RED BUTTON
DDoS Experts

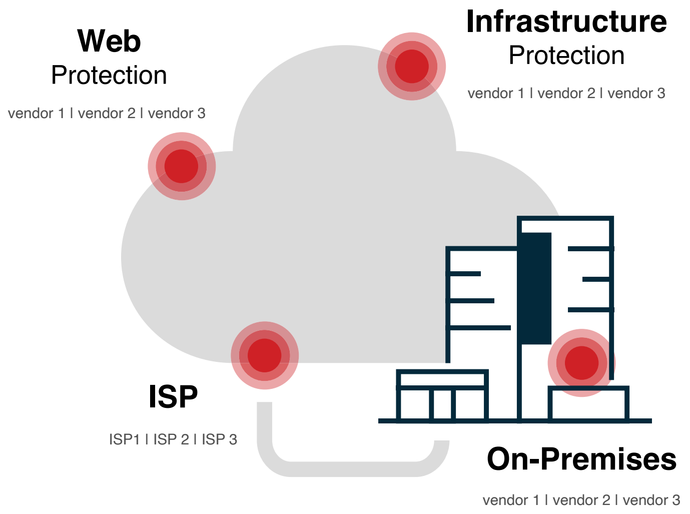
DDoS Technology Hardening

Our DDoS Hardening service strengthens your technology infrastructure to maximize protection against the most sophisticated DDoS attacks.

Network Architecture

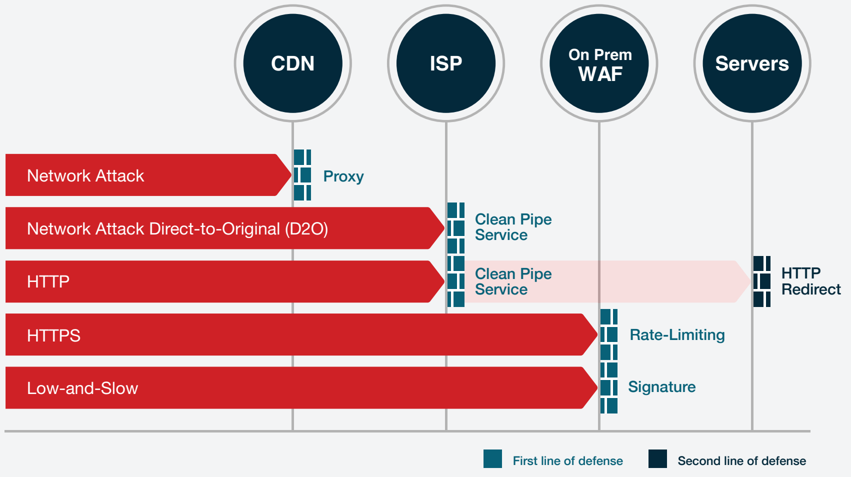
We begin by auditing your current DDoS network architecture infrastructure. Our experts identify weaknesses and provide recommendations for improving the underlying architecture to maximize DDoS protection. This step is taken regardless of any specific vendor and is intended to ensure that your protection foundation includes the right components at the right locations.

DDoS protection architecture. *We begin by defining the optimal protection architecture and examining all locations - web/infrastructure, on-premises, and ISPs. This foundation step takes place regardless of the specific vendor solutions.*


Web
Protection
vendor 1 I vendor 2 I vendor 3
Infrastructure
Protection
vendor 1 I vendor 2 I vendor 3
ISP
ISP1 I ISP 2 I ISP 3
On-Premises
vendor 1 I vendor 2 I vendor 3

Next, we conduct an analysis of attack vectors. We analyze all potential DDoS attacks and determine how each type will be handled by the protection components in your recommended architecture.

***The attack vector analysis** outlines the potential DDoS attacks on your systems and describes how each attack type will be handled by the different components in your protection architecture. The diagram is for demonstration purposes and is a simplified version of an actual analysis.*



Configuration Optimization

Installed DDoS protection gear is often underutilized. Our team dives into the setup of your protection solution(s) and provides detailed instructions on improvements to their configuration.

For example, we ensure that rate limit thresholds are well-calibrated, that you have chosen the most appropriate web challenge, that you fully utilize bot protection, geo-protection, etc.

Vendor Selection

As a vendor-agnostic consulting company, we are deeply knowledgeable about the capabilities of all DDoS vendors and can help select the DDoS protection solution that best meets your needs, thereby saving your team many man-hours.

Vendor selection is an optional service, which may be purchased separately from the core Hardening service. Our DDoS experts guide you through a meticulous and methodical vendor evaluation, using an RFP template that includes over 80 selection criteria, with the ability to adjust the weight for each requirement and assign scores to vendors. In addition, we provide a recommendations document presenting several DDoS vendor options that are most suitable for your requirements, with an analysis of the pros and cons of each in relation to your architecture and needs.

Deliverables

The DDoS Hardening service provides a detailed report with the following elements:

Current Protection Status

An analysis of the current DDoS protection, including a **DDoS Resiliency Score** - an objective measurement of the type of attacks that your organization can withstand prior to our service.

Topology Recommendations

Detailed recommendations on the optimal DDoS defense architecture (e.g., cloud-based, on-premises, hybrid), including a vector analysis diagram describing which component will stop which type of attack.

DDoS Configuration Recommendations

Specific instructions on changes and adjustments to be applied to the configuration of your DDoS protection solution.

Vendor Shortlist

In cases when we advise on adding DDoS technologies, we provide a recommended vendor shortlist.