Preferred Remediation Technology Alliance

Ensuring the Best DDoS Protection for Joint Customers

F5, the global leader in multi-cloud application security and delivery, is now a part of the MazeBolt Preferred Remediation Technology Alliance Program. This program is the first of its kind and the only combined solution on the market that ensures avoidance of a damaging DDoS attack, through fully automated and reliable DDoS protection for mutually valued customers.

This technology alliance enables MazeBolt's and F5's mutual customers to gain streamlined remediation of DDoS vulnerabilities identified in their online services. MazeBolt RADAR™, together with F5, allows organizations to obtain critical information on DDoS vulnerabilities and remediate them quickly, using F5 security solutions.

The Critical Challenge of DDoS Protection

DDoS Protection Configurations
Dynamic IT environments require DDoS protections to be constantly reconfigured to automatically protect.

Damaging DDoS Downtime
Successful DDoS attacks are a result of unpatched DDoS vulnerabilities.

DDoS attacks Incline
DDoS attacks increased from 2022 by over 60% in 2023, with more than 16 million attacks predicted in 2024.

No DDoS vulnerability data
No continuous visibility to vulnerability data.

Damaging SLAs time-to- mitigation & Emergency Response Time
When DDoS vulnerabilities are not patched, unnecessary damages are inflicted when targeted by an attacker.

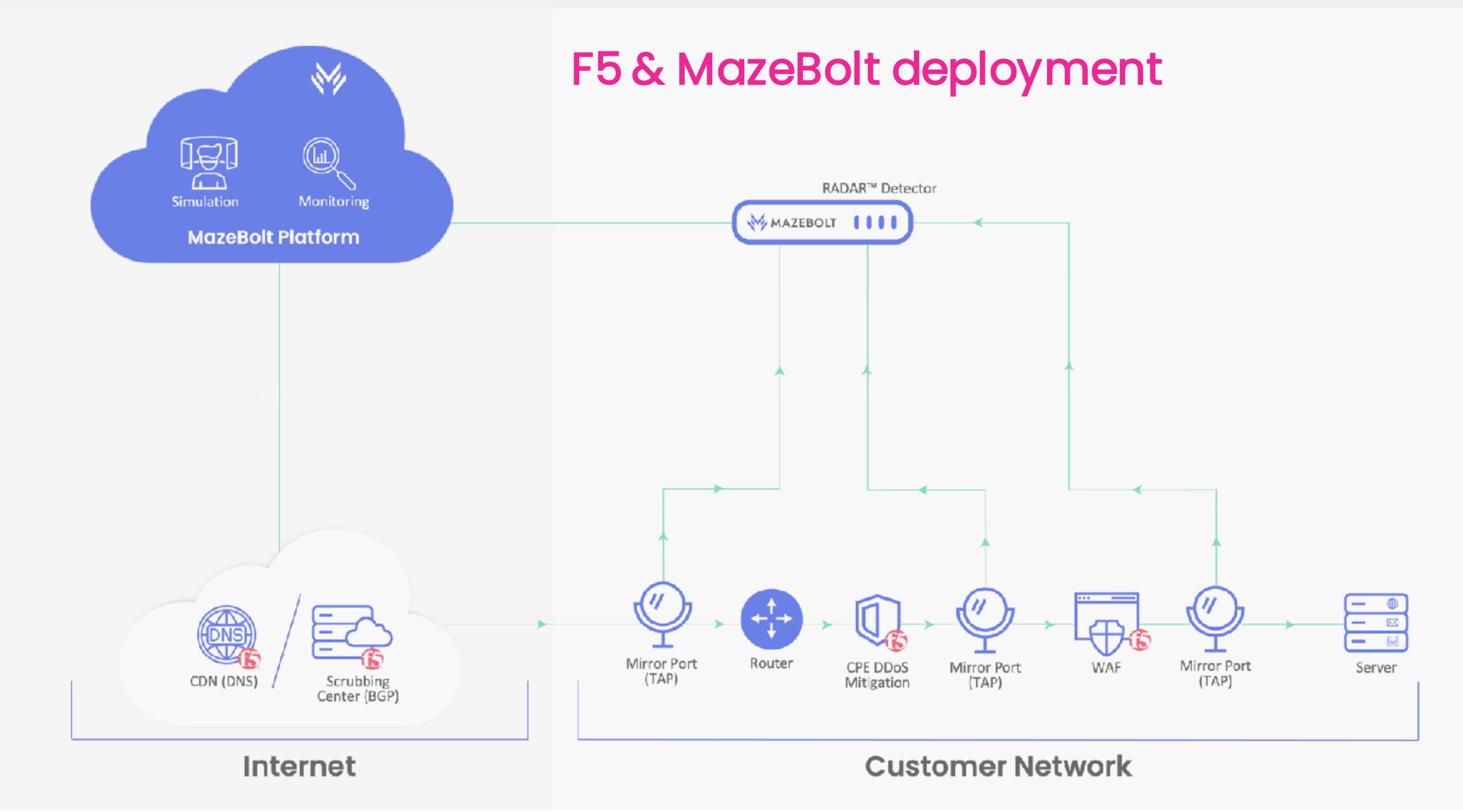
Downtime causes financial damages
And also reputational losses - both immediate and often a major impact on market cap.

