ISSN 2644-237X
CIOREVIEW.COM

CIOReview

The Navigator for Enterprise Solutions

CYBER SECURITY EDITION

Awarded by
CIOReview

74470 91626 0

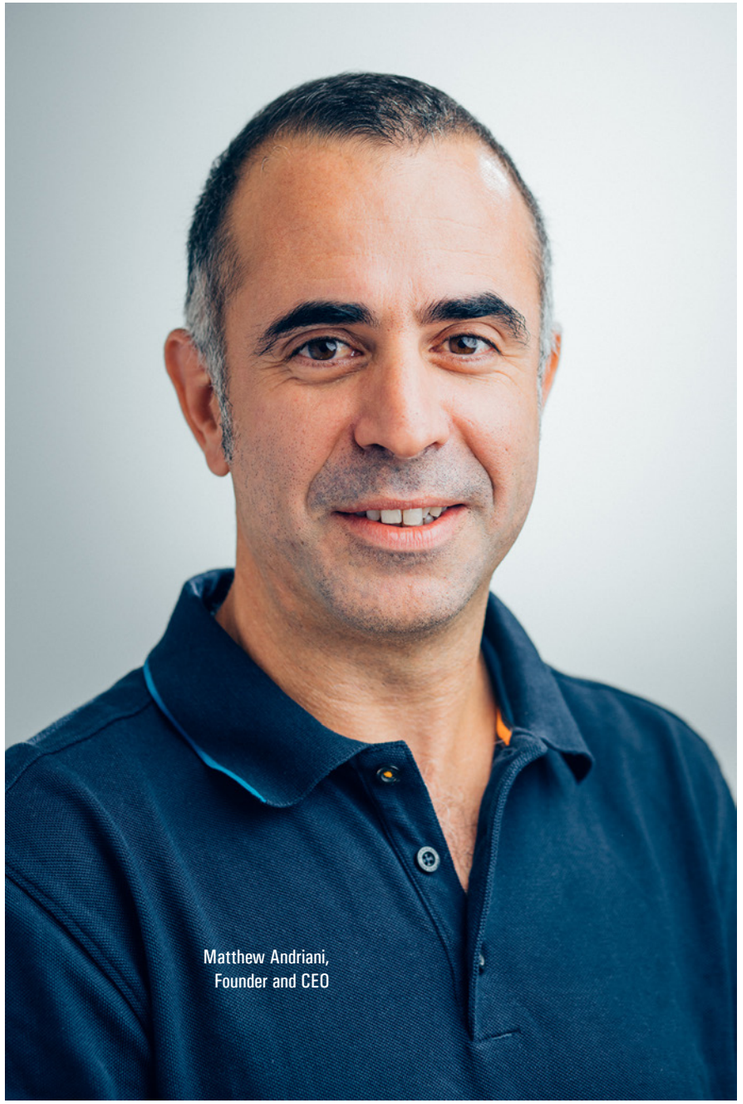
MazeBolt

Awarded by
CIOReview

The annual listing of 20 companies that are at the forefront of providing Cyber Security solutions and impacting the marketplace

MazeBolt

Ensuring Business Continuity in the Face of DDoS Threats



Business continuity represents one of the highest organizational priorities in the digital economy. When online services are driving the business around the clock, companies must ensure their architectures are resilient against attacks, including distributed denial of service (DDoS) attacks, which represent the most significant cyber threat to business continuity.

DDoS attacks can overwhelm a company's online services, making them inaccessible to users, disrupting operations, and potentially causing significant financial losses. Despite having DDoS protection in place, organizations can still face up to 75 percent exposure of their online services due to misconfigurations which cause un-seen vulnerabilities in their defenses.

MazeBolt presents the only reliable way to avoid a DDoS attack with its never seen before non-disruptive DDoS testing solution—RADAR—that identifies DDoS vulnerabilities and provides precise guidance for their remediation.

"Our solution is designed to complement all existing DDoS protection solutions, enhancing its efficacy significantly. While typical automated protection solutions operate at around 60 percent efficacy, integrating RADAR boosts this figure to over 98 percent," says Matthew Andriani, founder and CEO of MazeBolt.

