What's the right DDoS protection for your business?

A buyer's guide to Distributed Denial of Service (DDoS) security

Bell

What's inside

If you've already determined that your organization needs protection against distributed denial of service (DDoS) attacks, the next question is: "What kind of DDoS security solution do we need?"

This guide will help you find the answer based on your business and IT requirements, and equip you with questions you should ask a potential security provider.

Contents

How do you know if you're at risk?

Assessing your IT security risk profile is a fundamental first step to determining whether you need some level of DDoS protection. Answering "yes" to one or more of these questions suggests you could be vulnerable to DDoS attacks:

- Are you in a high-risk industry?
- Is your organization highly visible online?
- Is your web presence essential to your business?
- Would you suffer significant financial or reputational damage because of a DDoS attack?

For a more in-depth look at how to assess your risk, download our DDoS risk assessment guide at bell.ca/ddosassessment.

Know what you need to defend against

Before looking at any potential security solutions or providers, it's important that you're up to speed with how DDoS attacks work and the impact they can have on your business.

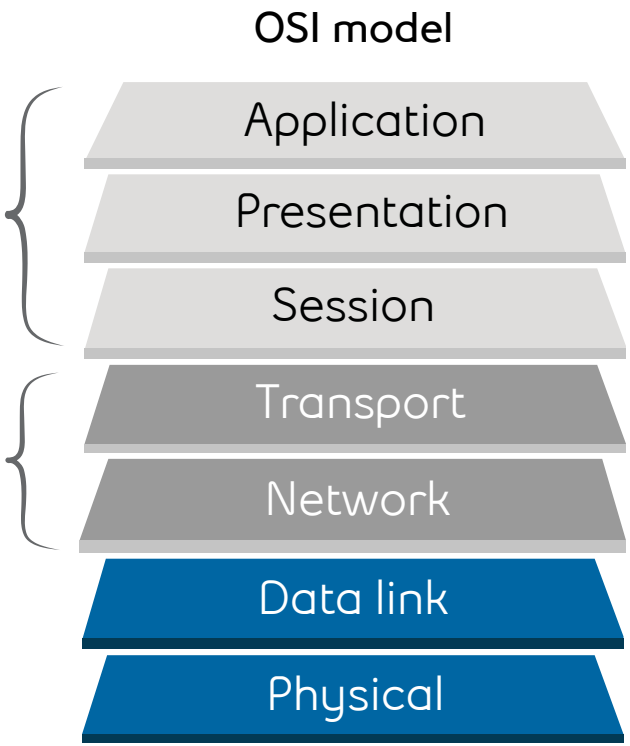
Remember, the goal of a DDoS attack is to stop legitimate user traffic from accessing your online services or resources. Two main types of attacks are used to achieve that goal:

Application-layer attacks

Application-layer attacks overload your servers by sending a large number of requests that require resource-intensive handling and processing to complete. This kind of attack targets protocols with exploitable weaknesses such as hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), file transfer protocol (FTP) and structured query language (SQL).

Network-layer attacks

Network-layer attacks use the brute force of thousands of simultaneous information requests to clog your Internet 'pipe', consuming massive amounts of bandwidth and overloading your network connections. Attackers target the network by exploiting vulnerabilities in areas such as user datagram protocol (UDP), network time protocol (NTP) and domain name systems (DNS).



With blended attacks increasingly hitting both of these layers and your servers simultaneously, it's critical for any DDoS solution to protect against the full range of possible attacks.

For more details on how DDoS attacks work and their potential impacts, download our Introduction to DDoS white paper at bell.ca/ddoswhitepaper.

Know your technical requirements

What does your organization require from its IT infrastructure? The DDoS solution you choose will need to align with your specific technical and business requirements, accounting for:

The scope of your online presence

If you have a very simple web presence, you'll need just a basic solution that can handle HTTP/HTTPS traffic. If you rely on a mix of public websites and application servers, you'll need more sophisticated DDoS protection. And if you have multiple branches or locations, the chosen solution will need to be able to protect all of them in the same way.

