RADAR™ von MazeBolt

Kontinuierliche, nicht-disruptive DDoS-Schwachstellentests

RADAR gewährleistet die Webpräsenz globaler Unternehmen, indem es deren DDoS-Abwehrmaßnahmen auf Live-Produktionssystemen validiert – ohne dass Wartungsfenster erforderlich sind.

Auf diese Weise können Unternehmen kritische Schwachstellen in ihren DDoS-Abwehrmaßnahmen und -Konfigurationen identifizieren und beheben, ohne den normalen Geschäftsbetrieb zu stören.

WICHTIGSTE VORTEILE

✓ Erreichen Sie eine messbare Reduzierung des DDoS-Risikos

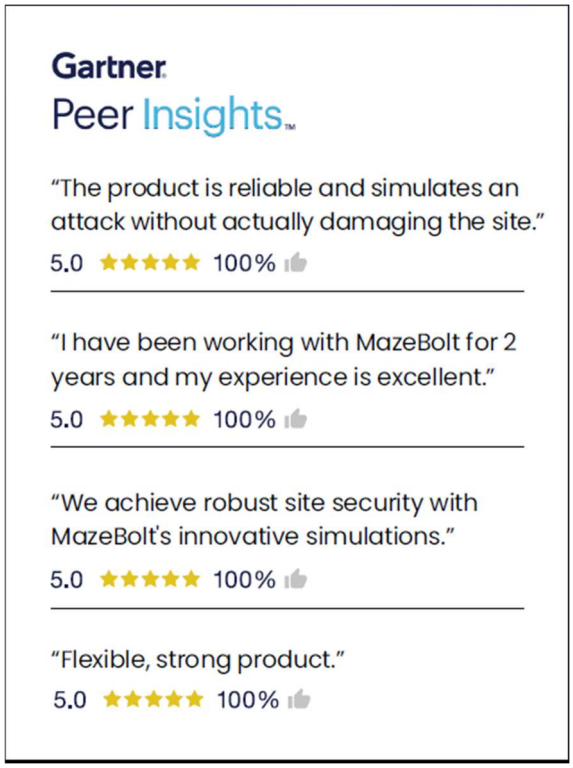
✓ Validieren Sie Ihre DDoS-Abwehr

✓ Stärkung der Einhaltung gesetzlicher Vorschriften

✓ Optimieren Sie Ihre Investitionen in eingesetzte DDoS-Schutzmaßnahmen

Die patentierte Technologie RADAR von MazeBolt nutzt KI, um priorisierte DDoS-Angriffssimulationen über die OSI-Schichten 3, 4 und 7 hinweg durchzuführen – sowohl mit menschlichen als auch mit KI-gesteuerten Angriffsvektoren.

RADAR ermöglicht es Banken, Finanzdienstleistern und Versicherungsunternehmen, die am stärksten unter DDoS-Angriffen und Ausfallzeiten leiden, Schwachstellen mit hoher Priorität zu identifizieren und zu beheben – ohne Unterbrechung der Online-Dienste. Mit RADAR können Unternehmen die durch DDoS-Angriffe verursachten betrieblichen, reputationsbezogenen und finanziellen Schäden vermeiden.