RADAR conducts continuous DDoS testing on targets, identifying as-yet unknown vulnerabilities. This allows clients to validate and remediate these vulnerabilities, ensuring a more comprehensive and proactive DDoS defense strategy. By providing a non-intrusive simulation solution, RADAR empowers businesses reliant on 24/7 online presence to strengthen their critical business continuity and adopt a preventative, proactive, and automated approach to DDoS security.

HOW CAN RADAR AUGMENT YOUR DDOS DEFENSE STRATEGY?

RADAR addresses a fundamental challenge in DDoS protection by shifting from a 'deploy and trust' philosophy to proactive vulnerability identification and remediation. Organizations traditionally lacked the means to continuously validate the effectiveness of their DDoS protections until RADAR, these vulnerabilities are the only way DDoS attacks still succeed.

"We give our clients a non-intrusive, continuous DDoS testing solution that allows them to identify and remediate all vulnerabilities before the attack occurs," says Howard Silverman, VP of marketing at MazeBolt.

They can easily identify vulnerabilities in their DDoS protection, preventing potential damaging attacks. The continuous validation of protections ensures a proactive, preventative mindset rather than a reactive one that depends on provider SLAs to recover after the breach has occurred.

> **We dramatically reduce the DDoS attack surface for our customers to completely prevent a damaging attack, with a non-intrusive, non-disruptive DDoS testing solution that allows clients to ensure that all vulnerabilities are identified and eliminated before an attack**

MazeBolt's recent strategic partnership with F5, a major player in the cybersecurity market, greatly expedites the remediation process. As a preferred remediation vendor, F5 aligns internal procedures to close vulnerabilities promptly, significantly enhancing the overall effectiveness of DDoS defenses. This greatly minimizes the time it takes to close vulnerabilities, and eliminates the risk of damaging downtime.

HOW IS RADAR DIFFERENT FROM TRADITIONAL DDOS TESTING SOLUTIONS?

RADAR is a patented solution that distinguishes itself from traditional DDoS testing solutions through several key features, addressing limitations in coverage, maintenance requirements, and downtime:

Complete Coverage and Continuous Testing: While traditional testing covers a minute fraction of the attack surface periodically, RADAR continuously validates 100 percent of the attack surface in real-time, ensuring comprehensive protection, using thousands of non-disruptive attack simulations to do so.

Elimination of Downtime: Unlike solutions that demand maintenance windows and disrupt online operations, RADAR operates seamlessly without interruptions, allowing businesses to validate DDoS protections without disrupting their services.

Proactive Vulnerability Mitigation: While traditional approaches focus on human response testing after the damage has already occurred, RADAR proactively eliminates vulnerabilities, going beyond procedural checks to actively mitigate weaknesses, and enhancing overall protection.

RADAR's innovative features represent a significant shift, offering a fully automated, continuous, and non-disruptive solution to completely prevent a damaging DDoS attack.

STRENGTHENING THE WALLS OF CYBERSECURITY AND PROTECTING BUSINESS REPUTATION

The effectiveness of RADAR can be seen in a recent deployment of the product MazeBolt undertook for a leading European bank with over 4 million customers and €1.5 billion in annual revenue. Despite investments in the best multi-layered DDoS mitigation infrastructure, the bank suffered repeated attacks that disrupted their services, attackers were able to do this by continuously exploiting undiscovered vulnerabilities in the DDoS defenses deployed.

Each incident resulted in revenue losses, inflated cyber insurance costs and reputational damage. The bank then turned to MazeBolt's RADAR solution for an initial proof-of-concept engagement.

RADAR's non-intrusive testing uncovered over 1,500 DDoS vulnerabilities that could result in future attacks. The bank had only 43 percent protection automated DDoS defenses with severe gaps that put core banking applications and infrastructure at risk.

By adopting RADAR's preventative approach, the bank now reduced its vulnerability exposure from 57 to under 5 percent. The European bank has withstood subsequent DDoS events without any service disruption.

For organizations where an 'always-on' paradigm is non-negotiable, MazeBolt is arming businesses with insights to preempt outages, architect resilience, and enable continuity. As attacks grow in complexity and frequency, the costs of outages will continue to rise exponentially in terms of lost revenue, customer churn, and damaged reputation. RADAR offers a way for companies to get ahead of this threat. By pre-emptively finding and fixing vulnerabilities, businesses can confidently keep mission-critical applications running 24/7 in the face of all known DDoS threats. CR