP Flowspec. This can be deployed based on information shared by customers regarding their active ports and protocols.

Aggregate on-net scrubbing capacity of 1.2Tbps.

Total scrubbing capacity of 50Tbps+ is available through carefully designed upstream agreements and systems.

Global distributed architecture with four scrubbing centres in optimal geographic locations.

Traffic is scrubbed at the closest entry point using our many Edge and IX locations in **Europe**: London, Dublin, Paris, Milan, Lisbon, Amsterdam, Marseille, Sofia, **North America**: New York, Newark, Los Angeles, Chicago, Dallas, Montreal, Toronto & **Asia**: Hong Kong, Singapore, Tokyo.

A10

Our A10 mitigation platform, which has been optimally integrated with our wider infrastructure, delivers a full suite of attack countermeasures that surgically remove attack traffic while maintaining legitimate traffic flow without interrupting network services.

NOKIA

Nokia Deepfield traffic monitoring and analysis delivers pervasive network visibility and actionable intelligence so we can proactively secure our customer network services, improve network performance and reduce costs.

GET IN TOUCH
sales@continent8.com

Asia: +65 3165 4649
Europe: +44 1624 694625

Latin America: +54 11 5168 5637
North America: +1 514 461 5120

CONTINENT8.COM/SECURE

FACEBOOK TWITTER LINKEDIN YOUTUBE

CONTINENT8 technologies

DDOS

secure8

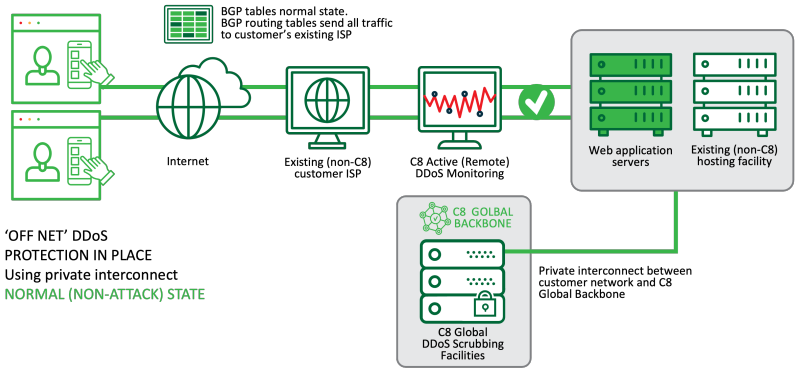
SECURE | DDOS

Off-net protection

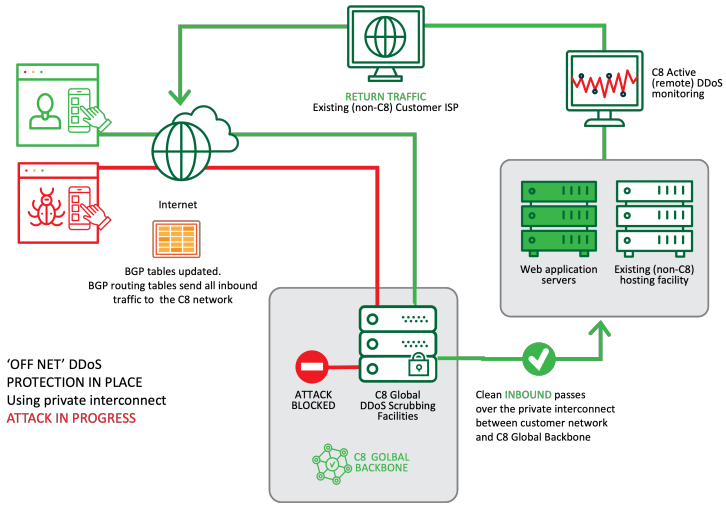
- Off-net protection is available for customers that do not use C8's IP bandwidth.
- Customer Internet traffic can either be advertised permanently by C8 so that traffic is continually routed via our network for effective DDoS monitoring and automatic mitigation, or manually diverted to C8 in the event of a DDoS attack (subject to the customer's network configuration).
- C8 can assist with the remote monitoring of sites to identify any attacks and advise when our DDoS mitigation services are required.
- There are two options available for monitoring and returning traffic to the customer's hosted infrastructure: direct delivery via an encapsulated private circuit, or using a GRE tunnel across the Internet.

Off-net option 1: Direct delivery using a private circuit

- Physical connection installed between C8's global network and the border routers of the customers network (for resilience two separate circuits recommended).
- C8 will perform private monitoring and profiling of the customer traffic, via the private circuits, using NetFlow, BGP and SNMP information from the customer routing equipment.



- When an attack is detected on a customer address range:
  - The address range will be advertised via BGP across C8's global network instead of with customer's existing ISP. (NB: the customer must have a minimum /24 provider independent public IP address space to subscribe to this service).
  - All inbound traffic bound for the customer (both attack traffic and legitimate) will then be routed to the C8 network and 'scrubbed', with clean traffic passed to the customer over the private circuit(s). (Outbound traffic will still route from the customer to the Internet over their 'normal' ISP).
  - This option is superior to using a GRE tunnel, as customer traffic is delivered over a private network on dedicated bandwidth, so backed by SLA.



TECHNICAL SUPPORT
support@continent8.com

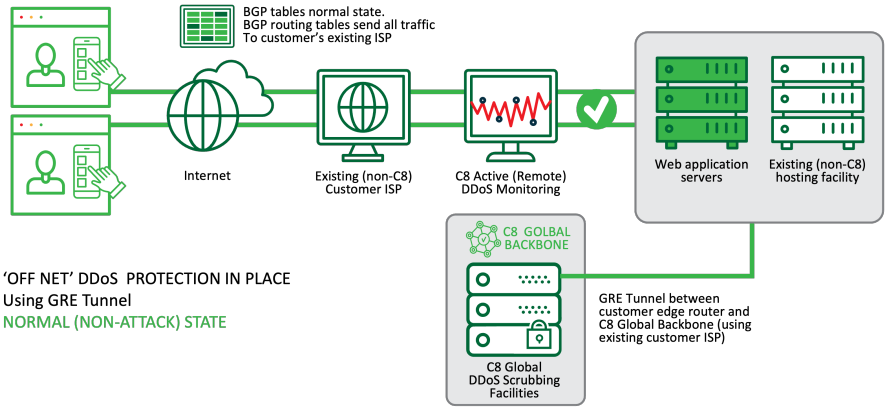
Asia: +65 3165 4796
Europe: +44 1624 694611
Latin America: +54 11 5168 5643
North America: +1 514 461 5111

CONTINENT8.COM/SECURE

FACEBOOK TWITTER LINKEDIN YOUTUBE

Off-net option 2 - IP Transit Delivery using a GRE Tunnel

- In this method, a GRE tunnel connection is established over the Internet between C8's core routers and customer's routers.
- When an attack is detected on a customer address range, the address range will be advertised via BGP across C8's global network instead of with customer's existing ISP. (NB: the customer must have a minimum 24 provider independent public IP address space to subscribe to this service).



- In the event of an attack, all inbound traffic bound for the customer (both attack traffic and legitimate) will then be routed to the C8 network and 'scrubbed', with clean traffic passed to the customer over the previously configured and tested GRE tunnel. (Outbound traffic will still route from the customer to the Internet over their 'normal' ISP).
- The GRE tunnel is able to retain all originating packet information, so the user's source IP and HTTP header info is all retained due to the encapsulation. • This option is inferior to the direct delivery method, as delivery of traffic over the Internet cannot be guaranteed. Further, if the customer existing ISP (i.e. not C8) is being attacked, or has bandwidth volume issues, this method may not allow for successful mitigation.