HADRIAN

The perimeter didn’t disappear

EXTRACT OF HADRIAN’S OFFENSIVE SECURITY BENCHMARK REPORT

INTRODUCTION

Internet-facing systems are continuously scanned, probed, and tested for weakness, often before vulnerabilities are formally disclosed. Foundational infrastructure like DNS continues to account for a significant share of verified external exposure, while testing frequency varies widely across organizations. More visibility has not resolved this imbalance. In fact, 99.5% of vulnerability scanner findings do not represent real-world risk, consuming security time without improving certainty.

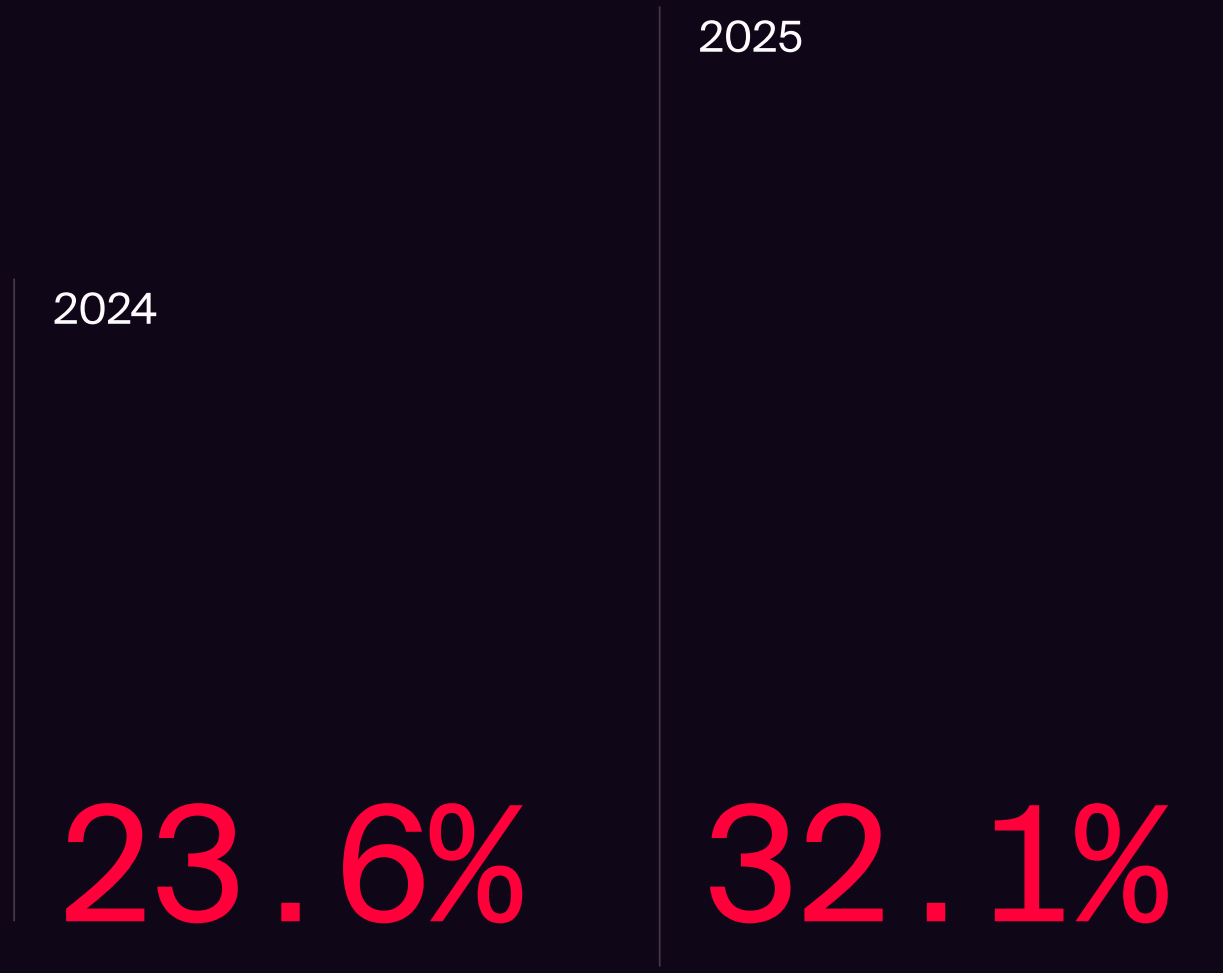
This report extract examines that structural gap, how exploitation timelines have shifted, where exposure concentrates, and why validation must align to attacker speed rather than calendar-driven schedules.

