ARBOR NETWORKS
The Security Division of NETSCOUT

arbornetworks.com

DDoS IN THE CLOUD:

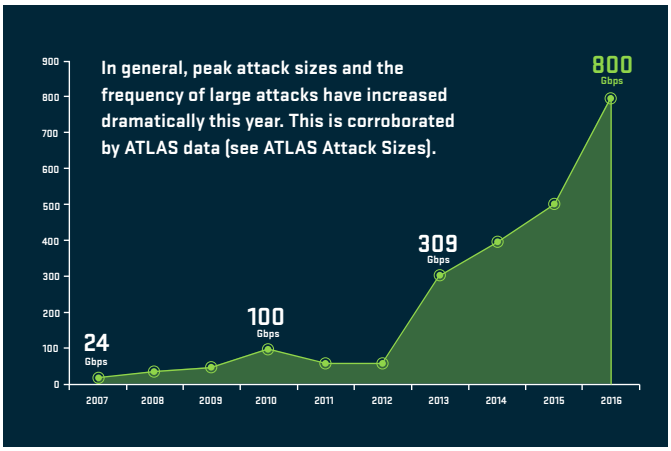
UNDERSTAND THE THREAT, MITIGATE AGAINST HARM

How present is the threat?

In recent years, one of the most dominant trends in enterprise computing has been the growth of cloud computing in corporate IT service delivery.

But along with the many upsides to this, there have been some unavoidable downsides too, including the extent to which it has put many corporate networks - and their users - directly in cyber attackers' line of fire.

One of the attack types growing in frequency and intensity is the distributed denial of service (DDoS) attack. Not only are they increasingly frequent (and growing in size, as the graph below illustrates) they are also widespread and indiscriminate – which makes them harder to plan for and recover from.



All-in-all, DDoS attacks – in which excessive levels of traffic flood the bandwidth or resources of a targeted system – are fast becoming one of the areas of greatest concern for corporate cyber security professionals, and those tasked with maintaining operations at organisations of all sizes, regardless of sector. While not a new problem, the size and scale is heading skywards at an alarming rate, driven in part by the growth in the number of botnets used to deploy these attacks.

According to Arbor Networks' latest Worldwide Infrastructure Security Report (WISR), only 8% of data center operators had experienced more than 50 DDoS attacks, or attempted attacks, per month in 2015. By 2016 that figure had grown to 21%.

The largest attack reported in 2016 was 800Gbps, which is in excess of the level most ISPs can withstand without suffering infrastructure-level damage or dropping clients' legitimate traffic. And while we're accustomed to reading in the media about 'sustained' attacks, the truth is an attack lasting as little as one minute could still lead to many hours of unplanned downtime.

Having to endure several hours of unexpected downtime is not an acceptable outcome to any business. Least of all one where connectivity is a fundamental part of its operations, like a media company, for example. Or one where ensuring availability to customers is vital, such as a retail bank. If your organization was hit by a prolonged period of unplanned downtime, it's not a question of whether or not you'd be affected; it's a question of how badly. And we're not just talking about your business operations but your hard-won reputation too.

Arbor Cloud runs the largest purpose-built DDoS mitigation network available, with the capacity to mitigate against even the largest attacks. Arbor Cloud's capacity is on target to reach 8Tbps. That's 10 times the size of the largest attack reported in 2016.

What is the scale of the current level of threat?

The largest attack of last year, which measured 800 Gbps, could be regarded as an exception. While that is statistically accurate, it shouldn't be the cause of any complacency. The average attack size may be considerably smaller at around 2-3Gbps, but that could be more than enough to put your internet connectivity in jeopardy - maybe even sever it completely. Even a data center with multi-Gbps bandwidth capacity could be overwhelmed by an attack of that size, and the scale of the problem is growing. We've already reached a point where 41% of enterprise organizations and 61% of data center operators have reported attacks exceeding their total Internet capacity. Plus there have been reports of multiple, combined attacks in excess of 1Tbps.

