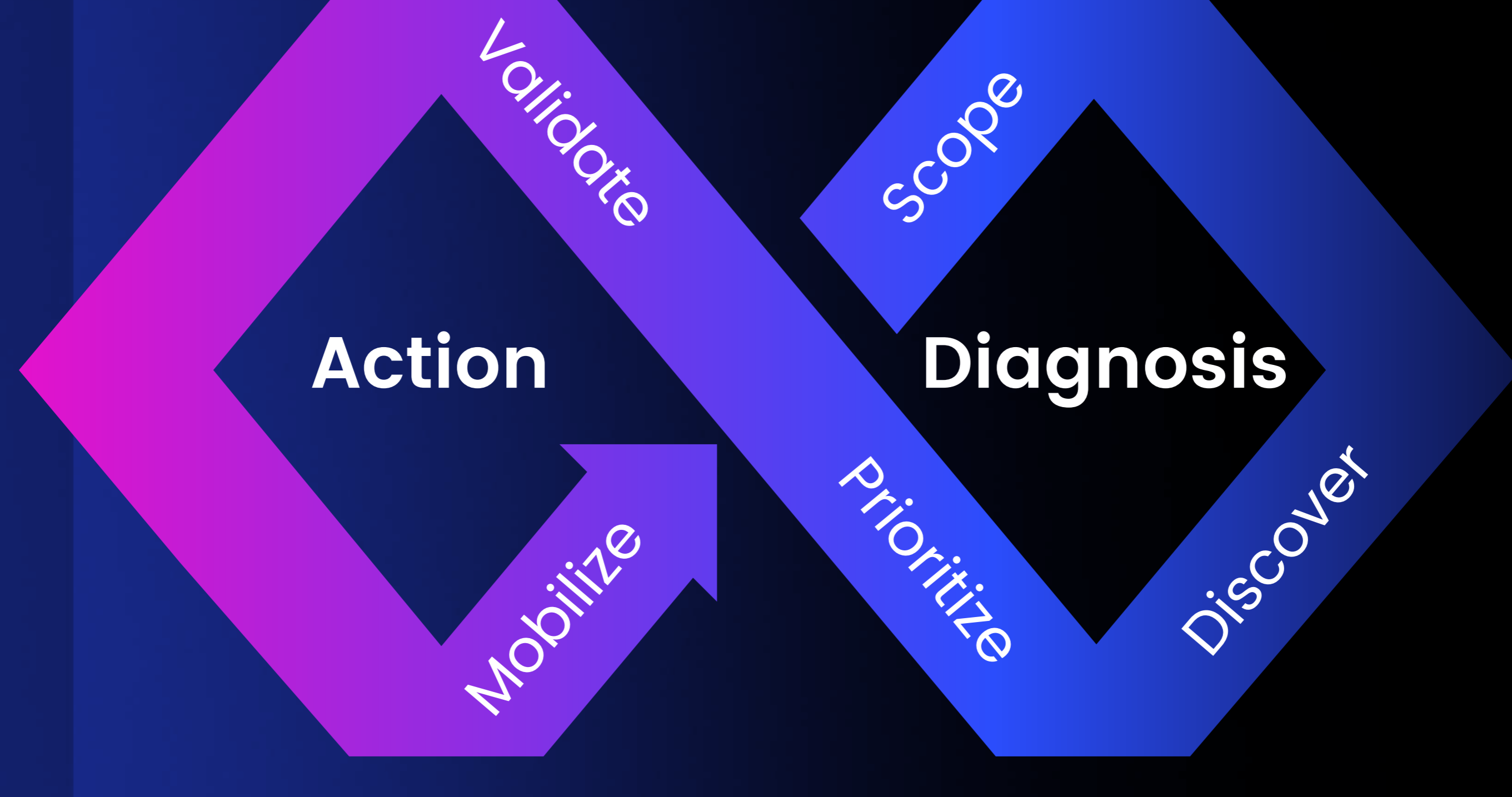


# Put Business Continuity First

MazeBolt RADAR Aligns DDoS Vulnerability Testing with Gartner's Continuous Threat Exposure Management (CTEM) Framework



**3x**  
less risk exposure

The risk of breach drops, when security investments are prioritized based on a continuous exposure management program.

