

# The ROI of Continuous DDoS Validation

Continuous DDoS validation is not just a smart security practice – it's a business investment with significant returns.



## Direct Costs of Damaging DDoS Attacks

In most situations, the direct costs of an attack are just a small fraction of the total losses. Direct costs include:

- Revenue loss from downtime
- Expenses associated with remediation and recovery
- Emergency spend

## Indirect Costs Often Drive the Biggest Losses

The potential impact of damaging DDoS downtime is significant when it comes to:

- Customer Churn
- Brand and Trust Damage
- Regulatory Scrutiny and Penalties
- Market Value (for Public Companies)

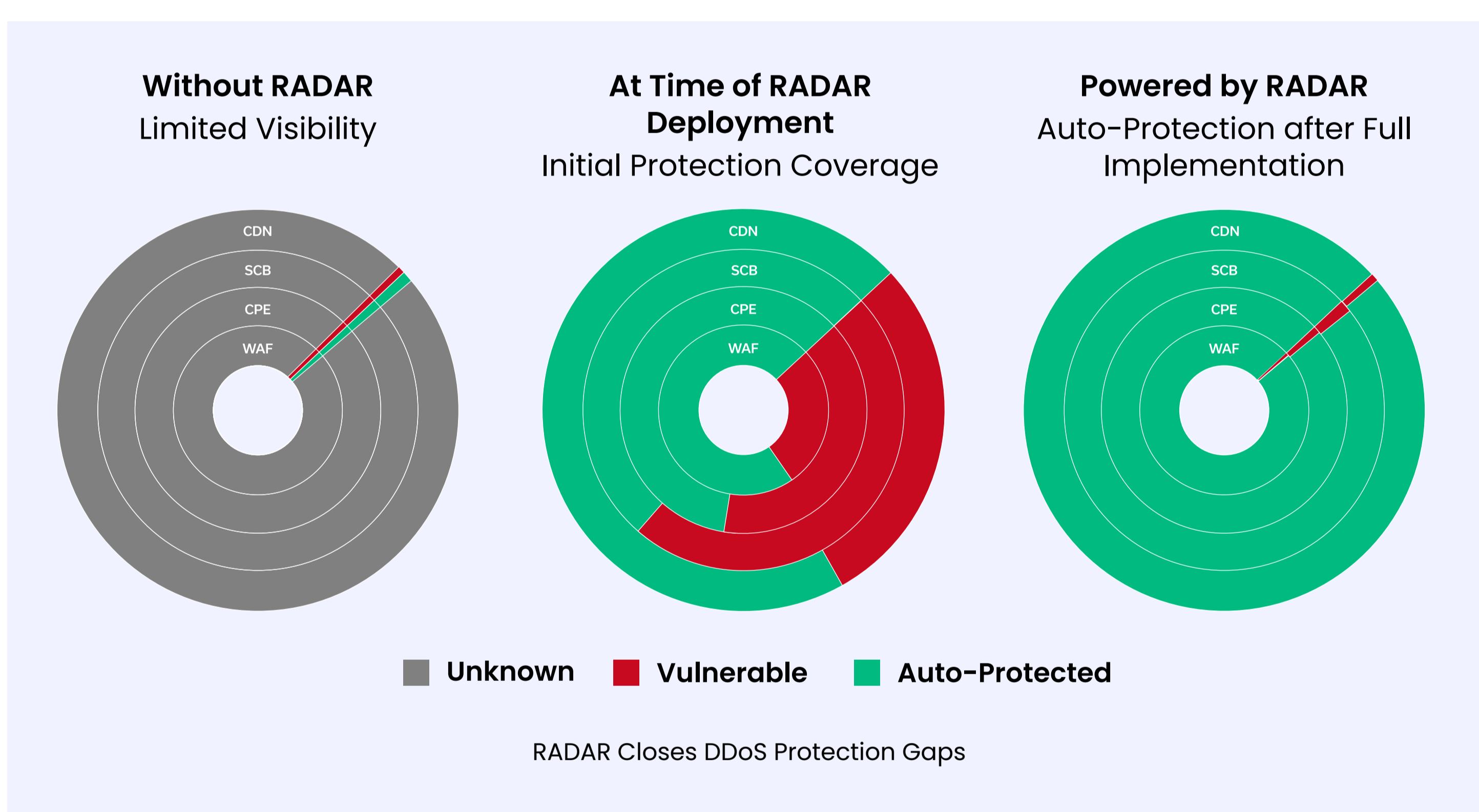
## Why Continuous DDoS Validation Pays Off

RADAR™ by MazeBolt tests the full DDoS attack surface across all public-facing IPs and FQDNs. It runs automatically in live production environments without requiring downtime or manual coordination, thereby supporting:

- Reduced risk of downtime
- Stronger compliance posture
- Validated defense readiness

