DDoS Shield

Acronym detects and mitigates DDoS attacks before they reach you

Distributed Denial of Service (DDoS) attacks aim to cripple an organization's network, servers or applications by overwhelming them with malicious traffic, which can cause them to go down for anywhere from a few minutes up to days at a time. Such attacks can severely limit an organization's ability to function and typically cost hundreds of thousands of dollars in damages, lost revenue and consumer trust.[1]

Why it matters

The rates of successful DDoS attacks continue to rise every year—with 4.83 million attacks in the first half of 2020 alone, and a 25% jump between March and June.[2]

DDoS Shield from Acronym can protect your business from the dangers of DDoS attacks before they reach your network. Featuring 24/7/365 detection and mitigation in seconds, plus an easy-to-use portal for comprehensive visibility into your threat landscape, you'll gain peace of mind knowing that your business is protected. And, because DDoS Shield can be added to your Acronym Internet service, you'll reduce your overall security investment and cyber risk in the process.

How it works

Acronym's DDoS Shield makes use of automated cyber threat detection and mitigation technology that works in real time to monitor for malicious traffic and block it in seconds, before it can affect your communications network.

Because the detection and mitigation of your traffic is contained within Canada in the Acronym network—unlike other solutions, many of whom do not have scrubbing centres in Canada—network latency is kept to a minimum and your data remains under Canadian jurisdiction.

And, for added insight into your organization's overall threat landscape, DDoS Shield offers access to a secure customer portal, for a real-time view of practical attack analytics (e.g., top attacked assets) along with details about each attack (e.g., status, type, frequency, duration and size), all of which is useful to improve your security posture. You can also choose to receive real-time email alerts that will notify you when an attack has occurred, as well as reports for clear and actionable intelligence on DDoS attack activity happening across your network.

1 Source: Corero, "The Impact of DDoS on Enterprise Organizations"
2 According to the Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac
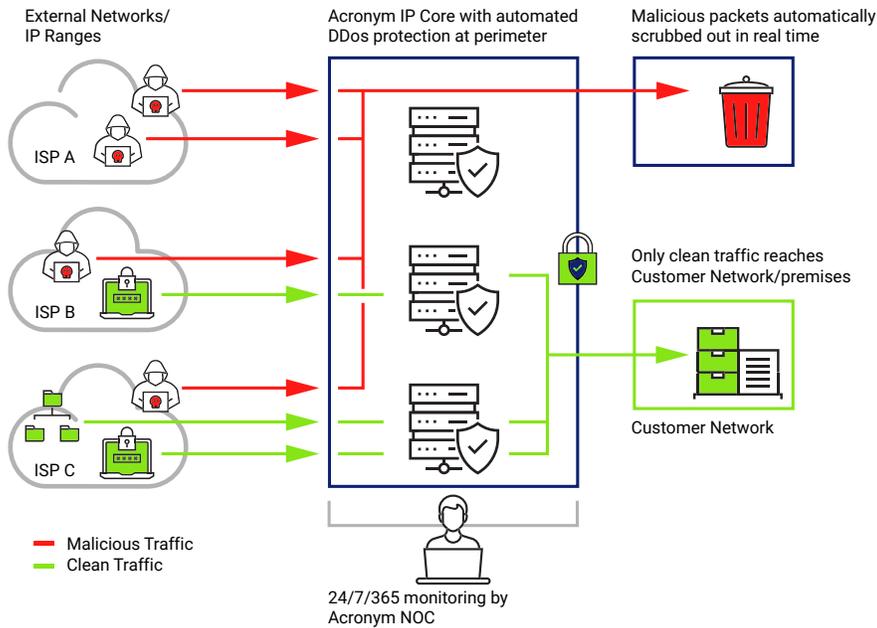
To learn more about this and other offerings

✉ HOTSales@HydroOne.com   📞 1.866.345.6820

Join our mailing list

Sign up

ACRONYM

Security

DDoS Shield

External Networks/
IP Ranges

ISP A

ISP B

ISP C

— Malicious Traffic
— Clean Traffic

Acronym IP Core with automated
DDos protection at perimeter

Malicious packets automatically
scrubbed out in real time

Only clean traffic reaches
Customer Network/premises

Customer Network

24/7/365 monitoring by
Acronym NOC

Features and benefits of Acronym's DDoS shield

Acronym's DDoS Shield solution delivers automated, intelligent defense that quickly and seamlessly protects against volumetric

Layer 3 through 7 and state exhaustion attacks, including multi-vector and zero-day threats. Features and benefits include:

24/7 Automated Detection	• Smart technology actively monitors all traffic that runs through the Acronym network to automatically detect and block malicious traffic before it impacts your network, without the need for in-house security expertise or manual intervention • Industry leading, innovative, multi-stage detection and mitigation enriched using behavioural and machine analysis • Comprehensive and accurate protection against the latest trends and attack vectors, which are continually enhanced based on real-world attack analytics
In-Line Detection and Mitigation	• In-line detection and mitigation in seconds, well before reaching your network—for ultra-low latency • Advanced technology protects legitimate traffic without degrading performance and with negligible false positives • Huge total mitigation capacity (100 Gbps)—comparable to other leading Canadian ISPs
Real-Time Customer Portal	• Complete visibility into history and nature of attacks, including size, frequency and duration, for deeper cybersecurity insight and situational intelligence • Alerting and reporting for clear, actionable intelligence and compliance reporting
Data Sovereignty	• Canadian sovereignty protection with a platform that resides in Acronym's Canadian-owned and -operated network, which means your traffic is monitored and protected under Canadian legal jurisdiction

To learn more about this and other offerings

✉ HOTSales@HydroOne.com   ☎ 1.866.345.6820

Join our mailing list

Sign up