THE COST OF DDoS ATTACKS
AND BUILDING THE BUSINESS CASE FOR PROTECTION

January 2017
CONTENTS

1. Abstract.............................................................................................................................................3
2. Introduction: What are DDoS Attacks? .........................................................................................4
3. Types of DDoS Attacks....................................................................................................................5
   I. Volumetric Attacks.....................................................................................................................5
   II. TCP State-Exhaustion Attacks (Protocol Attacks)...............................................................5
   III. Application-Layer Attacks.....................................................................................................6
   IV. Zero-Day DDoS Attack...........................................................................................................6
4. Impact of DDoS Attacks on Enterprises.......................................................................................7
   A Shifting Security Landscape......................................................................................................7
   Europe Now Under Fire................................................................................................................8
5. Assessing the Impact of DDoS Attacks..........................................................................................8
   Direct Revenue Loss....................................................................................................................8
   Loss of Productivity....................................................................................................................9
   Ransom Payments.......................................................................................................................9
   Reputational Damage..................................................................................................................9
   DDoS as a Smoke screen...............................................................................................................10
6. DDoS Attacks: Best Practices........................................................................................................11
   Create a DDoS Playbook..............................................................................................................11
   Never Overestimate Your Network Defenses............................................................................11
   Benchmark to Help Better Identify Active Attacks..................................................................12
   Stay on Top of Vendor Patches...................................................................................................12
   Secure Any IoT Devices...............................................................................................................12
   Deploy a Dedicated DDoS Mitigation Solution..........................................................................13
7. Summary: Adapt and Evolve..........................................................................................................13
1. ABSTRACT

At Cogeco Peer 1 we host over 8000 customers of whom 600 are ecommerce businesses. We fight distributed denial-of-service (DDoS) attacks day in, day out. They became even uglier in 2016 and so this paper sets out what we have been seeing. It also gives the reader some hints on how to protect against this growing menace at a time when no sector or size of business is immune.

This paper is written for business owners and decision makers who are looking to understand the business impact and needs in the rising DDoS threat landscape. It will introduce you to DDoS attacks; go through the different types; explain the impact they have on enterprises; and outline some of the best practices when faced with this particular security threat.

The fact that DDoS attacks do not discriminate – making any business in any industry a potential target – makes them a particularly worrying attack vector.

Furthermore, the relative ease with which they can be sourced (as a service), and at extremely low cost, means they are no longer just the chosen method used by state-sponsored hackers to cause chaos and disruption. They are ever more commonly utilized by individuals and small groups with an axe to grind or a point to make.

Some organizations have even suspected their competitors of being behind DDoS attacks which have knocked their systems offline and caused business downtime.

Therefore, if your business has an online presence or Internet-facing network infrastructure, you really need to understand the significant threat posed by DDoS attacks today, and put measures in place to mitigate them before they adversely impact your business.

As long as they can carry out DDoS attacks with relative ease, cyber-criminals will continue to do so. It’s up to every business to ensure that their defenses are fit for purpose and not helping to contribute to the global botnets (which you’ll read about) that are prevalent today.

The more DDoS attacks occur, the more we learn about them and the more you can do to prevent them. Investing in additional protection services generates a 50% reduction risk of DDoS attacks at the very least.

The swathe of statistics referenced herein will highlight just how big a threat DDoS attacks are today and outline the serious consequences businesses can experience – both financially and non-financially – if they find themselves on the receiving end of a large-scale DDoS attack.
2. INTRODUCTION: WHAT ARE DDoS ATTACKS?

DDoS attacks are used to overload the Internet-facing network infrastructure and services that many organizations rely on. Their ability to cause network outages and general chaos for any organization and their IT security staff makes DDoS attacks a particularly troublesome issue for enterprises large and small.

Unlike many of the techniques utilized by cyber-criminals today, DDoS attacks have their roots firmly in the past, and instead of falling off the threat landscape, they have evolved to become more devastating than ever.

This makes the case for implementing a dedicated DDoS mitigation solution more relevant than ever as we see more and more workflow operations, management strategies, products and services becoming reliant on web-based IT infrastructure.

As their name suggests, DDoS attacks are designed to prevent legitimate users from accessing a company’s website and/or business services, by knocking them offline with an overwhelming number of illegitimate requests, packets of data or other network traffic.

The distributed nature of DDoS attacks makes them extremely difficult to prevent completely, but bespoke mitigation solutions can significantly reduce the impact of them if implemented before an attack occurs.

