Pulsant
Business Unlimited

DDoS best practice

Can you do it alone?

Introduction

DDoS or distributed denial of service attacks are increasingly in the news spotlight — from high-profile breaches like Talk Talk, to the arrest of two teenagers responsible for DDoS for hire services. The reason is that DDoS attacks are on the rise and are targeting organisations of every size in every industry — in fact, according to Cisco, in 2015 these attacks rose by 25% from the year before.

Historically it was businesses in finance or banking that were targeted by cyber criminals, but today everyone is at risk because organisations simply can't afford the risk of downtime. This makes financially-motivated attackers bolder, something that's clearly demonstrated by a PwC report revealing 90% of large organisations and 74% of small businesses suffered a breach in 2015, up 81% and 60%, respectively, from the year before.

But as an organisation, what should you be doing to protect yourself and prepare for the inevitable? The next obvious question is: can I do it myself? The answer is no, not unless you are a tier one organisation with the budget and resource (and network capacity) to switch bandwidth and redirect traffic during an attack. On the other hand, DDoS protection isn't something that you should be completely outsourcing either. Rather, work with your service provider to make sure you've got the right cover, in the right places.

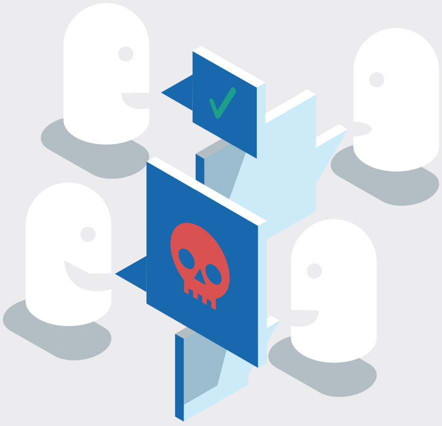
So apart from having the right network intrusion and firewall solutions in place, you should evaluate your current and/or future service provider. This is particularly important if you're in e-commerce or host your business critical data and systems in the cloud. While your organisation could be targeted directly, there is also the danger that you could be affected indirectly if your service provider or one of its customers is attacked.

Typically you should look at three areas when evaluating your service provider: assessment, mitigation and continual protection. This is essential as an overall approach, but there are also specifics within this that you should also consider.

A PwC report revealing 90% of large organisations and 74% of small businesses suffered a breach in 2015, up 81% and 60%, respectively, from the year before.

Assess — DDoS attack readiness

Working with your service provider you should examine your business processes and identify which areas are most at risk. In this way a customised risk profile can be developed. Typically your service provider should have a dedicated team of security specialists or professional services staff who have the expertise to carry this out. Once your organisation has been assessed, they can then develop a mitigation plan and suggest the appropriate enhancements to IT security, as well as help guide risk-reduction planning. Importantly, this step enables you to understand exactly what your DDoS attack readiness status is.

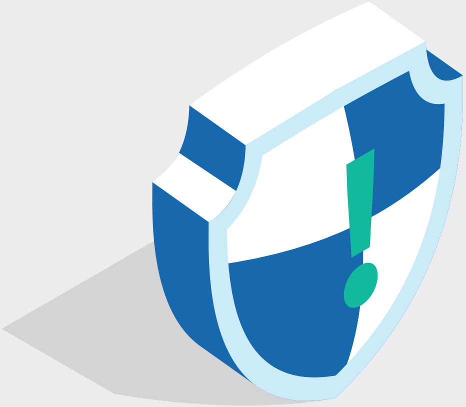


Mitigate — minimise the impact

Proper DDoS protection is about reducing the impact of an attack — because no security solution is 100% effective. As a result, working with a provider that has the capacity to guide you through an attack and help you mitigate the risk is essential. Does your provider have the technology and expertise to detect (proactively identify a threat), mitigate (minimise the effects of an attack), and monitor (keep an eye on your network on a continuous basis)? This could very well be part of automated approach — using techniques like scrubbing and blackholing — that removes “bad” traffic or re-routes all of it, effectively taking your site offline.

Ongoing protection

DDoS mitigation isn’t a one-off activity. The very nature of DDoS and the way in which attacks are evolving and adapting to the security landscape means that your protection strategy needs to change, too. In fact, your service provider should be working with you to ensure that your strategy is adapting and evolving, not only to the changing threat profile, but also according to changes that are occurring in your business, whether that’s implementing new infrastructure or business processes, or expanding into new markets.