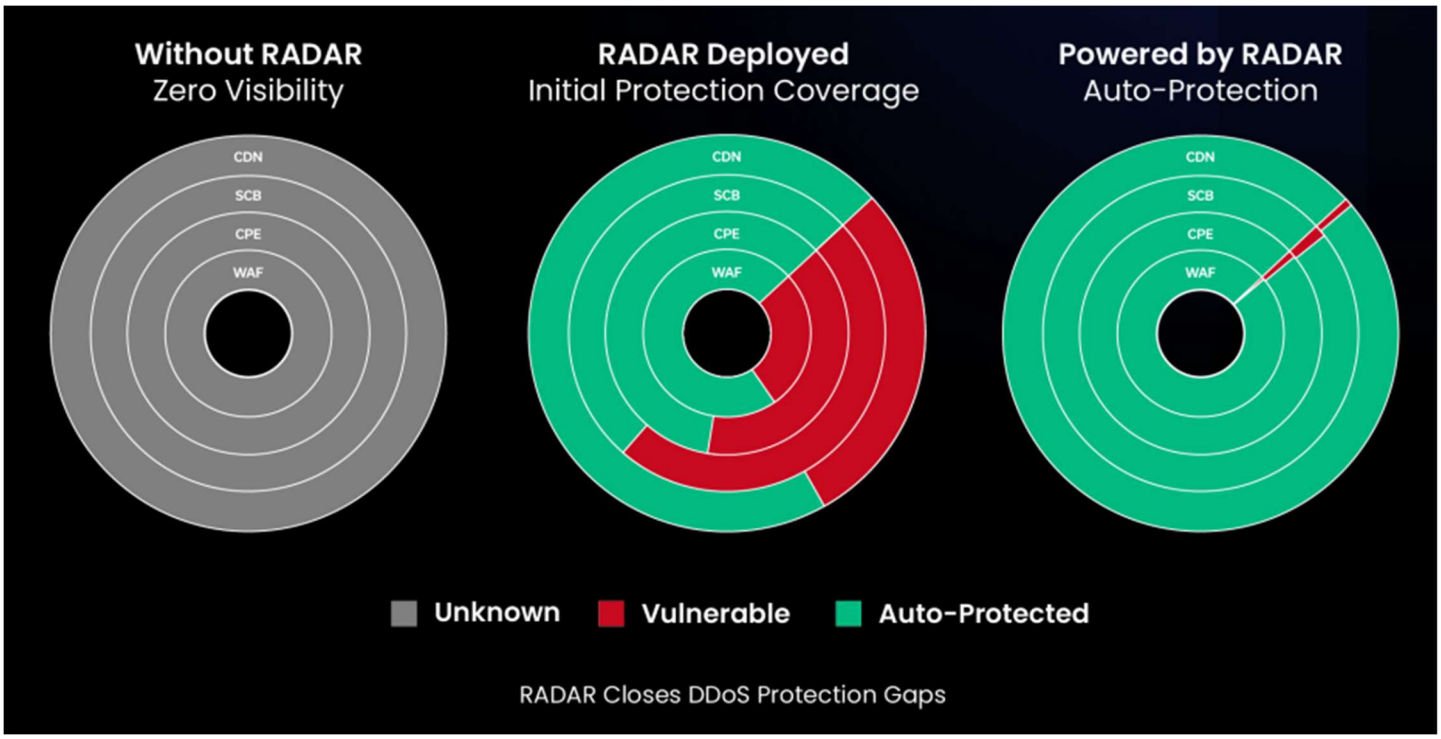
MAZEBOLT

Testen und validieren Sie Ihre DDoS-Schutzmaßnahmen ohne Beeinträchtigung des Geschäftsbetriebs

Unternehmen mit großer digitaler Präsenz und ständig verfügbaren Online-Diensten haben große Angriffsflächen mit Tausenden potenzieller Schwachstellen.

Um ihre Abwehrmaßnahmen zu testen, müssen sie jedoch Wartungsfenster einplanen – was bedeutet, dass sie immer nur einen kleinen Prozentsatz ihrer DDoS-Angriffsfläche zu einem bestimmten Zeitpunkt testen können. Daher sind Unternehmen auf reaktive SLAs angewiesen, um auf die Auswirkungen von Ausfallzeiten durch DDoS-Angriffe zu reagieren.