DDoS attacks can be perpetrated by a hacker, collective or a single individual, taking advantage of a botnet-for-hire – an increasingly popular and lucrative offering that unscrupulous parties have made available.

For as little as $150 US (£123), a botnet can be hired on the black market to carry out a DDoS attack for an entire week. At such low cost, DDoS attacks can even be taken advantage of by ex-employees who may feel unhappy with the way they were treated by a particular company.

Moreover, the growing ubiquity of the Internet of Things (IoT) is also lending itself nicely to hackers, with some of the world’s largest global botnets compromising Internet-connected devices such as smartwatches, municipal traffic cameras, thermostats and DVR players.

DDoS attacks are one of the top attack methods for extortionists, political activists (hacktivists) and disgruntled individuals/groups alike because they are easy to deploy, difficult to prevent, hard to trace and increasingly affordable for anyone to get their hands on.

Unlike more traditional attack techniques – which look to infiltrate business networks undetected – DDoS attacks are often brutal and anything but sneaky. This helps them achieve their primary aim of creating noticeable disruption.
3. TYPES OF DDOS ATTACKS

DDoS attacks have been used to cause chaos and disruption for decades. However, despite the fact they are one of the oldest threats on the Internet today, their continued evolution and overwhelming abundance makes them an extremely potent force to be reckoned with.

Cyber criminals, hackers, political activists and anyone else who wants to cause serious headaches for an online organization will usually go down the DDoS route. That’s because they are increasingly easy to carry out, difficult to mitigate, hard to trace and very cheap to buy – which makes them a high-impact, low-risk attack strategy.

Unlike their denial of service (DoS) attack counterparts – which are conducted using a single computer and Internet connection – DDoS attacks inevitably comprise hundreds or thousands of computers and Internet connections, which are distributed across a global network often referred to as a “botnet”.

At a very high level, DDoS attacks fall into two categories:

- **Connection-based**: An attack that occurs only when a “mutual” handshake between a server and a client has occurred using certain standard protocols.
- **Connectionless**: An attack that does not rely on a formal session to be established between the server and client first.

In addition to being connection-based or connectionless, DDoS attacks also fall into three main categories and one up-and-coming attack type:

I. VOLUMETRIC ATTACKS

Volumetric attacks (also known as “floods”) utilize botnets in an attempt to saturate a target with sheer traffic volume. Their connectionless nature means they can be carried out relatively easily and their ultimate goal is to cause the target – usually a website – to crash under the pressure of the phenomenal bandwidth being sent to it.

All of the computers and other Internet-connected devices in the botnet will have been compromised with malware at one time or another, allowing them to be controlled by a hacker or a collective. The infected machines and devices are then commanded to “attack” the target in unison and swamp it with traffic until it can no longer operate.

Volume-based DDoS attacks are particularly difficult to prevent because the disruptive traffic comes from so many different sources, potentially located all over the world.

User Data Program (UDP) floods and Internet Control Message Protocol (ICMP) floods – otherwise known as ping requests – are the two most commonly witnessed volumetric attack types.

UDP floods target random ports on the host with numerous UDP data packets. This causes the host to continuously check if an application is listening on said port, and when one isn’t found replies with an ICMP Destination Unreachable packet. This continual battering eventually causes the host’s resources to be depleted and ultimately fail.

ICMP floods overwhelm the target with a deluge of ping requests. They are sent as fast as possible without waiting for replies. ICMP floods often consume both outgoing and incoming bandwidth, since the target will often attempt to reply to the ping requests being sent to it. The overall result is severe system slowdown or failure of the target machine/device.

Volumetric DDoS attacks were traditionally measured in bits per second (Bps), but today it is more common to measure them in gigabits per second (Gbps), highlighting how they have grown in size over the years.

According to Arbor Network’s 2016 *Worldwide Infrastructure Security Report* – the 11th of its kind and latest at time of writing – volumetric attacks accounted for 65% of DDoS attacks seen in 2015.¹

II. TCP STATE-EXHAUSTION ATTACKS (PROTOCOL ATTACKS)

TCP state-exhaustion attacks – also referred to as protocol attacks – are more sophisticated than volumetric attacks and target specific network devices such as firewalls, web servers and/or load balancers. The specific aim of state-exhaustion attacks is to exhaust the target device’s available resources and cause it to fail.