Red Team Testing	RADAR by MazeBolt
Annual or biannual	Continuous
Tests <1% of the attack surface	100% attack surface visibility
Requires maintenance window	10,000+ nondisruptive simulations (OSI layers 3, 4 & 7)
Validation requires an additional Red Team test, requiring another maintenance window	Immediate validation of fixes

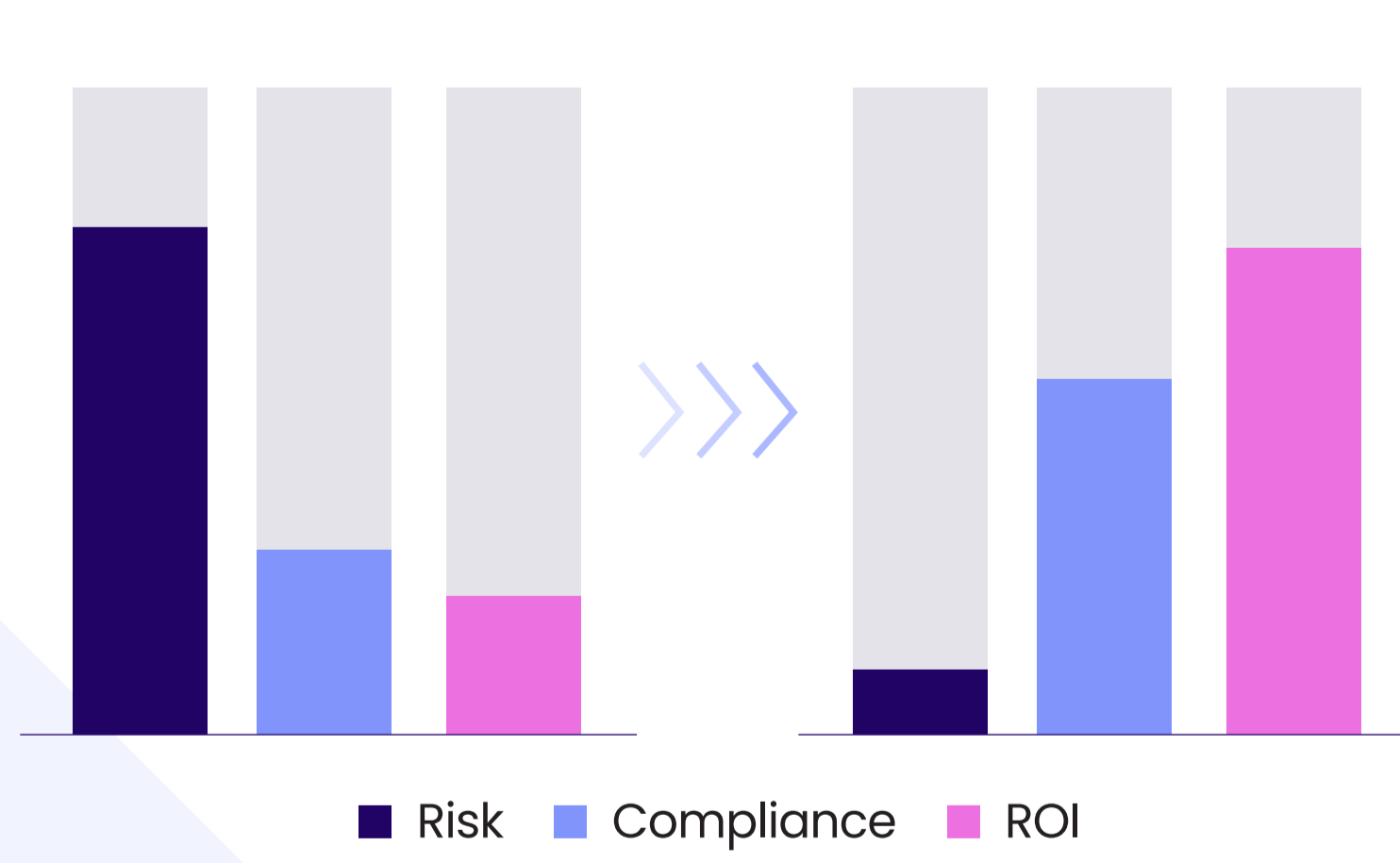
These capabilities eliminate the need for scheduled, DDoS-related maintenance windows and recovery procedures, reducing operational strain and freeing security teams to focus on other priorities.



## Visibility Becomes a Strategic Asset

Visibility is essential in order to eliminate existing DDoS vulnerabilities and misconfigurations. In other words, what you cannot see, you cannot fix. The data obtained by means of continuous DDoS validation provides valuable advantages and financial benefits:

- DDoS exposure insights
- Identifies gaps and misconfigurations
- Builds stakeholder confidence



## A Proven Adoption Roadmap

- 1 Integrate with existing DDoS defenses
- 2 Establish a testing baseline
- 3 Remediate based on priority
- 4 Report and align with stakeholders
- 5 Operationalize continuous cycles

Want to learn more about the ROI of continuous DDoS validation?  
[Download the eBook](#)