Your Internet connectivity

If you rely on multiple Internet service providers to ensure redundancy and availability, similar protection should be applied to each – which may require the implementation (and management) of several different solutions.

How responsive you need your DDoS solution to be

The cost and impact of downtime to your business will dictate the level of performance needed from your DDoS security solution. Faster response and resolution times might be a top priority if website and application availability are critical to your business.

Potential impact on your services

A solution that redirects incoming traffic to a cloud-based scrubbing centre may filter out malicious traffic – but the rerouting process can introduce latency, affecting application performance and stability. That kind of solution may not be suitable if your business depends on high-quality video or real-time financial transactions.

The experience of your IT team

It's important to know if your team has the specialized knowledge to use a self-managed DDoS solution effectively, especially as attacks become more sophisticated and complex. Your team also has to be willing to constantly learn and adapt as DDoS attacks evolve.

Your existing security practices

Some IT teams prefer to have a high level of control over any solution deployed in their environment. While self-managed, manually activated solutions may allow for more precise action in the event of an attack, detection and response times may be slower than a fully managed, always-on solution.

Your data management requirements

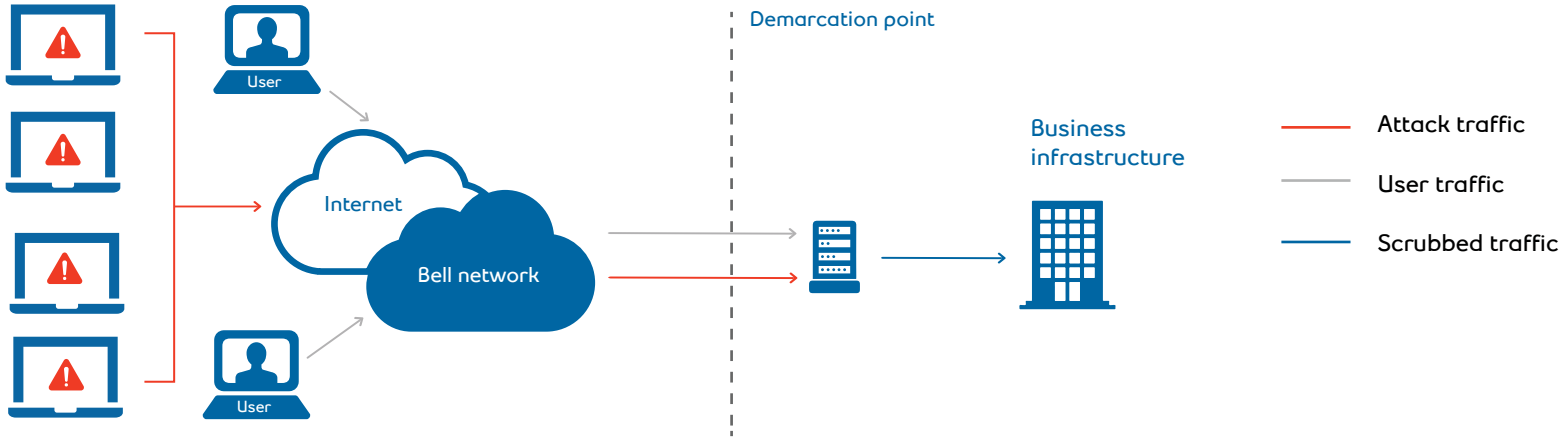
Governments and financial institutions often have corporate or regulatory requirements to keep their traffic within a particular country or region, which may exclude certain security solutions or providers from consideration if they have scrubbing centers outside the country.

Determine the right deployment model for you

There are many ways to implement DDoS protection. Before choosing a deployment model, it's important to understand the advantages and disadvantages of each – and to evaluate your own risk tolerance. You should also factor the relative value of each deployment model against your specific business and technical requirements.

On-premises equipment

Dedicated, on-premises security appliances can detect specific application-layer and encryption-based attacks, then protect your network by offloading any traffic matching a known attack signature. This kind of appliance is essential backup for firewalls and intrusion prevention systems, which can be overwhelmed by a high volume of open requests.