The Mirai botnet affected around two million Internet of Things (IoT) devices last year. Hot on its heels this year is the Reaper botnet, which is adding enslaved devices to its network by means of malicious code injections. If some industry predictions are right, and there will be more than 20 billion IoT devices by the year 2020, there is clearly enormous scope for botnets to wreak havoc via their expanding networks.

Some of the statistics detailed in our WISR report illustrate the extent of the current threat. For example, 61% of data center operators told us about attacks that completely saturated their data center's bandwidth. The effect of that was they couldn't guarantee availability of all the services they were providing to their hosting customers. What that means is that even if you're not the target of the attack, but you are reliant on a service provider that is affected you could be taken offline along with them. Despite the risk of becoming collateral damage in the wake of someone else's problem, only 52% of service providers have more than five people dedicated to security. And only 38% conduct DDoS attack drills more than once a year.

78%

Increase in demand for DDoS protection services

In the event of your organisation being targeted or affected by a large-scale DDoS attack, diverting the unwanted, harmful excess traffic could be your only salvation. With Arbor Cloud each location has the same level of mitigation.

How present is the threat?

It's not hard to see how the likelihood of being caught up in an attack is increasing. Especially as you don't need to be the intended target - where DDoS attacks are concerned, anyone and everyone is a potential victim.

DID YOU KNOW?

$100,000+

For $5/hr anyone can launch a DDoS attack and cause $1000,000+ in damage

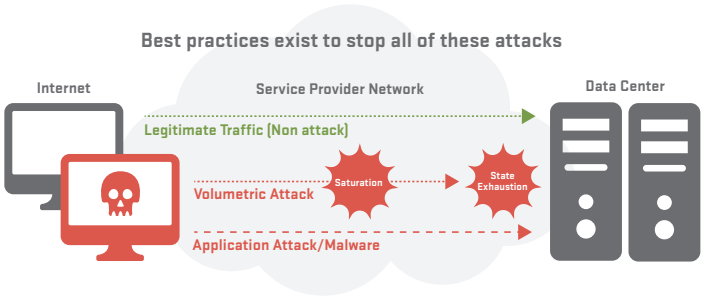
The anticipated growth in the use of botnets, as outlined above, means attackers will continue to spread their net far and wide. Those attacks can be motivated by everything from commercial rivalry to geopolitical agitation, from attempts to manipulate financial markets even down to disgruntled ex-employees looking to cause problems.

Data analysed in our WISR reports looks at which vertical industry sectors are most affected by DDoS attacks. It's a list that makes for pretty depressing reading: ecommerce, financial services, government, education, hosting, manufacturing, gaming, gambling, law enforcement, healthcare, energy/utilities and end-user/ subscriber businesses.

$1,000 - $5,000

Cost per minute of downtime of a DDoS attack

The architecture of your website also has a part to play in things. Many websites are increasingly hosted on large content delivery networks (CDN) which have a degree of redundancy built into them. But that won't necessarily help in the event of an attack. The customer-facing website might be able to absorb a large amount of traffic without too much trouble. But back-end infrastructures tend to be less robust.



The increased reliance on the cloud in enterprise computing has further complicated things. Websites are now often hosted by cloud giants such as Amazon AWS or Microsoft Azure. With the growth of software-as-a-service, tools like Office365 and apps for instant messaging, file sharing, or conferencing have become essential to many knowledge workers, but do not reside on the company's premises.

It is crucial that the internet connectivity used to access these services offers the highest levels of availability. It is also vital that all employees are able to reliably access the Internet from any company site, regardless of which ISP is providing the link. Service availability might be the responsibility of the service provider, but protecting your hosted assets remains your responsibility and ensuring safe, reliable access needs to be your priority.

Company assets hosted on a public cloud, such as AWS or Azure, must therefore be protected against all types of DDoS attacks.

Arbor Cloud operates at the internet level, which means it can cover all geographies and asset types under one single agreement. It also provides protection for your cloud-hosted assets together with on-premise assets under the same single agreement

Geography is also an important consideration. It's increasingly common for companies to operate in different countries and regions. Branch offices, data centers, or the headquarters of international subsidiaries all need reliable connectivity to the internet. If your organisation has multiple offices, whether nationally or internationally, it is likely that your internet connectivity is delivered by different service providers in each location. In the case of a DDoS attack, the level of protection provided by each ISP may differ, which further increases the possibility of prolonged downtime and loss of business. In the event of an attack your priority should be to shut down all unprotected connections. However, this requires manual intervention, which can leave you exposed to human error.

