SIXMAP

RESEARCH REPORT · JUNE 2026

# Enterprise **Attack Surface** Report 2026

Patterns in vulnerability distribution across 100 enterprise organizations whose internet-facing attack surfaces SixMap has fully assessed.

# Table of **Contents**

EXECUTIVE SUMMARY

# Most assets are well-managed. **A tiny minority carries virtually all the risk.**

Across 100 enterprise organizations whose internet-facing attack surfaces SixMap has fully assessed, the data tells a consistent story: the broad perimeter is healthier than headline narratives suggest, but a small, categorically different cohort of hosts concentrates the danger.

1.5% of internet-facing hosts carry **99% of the vulnerabilities.** CVE density on these hosts runs roughly **270×** higher than on the average service exposure.

| 99.63% | 36 | 78% | ~34% |
|---|---|---|---|
| of service exposures have zero known CVEs | mean CVEs per vulnerable host (median 23) | of organizations have a host with 10+ known CVEs | of observed CVEs are 5+ years old & exploitable |

## THE CLEAREST PRIORITY

**Asset visibility.** The most dramatic reduction in external cyber risk comes from simply improving the security team's understanding of internet-facing assets. Closing the gap between what organizations think they own and what they protect pays exponential dividends. The data shows the vast majority of assets are well-protected, while a small percentage are extremely vulnerable — a strong signal that those assets are not known to the security team, and therefore not managed or protected at all.

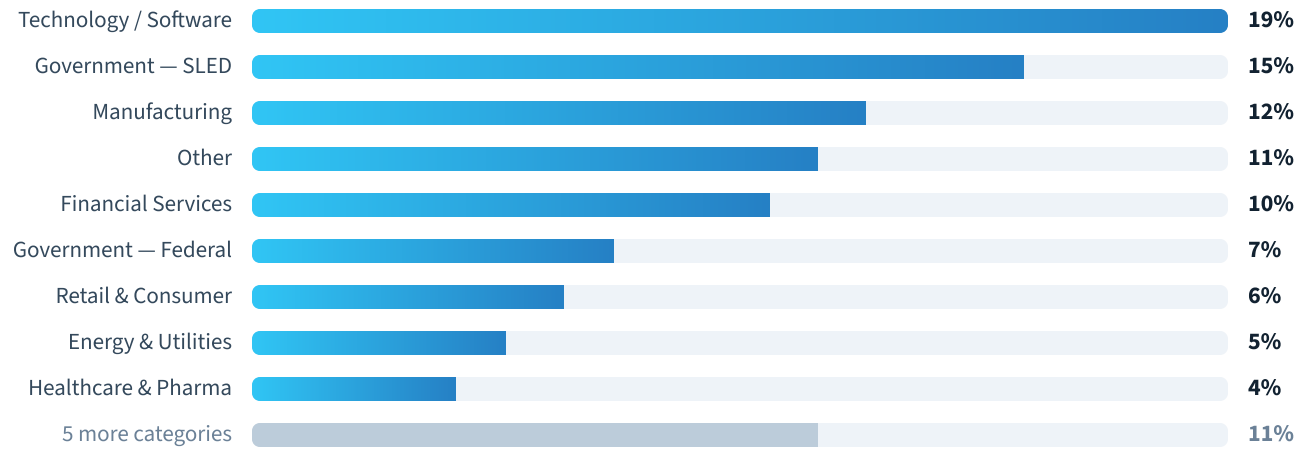
ABOUT THE DATASET

# 100 organizations across industries, **thoroughly assessed**

Each organization's internet-facing attack surface was fully assessed at least three times. Selected to resemble a representative sample of enterprises by industry and size, the sample is overwhelmingly North American — 84 of 100 organizations are headquartered in North America, with the United States alone accounting for 79%. This report does not name or comment on the security posture of any specific organization.