Advantages

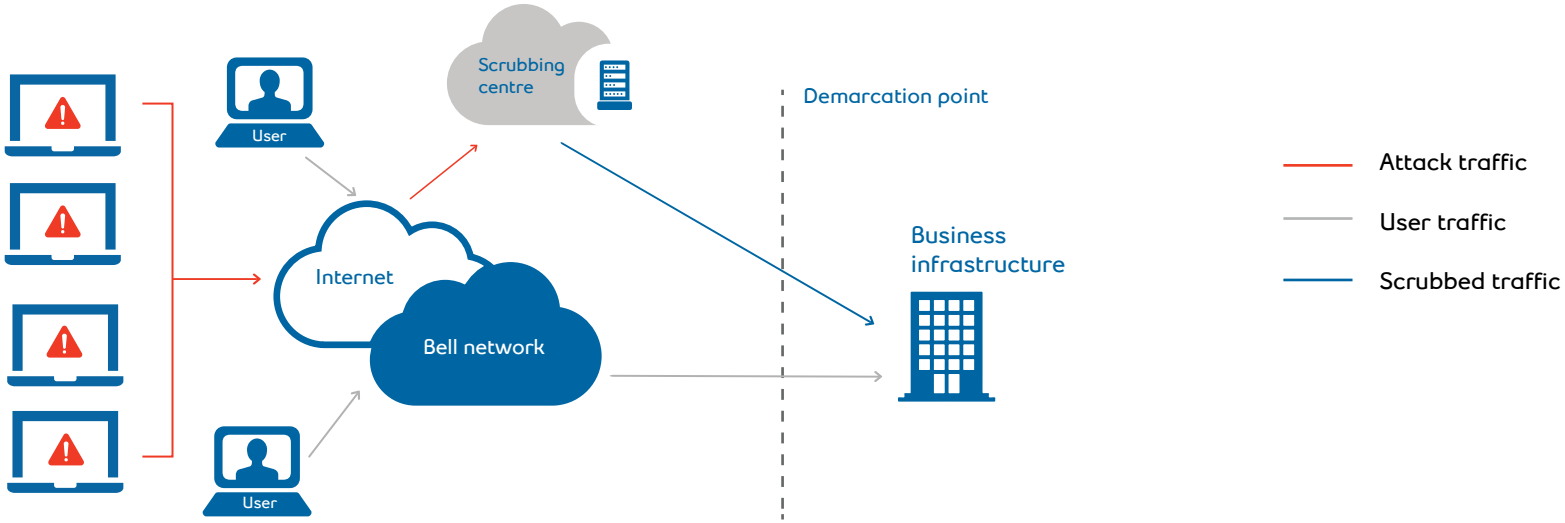
- Provides excellent protection for a wide range of attacks
- Can focus on very specific application-layer threats and attack thresholds
- Offers greater control over implementation, management and response
- Can meet stringent corporate or regulatory data-management requirements

Disadvantages

- Volumetric attacks could stress the system
- Requires ongoing management and configuration to keep up to date with the latest threats

Cloud-based scrubbing

Cloud-based solutions redirect all traffic to a third-party cloud provider for filtering when an attack is detected. After being 'scrubbed', legitimate traffic is sent on to your site. Redirecting traffic this way can cause latency and affect application performance. As well, until the border gateway protocol route announcement is propagated (telling the Internet to redirect your traffic), your site will continue to receive the attack traffic. Most scrubbers are located outside of Canada, which could violate your data-management requirements.



