DDOS PROTECTION AS A SERVICE (DDPAAS)

REAL-TIME, ALWAYS-ON AND SCALABLE MANAGED DDOS MITIGATION SOLUTION

KEY BENEFITS

✓ **Cost Effective & Scalability**
Mitigate the risk of a DDoS attack through a fixed and transparent OPEX monthly rental, priced to match your connectivity bandwidth as it scales.

✓ **Business Continuity**
The service keeps subscribers' services online for the attack duration – there is no sustained loss of service on-premises or in our Data Centre.

✓ **Fully Managed Service**
The service is 'always-on', protecting your cloud infrastructure or website around the clock. Delivered as a fully managed service, we deploy our expertise so you can focus on business outcomes.

✓ **Performance**
The mitigation has minimal impact on your host system as our inline solution architecture reduces traffic delays. Unlimited bandwidth protection is also available.

✓ **Comprehensive Protection**
Combined to defends against volumetric and application layer DDoS attack vectors.

Maintaining business continuity is critical - Distributed Denial of Service (DDoS) attacks threaten to disrupt that.

DDoS attacks overload your IT infrastructure, services and applications with malicious traffic, rendering them inaccessible to legitimate users. In addition, DDoS attacks are often used as a distraction technique while more sophisticated attacks are launched.

The result? Low productivity, lost revenues, reputational damage and the potential loss of sensitive data.

DDoS Protection stops attackers in their tracks. Our automated, always-on and scalable DDoS mitigation service identifies and discards malicious traffic, while legitimate traffic is forwarded as normal. We deliver this in a simple and transparent offering for a fixed monthly fee – a service with no surprises, fully managed by our team of experts.

DDoS attacks are frequently launched by hackers controlling Botnets – a cloud-based swarm of remotely controlled devices. In a typical attack, the resource of the target system is exhausted by the demands of the Botnet, either in terms of bandwidth or webpage requests. An attack can last for anything from an hour to several days, and during this time, internal and external users will be unable to access web content and cloud services. This will impact your stakeholders via loss of productivity, share price and online revenue.

Node4's DDoS Protection service provides a network traffic 'scrubbing', which allows us to re-direct high volumes of in-bound 'dirty' traffic away from our ISP infrastructure on which your connections are provisioned. Only valid 'clean' traffic is fed back in and reaches its correct destination. This mitigation is managed reactively when our intelligent network analytics detect abnormal traffic loads.

In addition to these 'volumetric' based attacks, application layer DDoS attacks – known as 'low and slow' - are rapidly becoming the most common type of attack on UK Data Centres, and 80% of attacks are below 50Mbps – small enough to slip past the volumetric network defences. Often, when used in conjunction with each other, the volumetric attack can mask the more subtle applications layer exploitation. So, with DDoS Protection as a Service your infrastructure is proactively protected from both attack vectors. Our intelligent network analytics are constantly monitoring your traffic looking for tell-tale changes in traffic patterns. Any traffic which is detected as anomalous is blocked before it reaches the host system, mitigating this "low-and-slow" application-based intrusions as well.

DDOS PROTECTION AS A SERVICE (DDPAAS)

BUSINESS CONTINUITY & CUSTOMER CONFIDENCE

Resilience
Withstand attacks without dropping good traffic, so you won't lose revenue or productivity.

Responsive and pro-active
Multi-layer defences against web security threats, malicious bots, volumetric and application-based DDoS attacks.

Always-on protection
Your global enterprise systems or customer facing web sites are likely to be in use outside of regular business hours, evenings and weekends. Not only are they the times when you are reliant on out-of-hours operational support - they are the most likely times for DDoS attacks. So having an always-on solution in place ensures your business is protected without delay, 24x7x365.

Compliance
Helping you to meet infrastructure and application security compliance requirements.

BEST PERFORMANCE

Fastest throughout
The service is delivered through our cloud delivery approach, with carrier-grade flexible infrastructure positioned at the network edge to ensure lowest latency and the ability to scale.

The inline service is transparent to your traffic which will continue to flow with minimal latency, offering a great user experience.

Effective from day zero
The service offers immediate mitigation and does not need to learn before it is effective; it protects your organization as soon as it is turned on.

Your users will be unaware of the mitigation, they don't need to evoke the service, and with Node4's accurate detection of malicious traffic legitimate traffic will continue unimpeded.

Extensive protection
Multiple approaches to DDoS mitigation combine in this one service, so even complex dual approach attacks can be stopped in their tracks.

INDUSTRY LEADING TECHNOLOGY

Heuristics engine
A Heuristics-based engine leverages behavioural analysis to track and rate-limit DDoS attacks.

Up-to-date protection
In conjunction with the cyber security community, attack 'signatures' detected by a range of agencies are used to inform the service, ensuring it is aware of the very latest attack types and vectors.

MANAGED SERVICE

Expert engineers
Our UK-based team of accredited engineers are highly experienced in delivering complex network solutions.

SLAs
Guaranteed performance backed by rigorous service level agreements.

Fully managed service
We provide friendly, flexible options for 24x7x365 service including access to reports and statistics.

SECURITY EXPERTISE

The service can be combined with other Node4 security services and overlayed with a SOC service, to take a layered approach to your organisation's cyber security and to improve your security posture.

AVAILABILITY

Any location
Protects the services of subscribers on the node4 network and connections provisioned by Node4.

For those offering time-critical or customer-facing services, this option is of particular importance to customers hosting essential services in a Node4 data centre.

Range of bandwidth options
Protecting customers at whatever bandwidth drives their business.