Exploitation before awareness

Exploitation now frequently precedes disclosure. In 2025, 32.1% of Known Exploited Vulnerabilities showed evidence of active exploitation on or before the day the CVE was issued, up from 23.6% in 2024. For a growing share of edge vulnerabilities, public disclosure no longer marks the beginning of risk, it reflects activity that is already underway.

This shift is driven primarily by internet-facing technologies such as VPNs, firewalls, and gateways, which are continuously scanned and attacked at scale. As organizations expand their external footprints and connect critical systems to the edge, the window between exposure and exploitation continues to shrink.

For security teams, this changes the role of disclosure itself. CVE publication is increasingly a lagging indicator rather than an early warning signal. When exploitation begins before formal reporting, reactive workflows anchored to advisories and patch cycles are structurally delayed. The challenge is no longer just remediation speed, but validation speed, understanding what is exposed and exploitable before attackers do.



VULNERABILITIES WITH ACTIVE EXPLOITATION OBSERVED BEFORE KEV CATALOG INCLUSION

— Vulncheck

Not just zero-day vulnerabilities

It is not only zero-day vulnerabilities that organizations need to be concerned about. One of the oldest and most fundamental pillars of the internet, DNS, continues to represent the single largest category of verified external risk. Across more than 300 organizations analyzed, DNS accounts for 23% of all verified findings, comparable to last year's 26%. No other single category contributes a larger share of confirmed external exposure.

This concentration reflects how modern infrastructure is built. Multi-cloud adoption, third-party SaaS dependencies, and the frequent provisioning and decommissioning of internet-facing assets all rely heavily on DNS. Records are created, modified, and deprecated continuously, often without centralized oversight or consistent validation.

Threat actors have recognized this structural weakness. DNS misconfigurations, dangling records, and misaligned routing create predictable footholds at the perimeter. Research by the Global Cyber Alliance (GCA) found that securing DNS servers can prevent more than 33% of cybersecurity data breaches from occurring.

For most organizations, DNS also represents one of the fastest opportunities for measurable risk reduction. When identified and correctly triaged, DNS issues are typically straightforward to remediate and have recorded the lowest median remediation time observed by Hadrian for two consecutive years.