Advantages

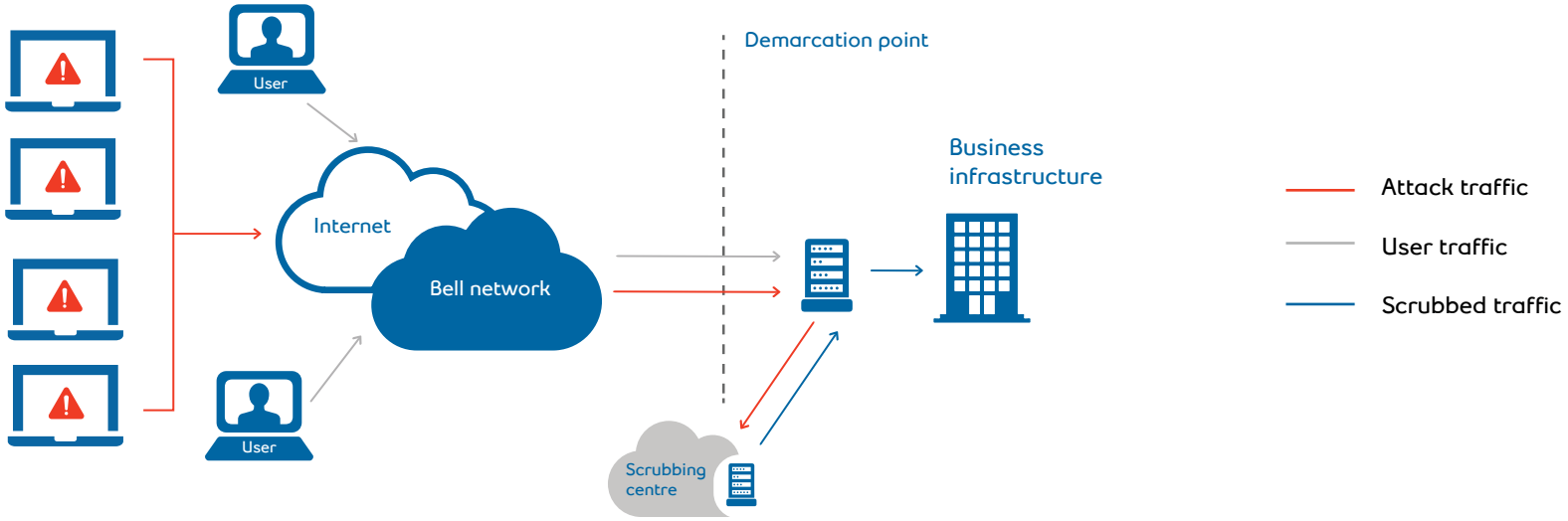
- Better protection against volumetric attacks than on-premises equipment
- Low false-positive rate
- No on-premises hardware required
- Always up to date

Disadvantages

- Traffic latency may affect application performance
- Cannot block some kinds of application attacks
- SSL protection requires giving up control of encryption process
- Delays in propagation of route announcement could lead to network link saturation
- Geographical concerns over location of scrubbing centres

Hybrid A: Cloud-based scrubbing and on-premises equipment

A better approach to DDoS protection involves deploying both on-premises equipment and cloud-based scrubbing. Cloud-based implementation provides greater protection against volumetric attacks with a low rate of false positives, while on-premises equipment gives you greater control over when and how to mitigate an attack. And with only legitimate traffic getting sent to your site, you avoid the possibility of having on-premises equipment overwhelmed by a flood of malicious traffic – meaning it is always available to ensure your servers and applications stay online.