What is MazeBolt's Critical Breakthrough?

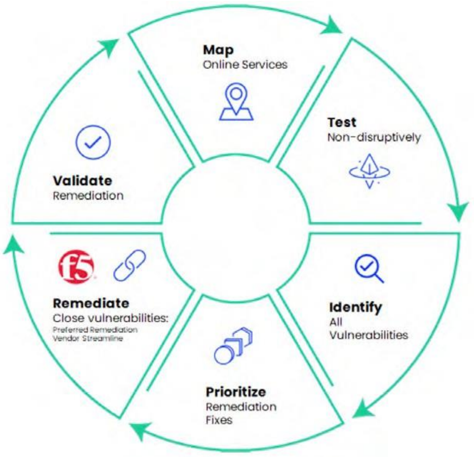
The only way to prevent a damaging DDoS attack is to have zero vulnerabilities in the DDoS protections deployed. RADAR is the first and only solution that identifies and enables the remediation of DDoS vulnerabilities. RADAR's technology is a patented and non-disruptive DDoS testing solution: automated, adaptive, and autonomous.

Continuously testing more than 150 DDoS attack vectors against all targets in an organization's environment, RADAR requires zero operational downtime or maintenance windows to run. The solution validates manual DDoS protection SLAs against automated DDoS protections with zero downtime, thus marking a paradigm shift in DDoS protection - from emergency remediation during a damaging attack to preventative remediation and attack avoidance.

F5 & MazeBolt deployment



F5 & MazeBolt: A technology alliance to take your DDoS security to the next level



Following the identification of DDoS vulnerabilities by RADAR, **remediation reliability and efficiency are key.**

The F5 SOC team works with the customer and MazeBolt to configure F5 products and services with zero downtime and no disruption to ongoing production, all according to a prioritized plan.

Once RADAR validates the fixes, it continuously tests the customers' environment for more vulnerabilities in layers 3, 4, and 7, against over 150 DDoS attack vectors, not allowing any vulnerability to cause damaging downtime to the IT infrastructure and online services.

A preferred remediation vendor is a mitigation provider that's been identified by MazeBolt as competent and cooperative in facilitating the streamlined process of vulnerability remediation. This groundbreaking alliance has been selected by governments, banks, stock exchanges, payment providers, insurance companies, and gaming organizations, among others, to achieve zero downtime from DDoS attacks.

Combining F5's solutions with RADAR provides the best protection SLAs available for any customer – an objective of zero-second automated SLAs.

MazeBolt acknowledges that F5 has the ability and capacity to prioritize and remediate DDoS vulnerabilities in a streamlined fashion that ensures the best security available for its customers - thus, empowering stakeholders and security teams to adopt the new transformative approach of automated DDoS security and achieve DDoS resilience.

> F5 and MazeBolt RADAR DDoS solutions allowed us to identify and reliably remediate hundreds of identified DDoS vulnerabilities over the last two years. At the start, the number of vulnerabilities RADAR identified left a major challenge for our DDoS vendors to remediate, causing remediation delays that could have led to damaging attacks on our services. The preferred remediation technology alliance between F5 and MazeBolt showed us that we can be confident that our target SLA of zero downtime and complete avoidance of damaging DDoS attacks can be reliably achieved. After working with both companies, I'm certain this alliance provides a reality where organizations using F5 and MazeBolt RADAR will no longer rely on out-of-touch damaging time-to-mitigation SLAs or emergency response time scenarios.
>
> Yaron Weiss, Chief Security Officer, Payoneer.

MAZEBOLT www.mazebolt.com

MazeBolt is pioneering a new standard in DDoS security. RADAR™, an industry-first patented solution, empowers organizations to identify and remediate vulnerabilities in every layer of DDoS protection. Global enterprises, including financial services, insurance, gaming, and high-security government environments, rely on MazeBolt to prevent damaging DDoS attacks.

f5 www.F5.com

F5 is a multi cloud application services and security company committed to bringing a better digital world to life. F5 showcases a portfolio of automation, security, performance, and insight capabilities which empowers our customers to create, secure, and operate adaptive applications that reduce costs, improve operations, and better protect users.