Perhaps the most well-known and one of the most destructive types of state-exhaustion attack is the infamous Ping of Death (POD). It works by exploiting the fact that the maximum packet length of an IP packet (including header) is 65,535 bytes.

An attacker sends a large IP packet that is split across multiple IP packets (known as fragments). The recipient host then reassembles the IP fragments to form the complete packet, which is larger than 65,535 bytes when reassembled. This causes a memory buffer overload to occur, causing the target to crash and denial of service for legitimate packets.

SYN floods are another common type of state-exhaustion attack which look to exploit a weakness that exists in the TCP connection sequence – the “three-way handshake” that is needed for a TCP connection to be initiated.

A SYN request is sent to a target which responds with a SYN-ACK response. Under normal circumstances the requesting machine would then reply with an ACK response, initiating the TCP connection.

However, with a SYN flood DDoS attack the original requestor (attacker) never sends the necessary ACK response. This causes the target computer to simply wait in anticipation. Subsequent SYN requests are then sent which remain unanswered and bind the target’s resources until no new connections can be made.

TCP state-exhaustion attacks are measured in Packets per second and accounted for 18% of all DDoS attacks witnessed in 2015, according to Arbor Networks.

III. APPLICATION-LAYER ATTACKS

Application-layer attacks, also known as Layer 7 attacks, specifically target weaknesses in an application or server, with the goal of establishing a connection and then exhausting said resource by monopolizing processes and transactions.

This type of attack is much harder to detect because it utilizes seemingly legitimate and innocent requests. Furthermore, application-layer DDoS attacks do not need many “attacking” machines to achieve their goal.

HTTP and DNS services have been the traditional focus of application-layer attacks, but it’s becoming increasingly popular for HTTPS and SMTP to be targeted too.

Application-layer attacks are measured in Request per Second and accounted for 18% of all DDoS attacks seen in 2015, according to Arbor Networks.

IV. ZERO-DAY DDoS ATTACKS

Zero-day DDoS attacks should also be mentioned here because they are a popular topic in both the security world and hacker community alike.

They refer to the DDoS attacks that target vulnerabilities which third-party vendors do not yet know about, and no official patches or fixes have been released.

The term “zero-day” refers to the fact that the vendor has zero days (before disclosure) to fix the vulnerability.

Once discovered, zero-day vulnerabilities are quickly communicated across the hacker community, making them a significant threat which vendors must work hard to mitigate.

Zero-day DDoS attacks are particularly hard to prevent as they exploit previously unknown vulnerabilities for which standard security protocols might be ineffective.

In some cases, online entities can be hit simultaneously by volumetric, TCP state-exhaustion and application-layer DDoS attacks. Such an occurrence makes DDoS mitigation/prevention even more challenging and important.
4. IMPACT OF DDOS ATTACKS ON ENTERPRISES

The scale of the global ‘Cybercrime as a Service’ infrastructure was finally fully realized in the last few months of 2016, according to the latest (at time of writing) Kaspersky Lab DDoS Intelligence Report Q3 2016.²

It is a fully commercialized operation, with DDoS as one of the most popular services available to interested buyers. Capable of launching attacks the likes of which the world has never seen before in terms of volume, duration and technological complexity.

Indeed, Europol's recently published Internet Organized Crime Threat Assessment (IOCTA) 2016³ report clearly ranks DDoS attacks as one of the biggest security threats facing organizations today.

The report also states that “any internet facing entity, regardless of its purpose or business, must consider itself and its resources to be a target for cybercriminals”.

A SHIFTING SECURITY LANDSCAPE

Akamai's Q3 2016 State of the Internet/Security Report⁴ (the latest at time of writing) shows that DDoS attacks increased by a staggering 71% in the third quarter of 2016 vs. Q3 2015. Furthermore, there was a 77% increase in infrastructure layer (layers 3&4) attacks, and a 138% increase in the number of DDoS attacks exceeding 100 Gbps.

In fact, Akamai also recorded two DDoS attacks in Q3 2016 that both topped their previous high water mark. The attacks – one at 623 Gbps and the other at 555 Gbps – started Sept. 15, 2016 and both targeted the website/blog of industry security expert, Brian Krebs.

The attacks on Brian Krebs’s site made international headlines and are thought to have been instigated following the security writer’s coverage of a stressor site called vDOS and the security firm BackConnect Inc.

However, despite both attacks setting new benchmarks in terms of volume at Akamai, an attack a month later against Dyn would go down as the largest of its kind in history.