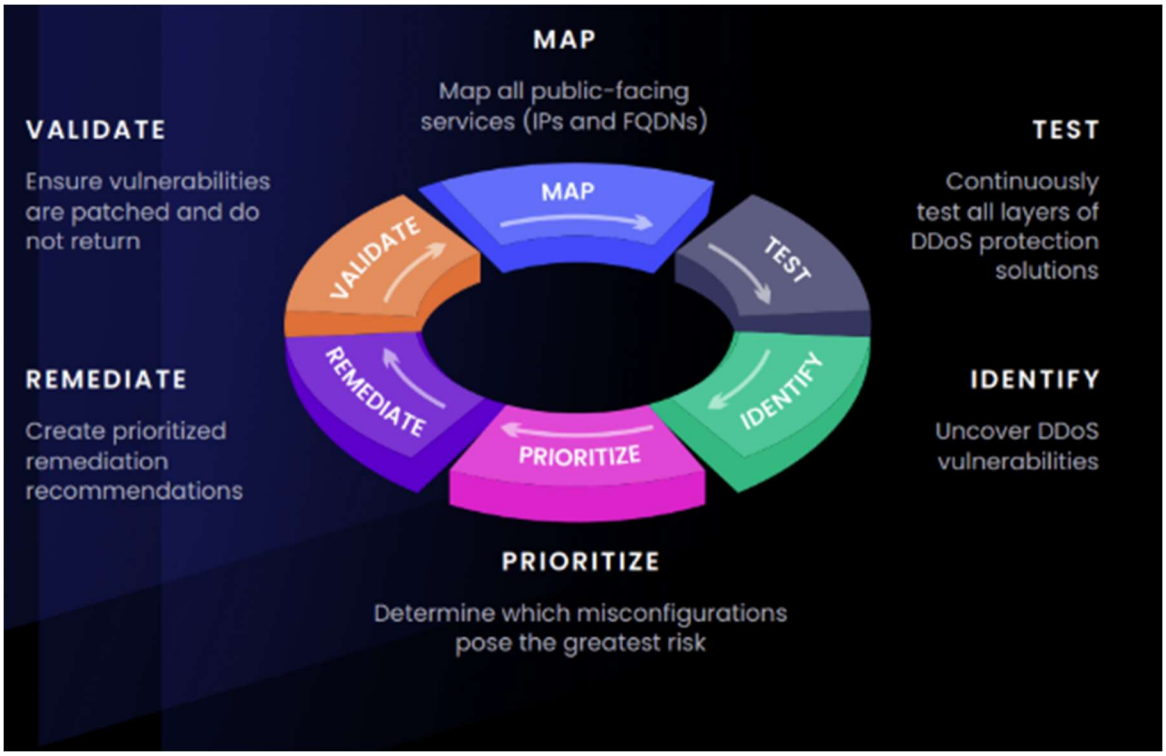
RADAR nutzt KI, um Angriffssimulationen zu priorisieren und Ihre DDoS-Abwehrmaßnahmen und -Konfigurationen kontinuierlich zu testen, ohne den normalen Geschäftsbetrieb zu stören. So können Sie kritische Schwachstellen identifizieren und beheben sowie Ihre DDoS-Abwehrmaßnahmen stärken und validieren – um schädliche Ausfallzeiten von vornherein zu verhindern.



So funktioniert RADAR™ von MazeBolt

RADAR validiert Ihre DDoS-Abwehrmaßnahmen, indem es kontinuierlich Tausende von DDoS-Angriffssimulationen durchführt, ohne Downtime oder Wartungsfenster.

Auf diese Weise kann RADAR menschliche und KI-gesteuerte Angriffsvektoren testen und validieren und so eine vollständige Abdeckung der DDoS-Angriffsfläche und ein proaktives Management Ihrer DDoS-Sicherheitslage gewährleisten. Und das alles, während Ihres Geschäftbetiebes.



Technologiepartner: [F5-Logo] und [Microsoft-Logo]

Über MazeBolt

RADAR™ von MazeBolt gewährleistet die Geschäftskontinuität für globale Unternehmen, indem es deren DDoS-Abwehrmaßnahmen validiert – ohne dass Wartungsfenster erforderlich sind. Die patentierte Technologie von RADAR führt kontinuierlich Tausende von unterbrechungsfreien Simulationen durch, sodass Unternehmen kritische Schwachstellen in ihren DDoS-Abwehrmaßnahmen und -Konfigurationen identifizieren und beheben können. Dies führt zu einer messbaren Verringerung des DDoS-Risikos und einer stärkeren Einhaltung gesetzlicher Vorschriften – und verhindert gleichzeitig operative, reputations und finanzielle Schäden, die durch DDoS-Angriffe verursacht werden.
Weitere Informationen finden Sie unter: www.mazebolt.com