Advantages

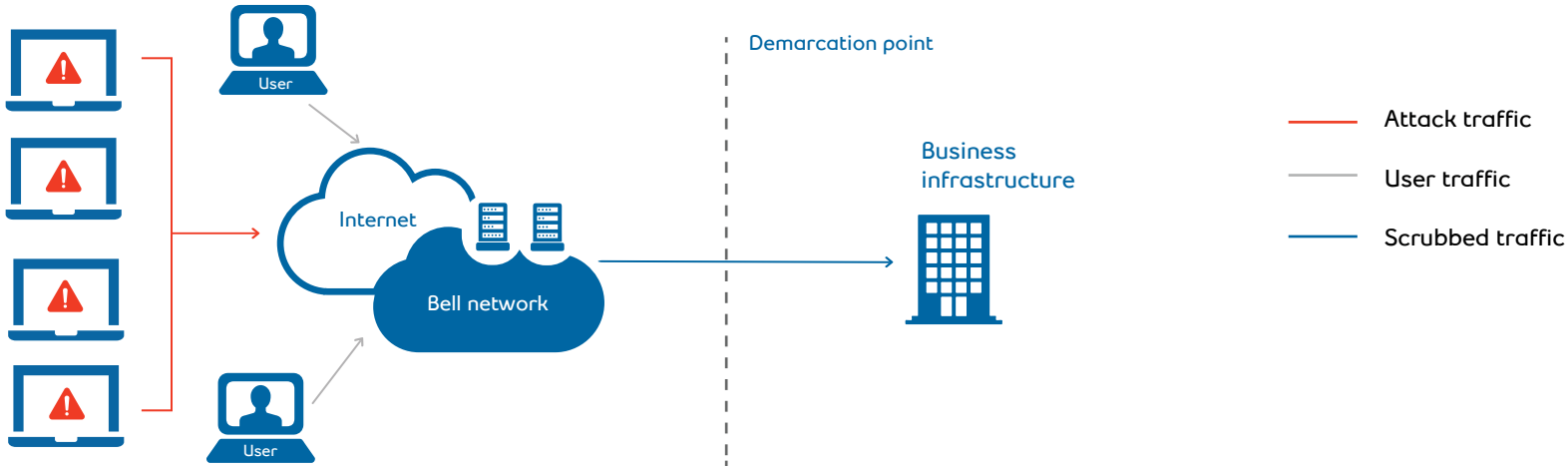
- Provides an additional layer of protection over either solution alone
- Better protection against volumetric attacks than on-premises equipment alone
- Low false-positive rate
- Cloud-based scrubbing is always up to date
- Offers greater control over implementation, management and response

Disadvantages

- Requires redirection to cloud provider for volumetric attacks
- Limited capacity to deal with volumetric attacks while waiting for redirection
- On-premises equipment requires ongoing maintenance and configuration to keep up to date with the latest threats

In-line network detection

The best stand-alone solution provides volumetric and application-layer detection and mitigation in the network itself – before bad traffic has a chance to reach your business. This type of solution is offered only by network service providers with advanced security capabilities, who are in the unique position of implementing the required mechanisms from within their own networks. In-line network detection is faster than cloud-based scrubbing: an attack can be mitigated within 30 seconds of being detected. Addressing packet anomalies and other bandwidth-intensive 'noise' upstream means less chance of bandwidth being consumed by unnecessary traffic.



Advantages

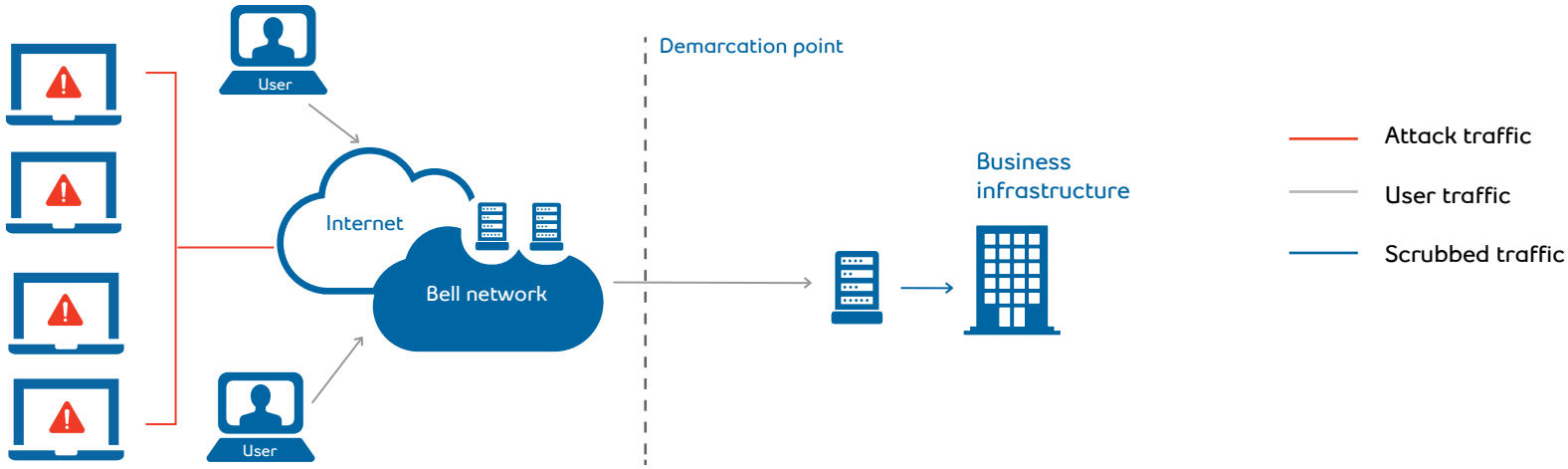
- Very low latency (no redirection to scrubbing centres required)
- Faster response and mitigation times
- Can handle large volumetric attacks
- Extremely low false-positive rate
- No on-premises hardware required