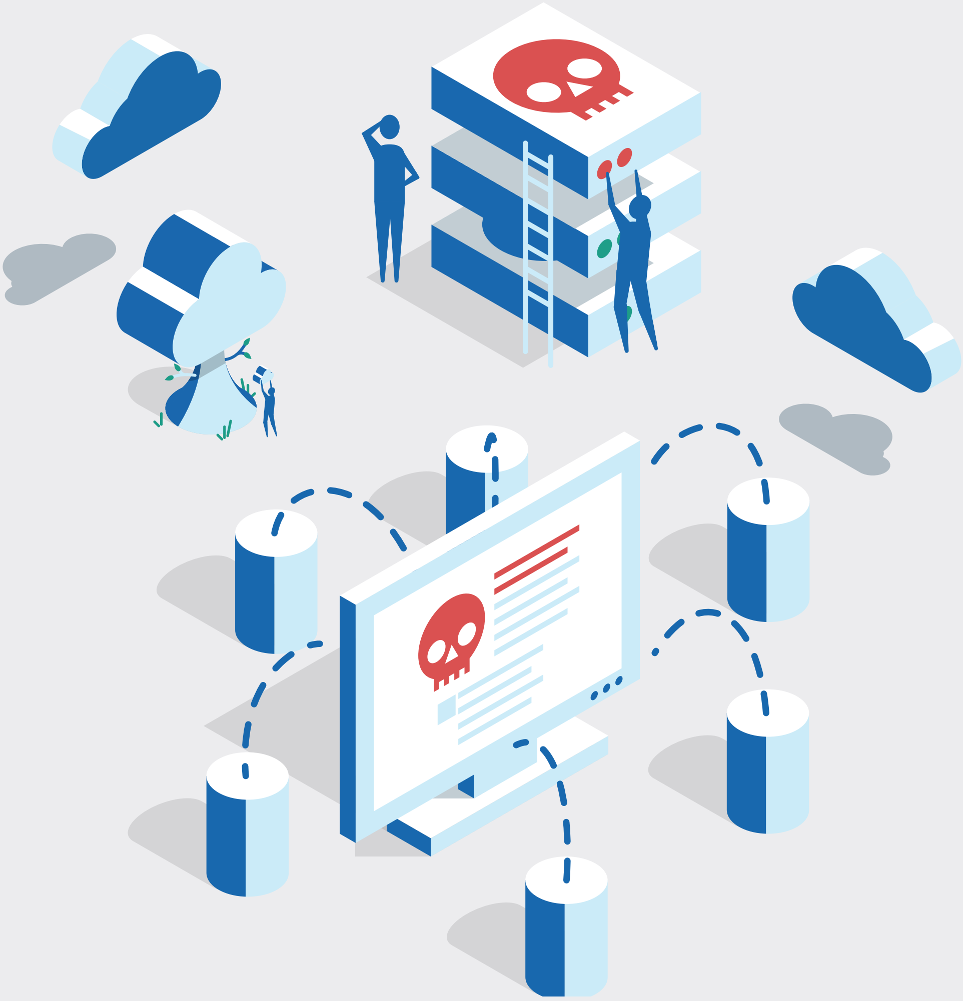


About DDoS

The key thing to remember about DDoS is that no-one is immune. That's not scaremongering; it's a fact backed up a number of high profile attacks and research, such as findings by Neustar that shows in 2015 73% of global brands experienced a DDoS attack.

Findings show that in 2015 73% of global brands experienced a DDoS attack.

As a business you need to do what you can to keep your brand and bottom line safe. And you also need to recognise that you can't do it all yourself — it's here that your relationship with your service provider can really help ensure you don't fall victim to DDoS and if you do, that the impact is low.



Challenge Pulsant to fulfil your business aspirations…

Contact Routes

Sales

Available:	**9am - 5pm Monday – Friday**
Telephone:	**0845 119 9911**
Email:	**sales@pulsant.com**

Accounts

Available:	**9am - 5pm Monday – Friday**
Telephone:	**0845 119 9999**
Email:	**accounts@pulsant.com**

Project Management

Available:	**9am - 5pm Monday – Friday**
Telephone:	**0845 119 9970**
Email:	**pmteam@pulsant.com**

Find out how we can help your organisation, call **0845 119 9911** or visit **www.pulsant.com**

Digital Marketplace supplier GOV.UK

CSA STAR CERTIFICATION

ISO 9001 FS 584994

ISO 14001 EMS 596899

ISO 27001 IS 571965

Cadogan House, Rose Kiln Lane
Reading, RG2 0HP

info@pulsant.com
pulsant.com

Pulsant
Business Unlimited