**200%**  
increase in DDoS attacks

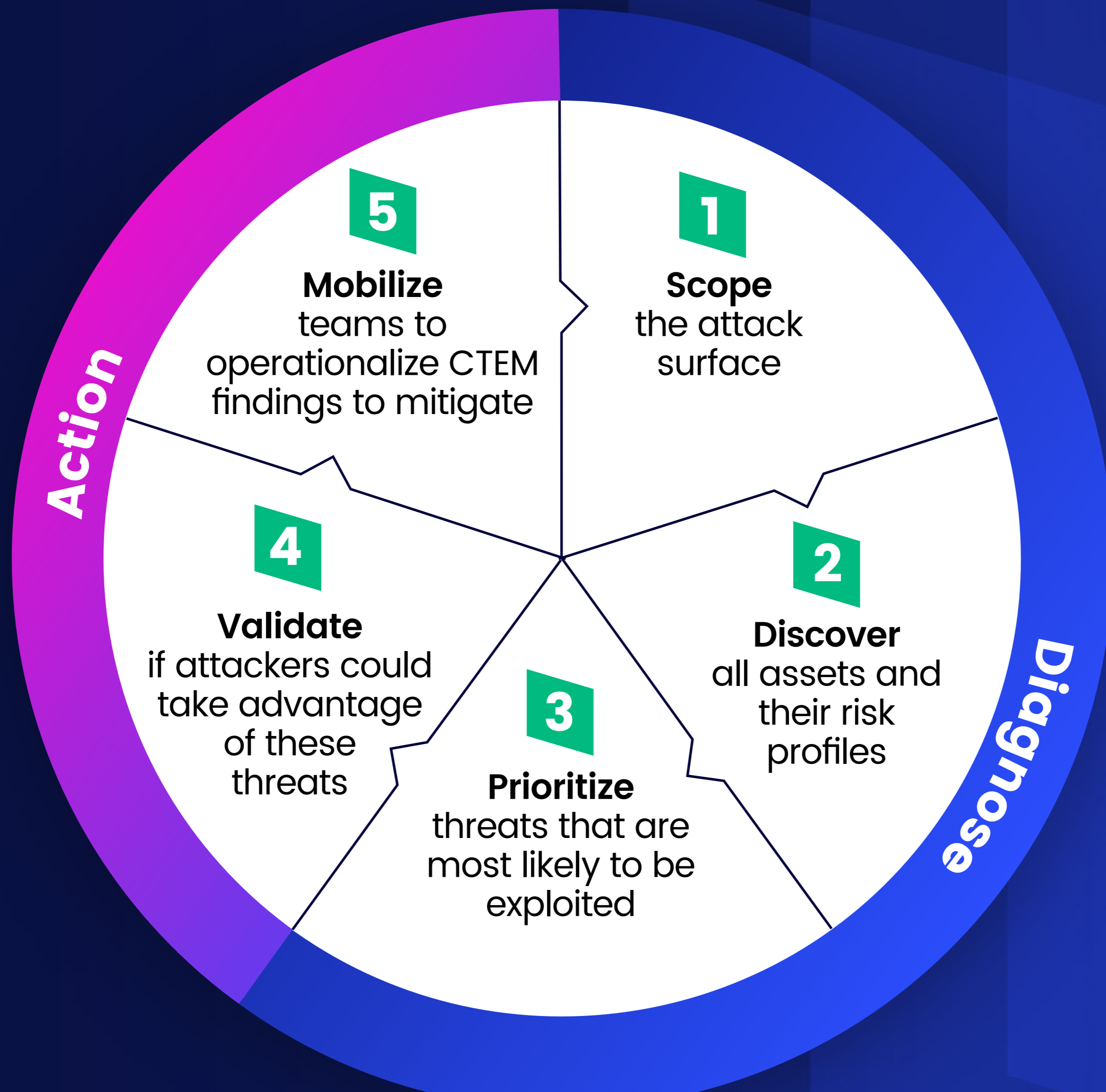
The number of DDoS attacks rose sharply in 2023 - compared to 2022.

**60%**  
implement framework

Most organizations surveyed are already pursuing, or planning to implement a CTEM framework.

By aligning proactive risk assessment of DDoS attacks with the CTEM framework, organizations can bolster the identification and mitigation of DDoS threats - proactively.

## 5 Steps in the Cycle of Continuous Threat Exposure Management



Source: Gartner CTEM Framework

## CTEM Alignment Calls for Continuous DDoS Testing

### The Problem

For DDoS risk assessment, organizations often hit a visibility wall.

How can leaders be sure that a deployed DDoS protection solution is effective?

Without insight into the effectiveness of DDoS protections, it's impossible to evaluate cyber resilience.

### The Solution

To diagnose risk across a complex network infrastructure in line with CTEM principles:

**1**  
Proactively look for gaps or weaknesses in current DDoS protections

**2**  
Ensure no business disruption - no downtime to live environments.

## MazeBolt RADAR™ Continuous DDoS Testing for Business Continuity

Proactively manage the risk of DDoS attacks

Align with Gartner's CTEM framework

Automate continuous testing, across online services and attack vectors

Avoid any disruption or downtime

Flag DDoS vulnerabilities immediately

Receive recommended steps for mitigation

Interested in implementing automated DDoS protection that's fully-aligned with CTEM principles?

[Reach out to MazeBolt](#) →