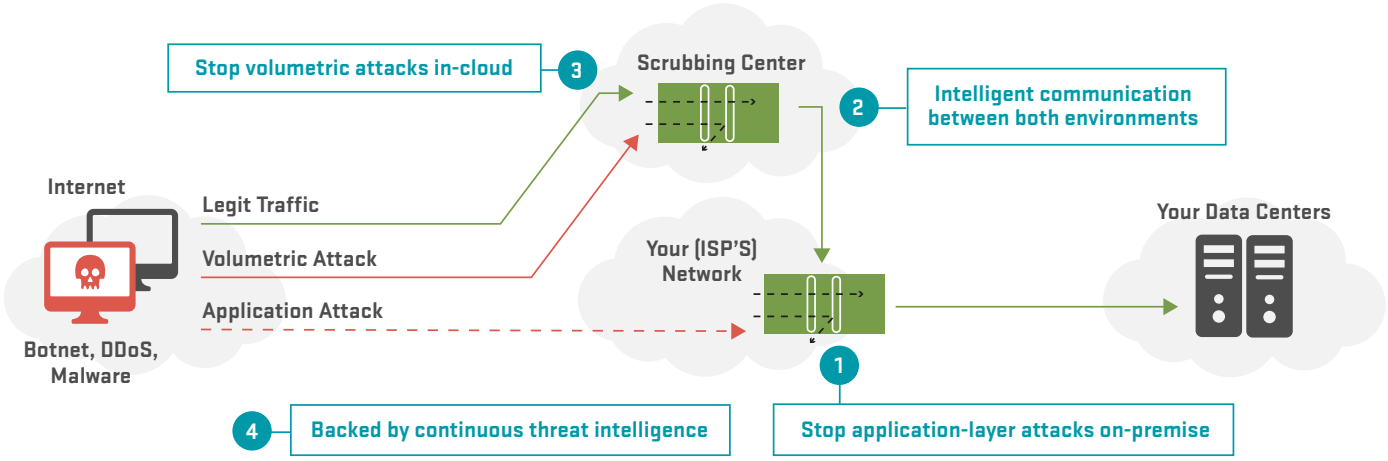
What steps should our organisation take?

In short, you need to accept there are certain things that fall outside of your sphere of influence, and instead focus your energies on the things you can control.

As already stated, the frequency and intensity of attacks is on the rise. Therefore, stopping attacks at source is not a practical option - as much as one might wish it were. Similarly, there is the constant danger of being caught up in an attack even though you're not the specific target. Yet there remain several actions you can take to mitigate the harm likely to be done by a DDoS attack. If it's going to be able to cope with the ever-present threat of attack, a modern DDoS strategy requires multi-layered protection from the edge of the network through to the cloud. Yet not all DDoS services provide this.

On-premise protection guards against state-exhausting attacks aimed at the security infrastructure of the enterprise. It also helps prevent stealthy attacks that bypass firewalls, intrusion prevention systems (IPS), and target business-critical applications. Today's low-and-slow application-layer attacks fly under the radar of many cloud-based solutions as well as traditional perimeter security solutions, such as firewalls and IPS.