What sets the Dyn attack apart is the immense impact it had, bringing down much of America’s Internet as a result.

Dyn, a company that controls much of the Internet’s domain name system (DNS), saw its servers hit on October 21, 2016. Websites including Twitter, Netflix, Reddit, CNN and the Guardian, as well as many others in Europe and the U.S., were all knocked offline.

But what’s even more alarming about the Dyn attack – and should serve as a warning of things to come – is the fact that it was orchestrated using a botnet made up of so-called “Internet of Things” (IoT) devices.

As these types of devices continue to proliferate, and IPv6 adoption gains further traction, the threat posed by botnets of this nature increases exponentially.

The Dyn attack is believed to have involved tens of millions of IP addresses, and peaked at an astonishing 1.2 Tbps (terabits per second) – effectively dwarfing the attack on Brian Kreb’s site a month earlier.

5. ASSESSING THE IMPACT OF DDoS ATTACKS

Any IT outage or episode of system downtime has an impact on any enterprise’s bottom line. However, the severe and often prolonged nature of DDoS attacks makes them particularly disruptive and damaging in a number of ways.

DDoS attacks are also estimated to account for one-third of all global downtime – a reality that when in play has a catastrophic effect on end user productivity, customer relations and company reputation.

DIRECT REVENUE LOSS

Enterprises that rely heavily – or solely – on their online presences to generate revenue, such as eCommerce businesses, undoubtedly stand to lose the most financially when struck by a DDoS attack.

Factor in the selling potential presented at certain times of the year – like Black Friday, Cyber Monday and Christmas – and the detrimental effect is almost immeasurable.

According to the Corporate IT Security Risks 2016 study conducted by Kaspersky Lab and market research company B2B International, a single DDoS attack can cost a company over $1.6 US million (£1.3 million), depending on how quickly the attack is detected.

Perhaps surprisingly, the biggest expenses for medium and large companies (20% and 19% respectively) were caused by changes to their credit and insurance ratings. This is especially true for companies that are the target of large-scale attacks and find themselves in the news as a result.

For smaller firms, overtime payments to employees (17%) are the largest DDoS-related costs. A fact that highlights the importance of having mitigation solutions in place before an attack occurs.

DDoS attacks are also cited as one of the top five threats that cause businesses to hire new employees, with 37% of companies who fell victim to such attacks saying they planned to significantly increase their number of IT staff.

Upgrades to IT infrastructure and software (10%); staff training (10%); and customer compensation (12%) were also cited as other major DDoS-related costs.

“ A SINGLE DDoS ATTACK CAN COST A COMPANY OVER $1.6 US MILLION (£1.3 MILLION). ”

EUROPE NOW UNDER FIRE

The aforementioned Kaspersky Lab report also shows that for the first time in a year, the Top 10 most attacked countries included three Western European countries: Italy, France and Germany. While these three countries only accounted for 1.29% of the total DDoS activity monitored during the period, the fact they have entered the Top 10 could signal the start of a trend which sees European organizations increasingly targeted.

Nevertheless, China remains the overall leader in terms of both the number of DDoS attacks and number of targets, with 72.6% and 62.6% respectively. The United States fills second place with 12.81% of DDoS attacks and 18.73% of targets, while South Korea comes in third with 6.31% of DDoS attacks and 8.73% of targets.

All of these increasingly alarming statistics highlight just how real the current DDoS threat to organizations is today.

LOSS OF PRODUCTIVITY

While it is often difficult to place a financial figure on the loss of productivity DDoS attacks can cause, a Ponemon Institute report, entitled The Cost of Denial-of-Service Attacks\(^6\), released in March 2015, shows that DDoS attacks have the potential to impact much more than just web-facing business services.

For example, 82% of respondents said that a DDoS attack shut down their entire data center (34%) or part of it (48%). These findings show how an enterprise’s non-eCommerce/online departments can also experience productivity drops as a result of a DDoS attack.

In addition, Ponemon found that lost user productivity as a result of a DDoS attack costs businesses, on average, $173,169 US (£141,550) per year.

These figures obviously don’t account for the frustration experienced by business users while a service-impacting DDoS attack is occurring. If such outages were to become a regular occurrence, businesses may find their staff turnover rates increase significantly.

RANSOM PAYMENTS

Many hackers use the threat of DDoS attacks to extort money from organizations and often get paid without having to even launch an attack.

