# Preventing DDoS attacks with a layer of Varnish

Even before COVID-19 hit, ***DDoS attacks were up 180%*** in 2019 compared to 2018.

**40%**
**Increase**

DDoS (distributed denial of service) attacks up by at least 40% since COVID-19 began *

* Source: Telecoms.com, 2020

**$2M**
**Cost**

A Kasperksy study estimated that the average downtime cost due to lack of availability for enterprise DDoS outages, as high as USD 2 million


More than ***58% of cybersecurity execs*** cite DDoS as an increasingly menacing threat vector, according to Neustar International Security Council*

* Source: Neustar, 2020

# *Varnish solutions for security/DDos*

## Varnish High Availability

Boosts resilience by reducing risk of cache misses that can cause latency and traffic surges

Simple configuration, maximum stability

## Use Varnish, VCL and HTTP protocol to:

Ensure capacity to handle incoming traffic volume

Identify and stop attacking requests at the edge

## Security by design - VMODs:

Request inspection with vmod-bodyaccess to help identify potentially dangerous traffic

Throttling with vmod-vsthrottle slows incoming requests when suspicious activity is detected

To find out more about how **Varnish Software** can ensure you can meet all your content delivery needs at scale, visit **www.varnish-software.com**

VARNISH SOFTWARE