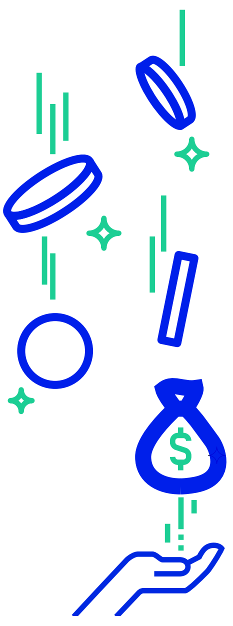
Ultimate DDoS Coverage for Fintech Companies

The DDoS Problem

The Financial Services Information Sharing and Analysis Center (FS-ISAC) disclosed that more than 100 financial services firms were targets of a wave of DDoS extortion attacks last year. Customers' demands such as security, faster transactions, and unlimited access put fintech companies under constant pressure to make their service available 24*7. Why is it not easy to achieve this goal? DDoS attackers love to target fintech companies because they have money and they must make their services available 24*7.

Below examples of DDoS attacks prove criminals are successfully launching more sophisticated attacks and getting past the best mitigation systems. With increasing DDoS threats, are fintech companies prepared enough to block DDoS attacks?



Damaging DDoS Attacks on Fintech

	Country	Company	Impact of the Attacks
2021	US	EXMO Cryptocurrency	The massive attack (30GB per second) affected the company's entire infrastructure, including the website, API, Websocket API, and the exchange charts.
	USA	Bitcoin.org	The website was hit with an "absolutely massive" DDoS attack along with a ransom demand for 0.5 Bitcoin (BTC).
2020	USA	Trezor, Poloniex, The Block	Several DDoS attacks have hit the crypto industry. Trezor's online store was hit with a DDoS attack several days after The Block and Poloniex were targeted.
	UK	Trading 212	Several DDoS attacks have hit the crypto industry. Trezor's online store was hit with a DDoS attack several days after The Block and Poloniex were targeted.
	USA	MoneyGram & PayPal	Targeted by the DDoS-for-Bitcoin group with attacks of up to 200 GB/sec worth of bandwidth on backend infrastructure, DNS servers, and API endpoints.
	New Zealand	NZX Stock Exchange Broker	Sporadically disrupted network connectivity, websites, market announcement platform, and trading in its cash markets.

Why DDoS Mitigation Solutions are Not Enough

Damaging attacks are penetrating the best mitigation solutions

DDoS mitigation solutions need manual configuration after every minor upgrade in the system. So unless the security team ensures its reconfiguration, there is no guarantee the solution can protect the network from a sophisticated DDoS attack.

In addition, the solutions are reactive in nature, meaning they are designed to act only after a DDoS attack has already been launched at the network.

Therefore, waiting for a mitigation solution to identify an ongoing DDoS attack is risky because the network will suffer downtime in case of delays or failure to detect the attack.

The DDoS Pain

Fintech companies have to continuously upgrade service policies and technology to meet the dynamic industry requirements. As a result of such digital transformation, several vulnerability points are created in the network; those can become susceptible to DDoS downtime if not detected and fixed timely. Security personnel can patch ongoing DDoS vulnerabilities only if they get real-time insights. However, traditional testing tools cannot be used to identify ongoing DDoS vulnerabilities because such tools perform only when the website is in maintenance mode. As a result, the dire need for fintech companies to stay online minimizes the application of traditional testing tools for vulnerability identification. It means the security team does not get real-time information, and the test results become obsolete whenever there are any changes in the network.

Benefits of Simulating DDoS Attacks with New Technology - RADAR™

Companies can validate the deployed mitigation policy and confirm if it is truly protecting networks by continuously simulating DDoS attacks using the latest sophisticated DDoS vectors. As a result, companies can identify DDoS vulnerabilities in real-time and perform quick remediation.

MazeBolt's new technology, RADAR™, is the only 24/7 automatic DDoS attack simulator. Working with any mitigation solution installed, RADAR™ offers superior DDoS coverage and automated DDoS protection. RADAR™ simulates over 100 attack vectors with all public-facing IPs 24/7, giving real-time visibility to all DDoS vulnerabilities with zero downtime.

Learn more about RADAR™

About MazeBolt

MazeBolt introduces a new standard in DDoS coverage, automatically detecting, analyzing, and prioritizing remediation across the network, doubling coverage, and virtually eliminating DDoS exposure without shutting down organizational operations. MazeBolt's continuous defense supercharges the performance of CISOs as well as the mitigation service provider.

www.mazebolt.com | info@mazebolt.com