In one example, cyber criminals using the Armada Collective moniker were able to successfully extort over $100,000 US (over £81,000) from global businesses in just two months.

The so-called “protection fee” – to be paid in the virtual currency Bitcoin – was to stave off a DDoS attack from the collective. However, it was discovered that the hackers had no way of knowing who had paid the fee and who hadn’t. As a result, none of the potential victims were attacked.

That being said, this episode highlights just how lucrative threats can be, and the financial impact they can have on organizations.

REPUTATIONAL DAMAGE

Despite being extremely difficult to quantify, reputational damage was cited by 64% of respondents in the Ponemon study as the number one consequence of a DDoS attack. This significantly outweighs both diminished productivity for IT staff (35%) and revenue losses (33%).

The bottom line is that large-scale DDoS attacks that cause service outages often hit the headlines, and the impacted organization inevitably experiences a hit in terms of reputation. It may even be the case that the only consequence was a service outage, but said business will still likely be tarred with the “victim of cyber-crime” brush.

This undermines the company’s reputation and could cause its loyal customers to seek alternatives in the future. In already highly-competitive marketplaces, businesses simply cannot afford for this to happen – and it has happened a lot in recent years, to some of the world’s largest organizations.

Such reputational damage is why some businesses don’t even think twice about paying extortionists if it means the threat of an attack is removed.

**DDoS as a Smoke Screen**

While DDoS attacks are primarily designed to cause service disruptions and send an organization’s IT staff into an incident management frenzy, they can also be used as a smoke screen for other criminal activities.

A Kaspersky Lab report, entitled *Denial of Service: How Businesses Evaluate the Threat of DDoS Attacks*, released in Sept. 2015, found that 74% of organizations that experienced a service-impacting DDoS attack also registered other cyber-security incidents at the same time. This suggests that the actual DDoS attack could have been used as a decoy to distract the company’s IT staff while the cyber-criminals focused on breaching other parts of the organization’s security.

Typical examples of attacks experienced by businesses at the same time as a DDoS attack are malware attacks and network intrusion.

This worrying and rising trend of DDoS as a smoke screen adds even more weight to the argument for businesses to employ a real-time, behavioral-based attack mitigation system.

---

6. DDOS ATTACKS: BEST PRACTICES

After the digital dust had settled following the Dyn DDoS attack, numerous rumors circled about the motivation for the attack. The general consensus however, is that the world’s biggest DDoS attack was the work of amateurs – a revelation that will no doubt have IT security professionals very nervous.

The fact that a group of “script kiddies” – to utilize the phrase used by business risk intelligence firm Flashpoint to describe the perpetrators – were able to take much of America’s Internet offline is extremely concerning.

That’s why now more than ever, enterprises need suitable DDoS protection in place to mitigate the potential risks and ensure business continuity. As with most security plans, the key when it comes to DDoS prevention is addressing the threat before an attack has occurred.

Here are some of the ways your organization can reduce the risks associated with DDoS attacks:

“EFFECTIVE COMMUNICATION CAN HELP TO KEEP THE COSTS ASSOCIATED WITH A DDoS ATTACK DOWN.”

CREATE A DDoS PLAYBOOK

One of the best ways to ensure your organization is in the best shape possible when a DDoS attack strikes is by creating a DDoS playbook.

It should include the names and contact numbers of the individuals and teams who are to be called upon when an attack hits. Their roles and responsibilities should also be documented, so that nothing is left to chance while your company is being DDoS’d.

An important aspect of your DDoS playbook should be how you communicate the ongoing problem to customers, staff and other business stakeholders. Effective communication can help to keep the costs associated with a DDoS attack down, and instill confidence in the people who matter most to your business.

Your DDoS playbook should be periodically tested to ensure that it covers every eventuality and contains all the most relevant, up-to-date information.

NEVER OVERESTIMATE YOUR NETWORK DEFENSES

Modern networking technology has come on leaps and bounds from the infrastructure of yesteryear utilized by businesses. However, you should never blindly assume your network defenses will be able to cope with the onslaught of a modern-day DDoS attack.

Last year’s attack on Dyn saw data volumes of 1.2 Tbps – that’s terabits, not gigabits! Virtually no network hardware could cope with such unprecedented volumes, regardless of how advanced it is.
BENCHMARK TO HELP BETTER IDENTIFY ACTIVE ATTACKS

Some businesses, quite worryingly, have no idea what levels of network traffic they experience under “normal” operation. Therefore, how can these companies ever tell if they are being subjected to a DDoS attack or not?