The percentage of data breaches can be prevented by securing DNS servers

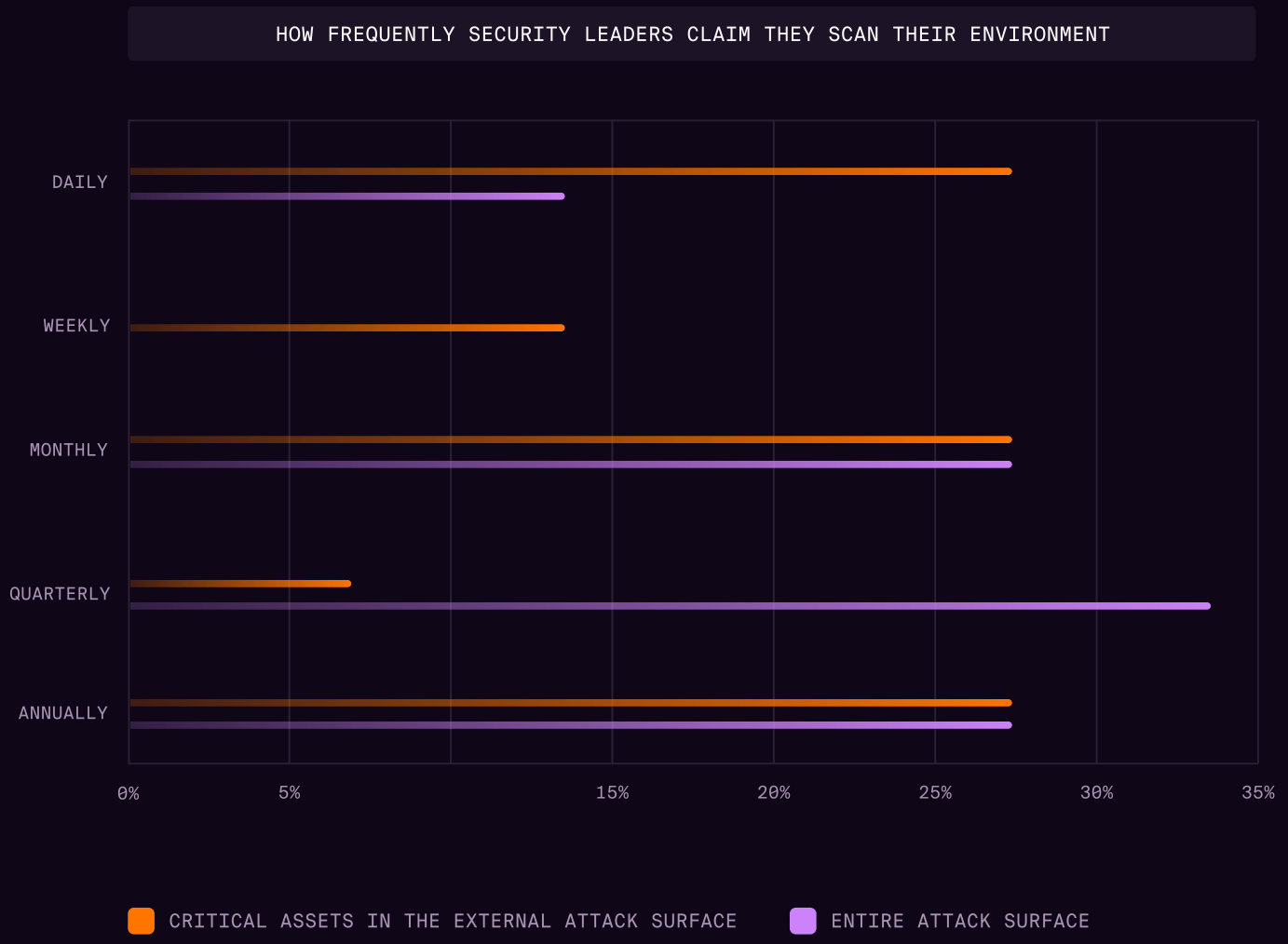
33%

Validation on a schedule

Despite accelerating exploitation and persistent infrastructure exposure, testing frequency varies widely across organizations, even for critical assets. Twenty seven percent test critical assets daily, while an equal percentage test them annually. Monthly testing accounts for another 27%, with weekly and quarterly testing representing smaller segments. This variation reflects inconsistent definitions of acceptable risk rather than intentional strategy.

Most organizations continue to validate their environments on schedules driven by resource constraints, compliance cycles, or internal processes. As a result, long windows of unvalidated exposure remain common across external attack surfaces.

When exploitation can begin before disclosure, and foundational systems like DNS account for nearly a quarter of verified findings, periodic testing creates structural blind spots. The challenge is no longer whether testing occurs, but whether it aligns with the pace of infrastructure change or adversary activity.



RECOMMENDATION

The data shows that exploitation is accelerating at the perimeter while validation remains periodic and inconsistent. Vulnerabilities are abused before disclosure, DNS continues to concentrate verified exposure, and testing frequency varies widely across organizations. In this environment, schedule-driven security increases uncertainty rather than reducing it.

Teams should shift toward continuous, attacker-aligned validation. This means verifying real-world exploitability at the edge, continuously assessing structural exposures like DNS, and prioritizing remediation based on what can be exercised in practice, not what appears in a scanner report. Exposure management must operate at adversary tempo, not calendar pace.

This extract highlights one dimension of that gap. The full Offensive Security Benchmark Report details how continuous verification reduces perimeter risk and what programs must change to keep pace with modern exploitation.

Get the full report

ABOUT HADRIAN

Hadrian is an offensive security platform built for teams that need proof, not predictions. We reveal exactly how an adversary could break in today by executing real attacker techniques against your external attack surface. By validating exploitability in production-safe ways, Hadrian eliminates false urgency, sharpens prioritization, and gives teams confidence to act.

Deployed in minutes and engineered for scale, Hadrian seamlessly fits into existing security workflows. Security leaders use Hadrian to move from periodic testing to continuous, evidence-backed exposure reduction.

RECOGNISED BY LEADING ANALYSTS

Gartner GIGAOM

FROST & SULLIVAN

TRUSTED BY MARKET LEADERS

NBC · amadeus · McKESSON · BLINQX · CRÉDIT AGRICOLE · SHV ENERGY · ABN·AMRO · London Business School · RITUALS... · SIEMENS energy · LOTTOMATICA · LEROY MERLIN · WeatherTech · BIOLANDES · BLINQX · DAMEN · =EXACT · nedap