Disadvantages

- Cannot protect against SSL/SSH attacks
- Lack of direct access to protection equipment

Hybrid B: In-line network detection and on-premises equipment

The most complete and comprehensive solution is one that provides the best of both worlds: in-line detection and mitigation augmented by the more granular capabilities of an on-premises device.



Advantages

- Very low latency (no redirection to scrubbing centres required)
- Faster response and mitigation times
- Can handle large volumetric attacks
- Extremely low false-positive rate
- Complete protection through on-premises redundancy
- Can focus on very specific application-layer threats and attack thresholds

Disadvantages

- Additional cost for implementing two solutions

What you should look for in a DDoS security partner

Once you know the deployment model you think will best meet your needs, you need to choose a security provider. Here are some important questions to ask about the experience, performance, capacity and capabilities of a potential provider when trying to determine if they're a good match for your organization:

Experience

How long have you been providing DDoS protection?

Providers with a lot of first-hand experience will know what to look for when it comes to detecting and preventing attacks. They also tend to have more resilient infrastructures and more effective countermeasures, making them better prepared to handle unexpected or zero-day attacks.

What types of attacks have you mitigated?

The best providers are able to handle a wide variety of attack types. Understanding the kinds of attacks the provider has mitigated in the past will give you good idea as to the type of coverage you can expect to receive.

What's your experience researching threats?

Providers that invest in threat intelligence can offer greater insights into how the threat landscape is changing – and what it means to your business. As attacks continue to evolve, intelligence becomes an increasingly important element of an effective defence.

Performance

What is your response/mitigation time?

Being able to respond quickly to an attack is critical. If an attack persists for too long before the provider can take action, your business could experience significant downtime – resulting in lost revenue and damage to your brand.

What service level agreements/ objectives (SLAs/SLOs) do you have?

The longer it takes to mitigate an attack, the longer you're exposed to malicious traffic – making the response-time guarantees outlined in SLAs/SLOs extremely important. A provider that confidently stands behind their SLAs/ SLOs shows a commitment to delivering quality service.

What redundancies do you have in place to deliver on your SLAs/SLOs?

A provider with a service that takes into consideration uptime and has redundancies built in at every level is much more likely to live up to their SLAs/SLOs. Take the time to understand the provider's architecture to feel confident they will deliver as promised.

Capacity

What type of bandwidth can you handle?

DDoS attacks can consume massive amounts of bandwidth, often exceeding 10 or even 100 Gbps. Be sure that the provider's network and infrastructure can address huge attacks without being overwhelmed.

Are there any caps or fees that vary depending on attack size?

Some providers' fee structures include basic pricing for the service itself as well as usage fees that vary depending on the frequency and size of attacks (i.e., how much bandwidth they consume). This can result in unexpected charges and unpredictable IT expenses. Make sure you know what is and isn't included in the base price, and understand the factors that can affect your monthly costs. Wherever possible, look for fixed pricing that isn't based on bandwidth consumption.

