

Eliminate DDoS Vulnerabilities

Industry: Government

Governmental institutions and the public are reliant on online services must have continuous online business continuity. Disruptions to these online applications and services damage public confidence and could become an issue of national security.

Governments are a major target for DDoS attackers

-  **Political and ideological motivated attacks**
-  **Successful DDoS attacks are highly publicized and shake public confidence**
-  **Many governments move online to provide multiple public services, online payments, and other informational services**

Case Study: National Elections

RADAR was deployed by the Israeli government to protect over 2,300 digital services from DDoS attack.



Under Fire

Government departments are under constant threat from multiple groups



Stable Elections




Online availability during elections is critical for democracies

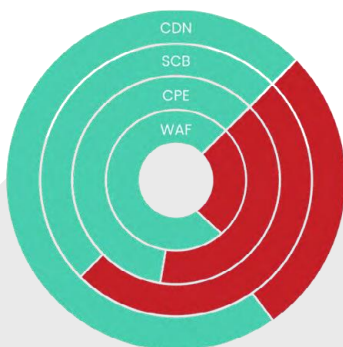


Zero Downtime

With over 2,300 governmental services provided, downtime due a DDoS attack is not an option

DDoS Gap

-  Vulnerable
-  Protected
-  Partially Protected



DDoS Protection Coverage Before RADAR



RADAR for Government

DDoS Protection Following RADAR Deployment



The Solution

Once RADAR was deployed, the governmental cybersecurity unit gained complete visibility into its DDoS security posture. Following initial testing, several DDoS protection layers were identified as vulnerable. Working with DDoS protection providers, MazeBolt prioritized remediation efforts to ensure continuous availability with zero disruption to online services.

- > Remediated Vulnerabilities**
Discovered regions of the network that weren't protected and closed vulnerabilities quickly and efficiently.
- > Zero Downtime**
Zero interruption to online services during testing and remediation periods, while successfully blocking all attack attempts.
- > Full Visibility**
The security team gained full visibility into each security layer.
- > Complete Resilience**
Despite being targeted by threat actors, no sites that implemented RADAR experienced a DDoS attack.

THE BENEFITS

The government's head of IT security indicated that the continuous visibility provided by RADAR, combined with the clear and precise reports allowed the cyber security department to dramatically reduce their DDoS risk and ensure the parliamentary elections took place without disruption.

The Israeli government is constantly under attack by threat actors, but since implementing RADAR, it has experienced zero downtime and gained complete visibility into its online services.

MazeBolt takes pioneering a new approach in DDoS security. MazeBolt RADAR™ is the only solution that identifies and enables the elimination of DDoS vulnerabilities in every layer of DDoS protection, by continuously testing every attack vector across online services, with zero operational downtime. Using RADAR's patented vulnerability testing technology, enterprises have unparalleled visibility into their DDoS protection solutions so they can be confident that damaging DDoS attacks can be prevented - before they happen.