That’s why every business should monitor their network traffic and set benchmarks. These will help determine whether an increase in network traffic is the result of an attack or just the kind of throughput usually seen at that particular time of day, month or year.

Equally important is to understand where the majority of your network traffic comes from. If your business has zero customers and/or no network presences in a certain country, but you’re seeing a lot of traffic coming from said country, alarm bells should start to ring.

The sooner you identify a DDoS attack, the better chance you have of mitigating it.

However, slow network performance and sluggish business websites are not always due to DDoS attacks, which is why it’s important to identify the root cause(s) of any degradation of service as soon as possible.

STAY ON TOP OF VENDOR PATCHES

Keeping servers and network devices up-to-date with vendor-released patches is a crucial element of any IT security plan, but it’s particularly important when it comes to DDoS attacks.

The last thing you want when your company is under fire is to find out a third-party vendor is reluctant to help because you’re not running the latest firmware or aren’t patched in accordance with their releases.

With new and ever-sophisticated DDoS attack methods emerging all the time, known security vulnerabilities for which patches exist should be treated as a priority. While they can’t mitigate zero-day DDoS attacks, they will position your company in much more favorable space in preparation for the worst case scenario.

SECURE ANY IoT DEVICES

If your organization is especially forward-thinking and looking to leverage the opportunities afforded by IoT devices, make sure they are all protected against remote access.

While remote access is sometimes necessary for third-party troubleshooting, it’s also a gateway for hackers to infiltrate your network and possibly recruit your IoT devices into a global botnet.
DEPLOY A DEDICATED DDoS MITIGATION SOLUTION

While there are emergency DDoS mitigation solutions on the market which can be deployed within an hour in most cases, why would you respond reactively to a situation where proactive solutions are available?

Dedicated, behavioral-based DDoS mitigation systems are not only much safer, but also help to afford greater peace of mind for your business. They should be reviewed and selected based on your own benchmarked best efforts, taking into account source flow metrics, time to mitigate attacks, performance capacity, and other critical factors.

Such solutions usually reside in line with your data flow and send network traffic through dedicated scrubbing centers which filter out most suspicious traffic and allow only genuine communications in real time.

Systems like this should form part of your overall incident response plan to ensure that any anomalies are quickly identified and addressed.

7. SUMMARY: ADAPT AND EVOLVE

It wasn’t so long ago that DDoS attacks were still being measured in Bps (bits per second). But as we’ve seen with the Dyn attack last year, terabits per second (Tbps) could soon become the norm.

That’s why it is important to remain on top of industry news and work with your DDoS mitigation partner to ensure that your implemented solution remains fit for purpose.

Such mitigation partners can also help with simulating DDoS attacks to test how well your defenses hold up under pressure, and see whether your DDoS playbook contains everything it needs to.

The fact that DDoS attacks constantly evolve means that businesses need to adapt with speed and resiliency to the techniques being used. A DDoS mitigation solution that was relevant a few years ago might be completely obsolete today. Alongside your chosen security partner your company should ensure its security protocols and defensive measures are always appropriate and up-to-date.

DDoS attacks pose a very real and significant threat to every business with an online presence or Internet-facing network infrastructure. The low cost of being able to purchase DDoS as service offerings, relative ease with which they can be obtained and then deployed, make them a formidable threat for organizations today.

As such, the threat of having your IT infrastructure compromised has never been more real.

ABOUT COGECO PEER 1

Cogeco Peer 1 is a wholly-owned subsidiary of Cogeco Communications Inc. (TSX:CCA) and is a global provider of essential business-to-business products and services, such as colocation, network connectivity, hosting, cloud and managed services that allow customers across Canada, Mexico, the United States and Western Europe to focus on their core business. With 17 data centers, extensive FastFiber Network® and more than 50 points of presence in North America and Europe combined, Cogeco Peer 1 is a trusted partner to businesses small, medium and large, providing the ability to access, move, manage and store mission-critical data worldwide, backed by superior customer support.

CONTACT US

TORONTO 1.866.579.9690
USA 1.844.712.3183
LATIN AMERICA 1.888.978.3518
UK 0800.840.7490
FRANCE 0033.486.801.344
ALL OTHER COUNTRIES +1.646.396.0423

© 2017 Cogeco Peer 1

READY TO LEARN MORE?

Streamline your IT with Cogeco Peer 1.
Visit cogecopeer1.com