Capabilities

Is your service always on or on demand?

An always-on service will automatically detect an attack and take action without any intervention from your team. With an on-demand service, you will need to monitor your infrastructure and manually activate a response at the first signs of an attack. Choosing one approach over the other depends on your team's monitoring abilities and the response times you require.

Is your service fully managed?

Having your security solution fully managed removes the burden from your team and ensures your protection is always up to date to handle the latest threats.

What types of attacks (and how many) do you prevent?

If the service redirects traffic to a cloud-based scrubbing centre, be sure to ask if the provider uses DNS or BGP:

- DNS is easier to set up, with no configuration changes required to your web servers. DNS routing is always on, but it is effective only for HTTP traffic.
- BGP redirects traffic based on the AS range of an IP address. While it requires more work to set up, it has the advantage of being able to protect your entire network. A BGP service can be always-on or activated on-demand.

Are your DDoS protection facilities located in Canada?

When traffic is redirected to a scrubbing centre, it may be sent outside of Canada. This may be a cause for concern for some organizations, as that traffic is then exposed to the regulations (or lack thereof) of the countries housing the scrubbing centre.

DDoS security solutions from Bell

No matter which deployment model you choose, Bell has the security expertise and network capacity to deliver a solution that meets your needs – and keeps your business up and running.

In-line network detection

A fully managed service that requires no on-premises equipment or manual intervention, Bell Network DDoS Security takes advantage of the reach of and insights gathered from the Bell network to provide multi-layered, always-on, end-to-end security at the infrastructure level, proactively identifying and mitigating attacks before they reach your corporate network.

All types of DDoS attacks are continuously monitored, regardless of their origin, size or duration.

Traffic passing through our network is continuously scrubbed and filtered, allowing us to detect and mitigate known threats within 30 seconds. And because our scrubbing facilities are located in our network core, latency is reduced to milliseconds.

Access near real-time threat reports for deeper insights into your current traffic and potential threats, as well as historical summaries of previous threats encountered.

Cloud-based scrubbing

Ideal for businesses with remote or international locations that aren't connected to the Bell network, and for those that rely on multiple Internet service providers for their connectivity, our cloud-based scrubbing service provides a consistently high level of protection against volumetric attacks without the need for any on-premises hardware.

On-premises equipment

Our network- and cloud-based services can be further augmented by one or more on-premises deployments, providing more granular defence by enacting additional application-layer protection profiles, botnet detection for outbound traffic and protection from encrypted attacks. We take care of installation and configuration, setting up the security policies needed to protect against DDoS and other cyber attacks. We can also take on the ongoing monitoring and management of your solution to ensure attacks are being mitigated properly and that attack thresholds and protection profiles are always up to date.

About Bell

Businesses that demand a reliable, highly secure IT infrastructure choose Bell. As an integral part of Canada's critical infrastructure, we deliver the most advanced threat detection, mitigation and prevention expertise in the country.

By owning and operating Canada's largest voice and data network, we have the greatest scope of visibility into potential threats against your business. We can aggregate massive amounts of data and correlate traffic patterns to proactively detect and mitigate malicious traffic – and reduce response times when incidents do occur. With a team of more than 300 security professionals and a deep understanding of the Canadian threat landscape, we have the experience to help you plan, design, build and manage an end-to-end security solution that's right for your organization.

For more information about our DDoS security solutions, request to be contacted by a Bell representative at bell.ca/contactsecurity. You can also explore related resources at the links below.

- Bell Network DDoS Security – Learn more about the benefits and capabilities of our network-based service
- Blog: An introduction to DDoS attacks – Understand how DDoS attacks work and why they happen
- Blog: The costs and consequences of DDoS attacks – Find out about the impacts an attack can have on your organization
- What is your DDoS risk profile? – Assess your organization's risk and determine the level of protection you need
- Blog: How to protect your business against DDoS attacks – Read more about what you can do to protect your digital assets and infrastructure