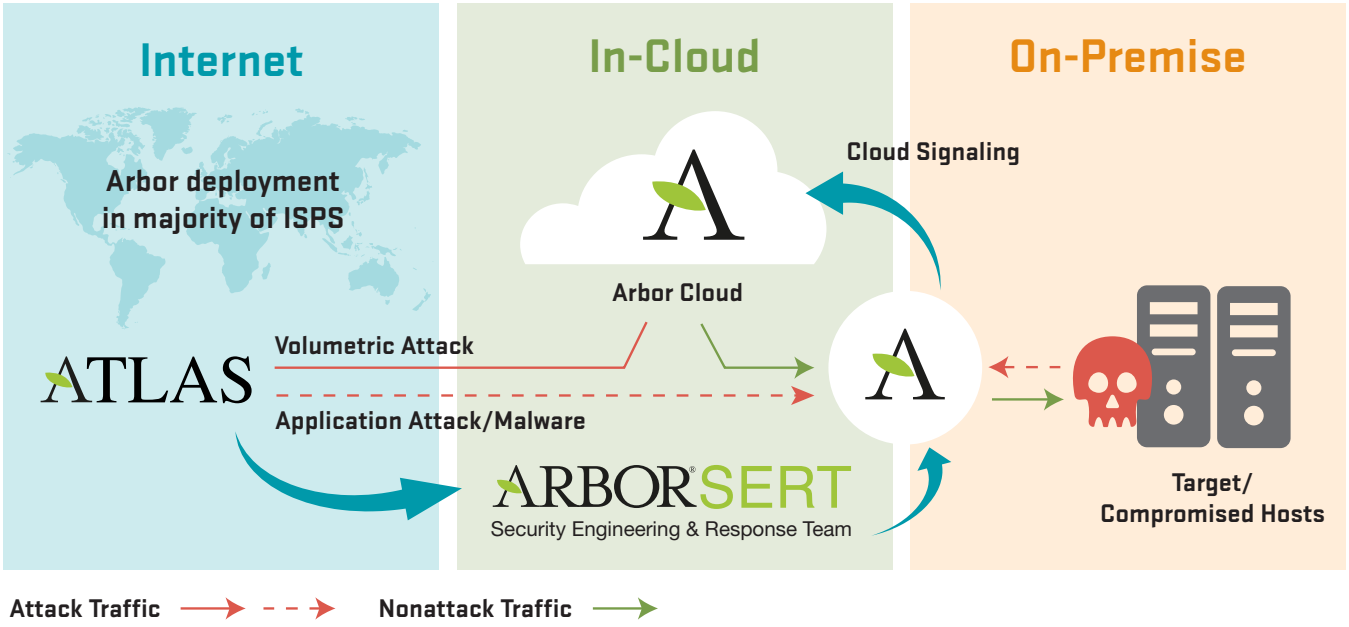
Stopping modern day DDoS Attacks Layered, Automated DDoS Attack Protection



A local-only approach to DDoS mitigation is not going to be enough to manage the growing size of attacks; Arbor Cloud offers sufficient capacity to cope with the biggest of DDoS attacks, and provides protection for all cloud-hosted assets together with on-premise assets under one single contract.

They can only be detected and blocked using a purpose-built intelligent DDoS mitigation solution on premise. Flood attacks overwhelm the capacity of enterprise data centers, negating the effectiveness of any perimeter defenses. The best place to stop these high-volume DDoS attacks is in the cloud.

The on-premise protection delivered through the Arbor Cloud solution provides the first line of defense against DDoS attacks that threaten service and application availability. When the on-premise solution detects an attack, you can manually signal the cloud deployment about the attack. Alternatively, you can preset the on-premise solution to automatically send a cloud signal upstream when a threshold is reached. It also proactively protects against high-bandwidth DDoS attacks. Unlike other managed DDoS solutions, Arbor Cloud enables enterprises to maintain control over DDoS mitigation via the on-premise solution.



The Arbor Cloud DDoS Managed Service was recognized as "Best Cloud Product" at Computing Magazine's Cloud Excellence Awards in September 2017. Currently, the Arbor Cloud global scrubbing capacity is 4Tbps, but is on track to double to 8Tbps.

Our expansion effort includes upgrades of existing nodes and the introduction of more than a dozen new nodes in major traffic centers in North America, Europe, Asia and South America, and promises even greater protection for enterprise and data center customers going forward.

To learn more about Arbor products and services,
please visit our website at **arbornetworks.com** or follow us on Twitter **@ArborNetworks.**

ARBOR NETWORKS
The Security Division of NETSCOUT

About Arbor Networks

Arbor Networks, the security division of NETSCOUT, helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor Networks Spectrum™ advanced threat solution delivers complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of attack campaigns, malware and malicious insiders. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context so customers can solve problems faster and reduce the risks to their business.