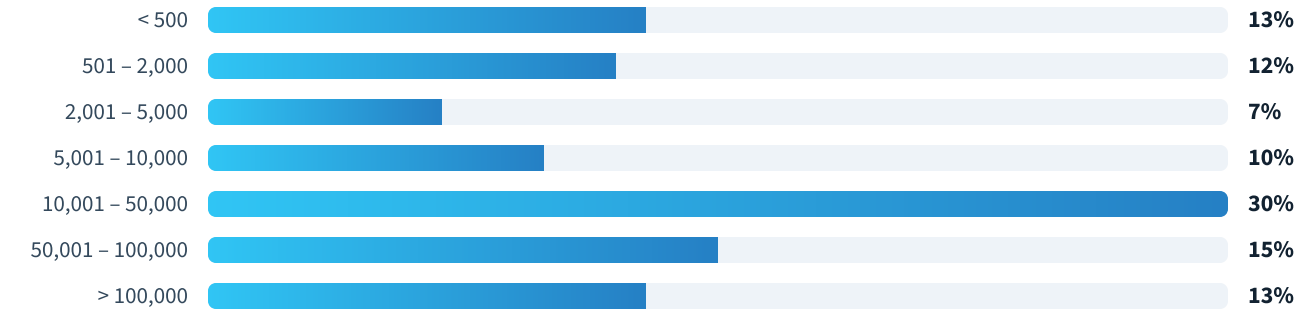
## By industry

% of the 100-organization sample · 14 categories




## By organization size

% of organizations, by employee count



THE SIZE OF THE ATTACK SURFACE

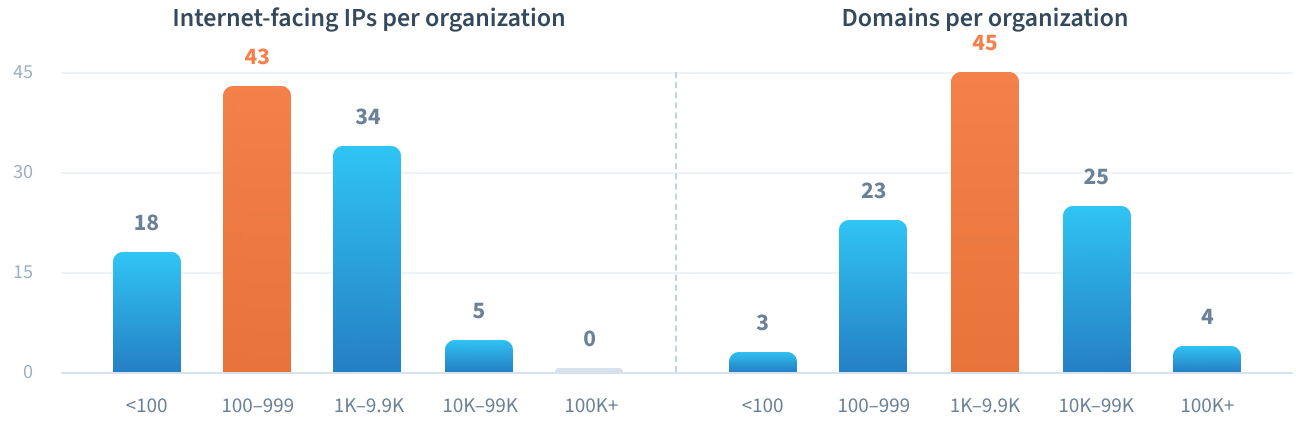
# A heavily skewed distribution, **dominated by outliers**

| 175,648 | 997,640 | 1,960,591 |
|---|---|---|
| internet-facing IP addresses | service exposures | distinct domains |

The median organization has **547 internet-facing IPs** and **3,486 domains**. The mean — pulled up by the very-large outliers — runs to 2,280 IPs and 20,383 domains. The report presents per-organization rates throughout to keep the framing comparable across the size range.

### Attack surface size distribution

Number of organizations per range. Median: 547 IPs and 3,486 domains per organization.




The sample is mixed in terms of size, but it is a representative slice of organizations — both public and private — that could plausibly be targeted by cyber threat actors. As a group, these organizations sit at a somewhat heightened level of risk relative to the universe of organizations globally.

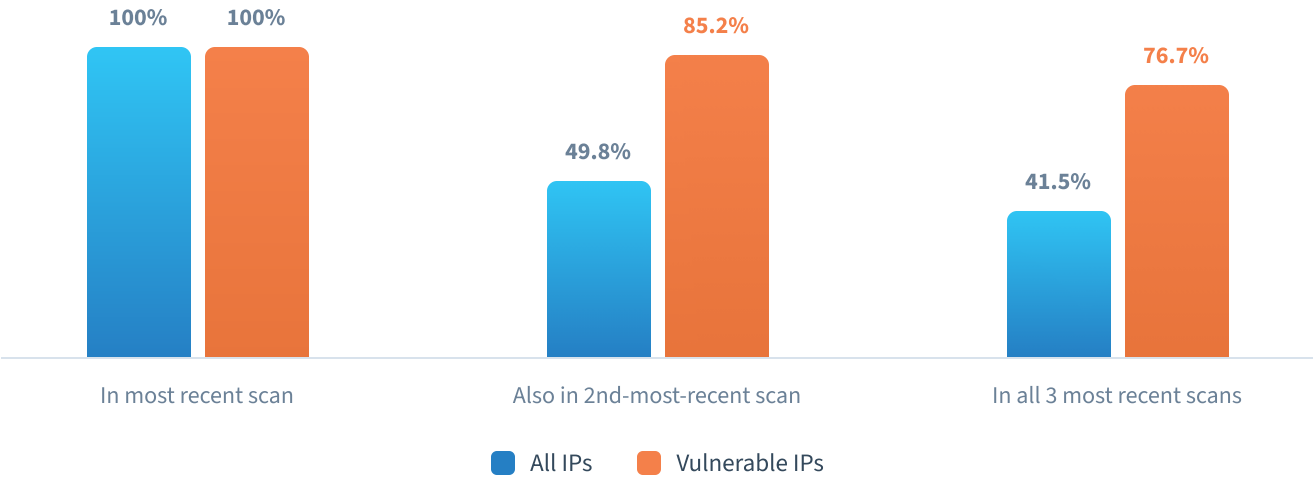
STATIC AND DYNAMIC IP ADDRESSES

# Vulnerable IPs are **dramatically more persistent**

SixMap compared each organization's most recent scan against its two prior scans. Of all IPs in the latest scan, roughly half (49.8%) were also in the prior scan, and 41.5% appeared in all three — a reasonable rate for large enterprises actively cycling cloud infrastructure.

### Persistence across the 3 most recent scans

Vulnerable IPs are roughly 1.8× more persistent than the typical IP. Most do not come and go.




**85.2%** of vulnerable IPs were still vulnerable in the prior scan and **76.7%** in every one of the three most recent scans. The IPs carrying the bulk of the risk are persistent, long-standing infrastructure — the signature of assets nobody is actively managing.

Enterprises run heavily on the cloud, so the attack surface is dynamic — roughly half of all IP addresses turn over from one week to the next. Yet the cloud-resident IPs appear relatively clean. It is the persistent IPs — the static ones that reappear scan after scan — that carry the most vulnerabilities and the greatest risk.

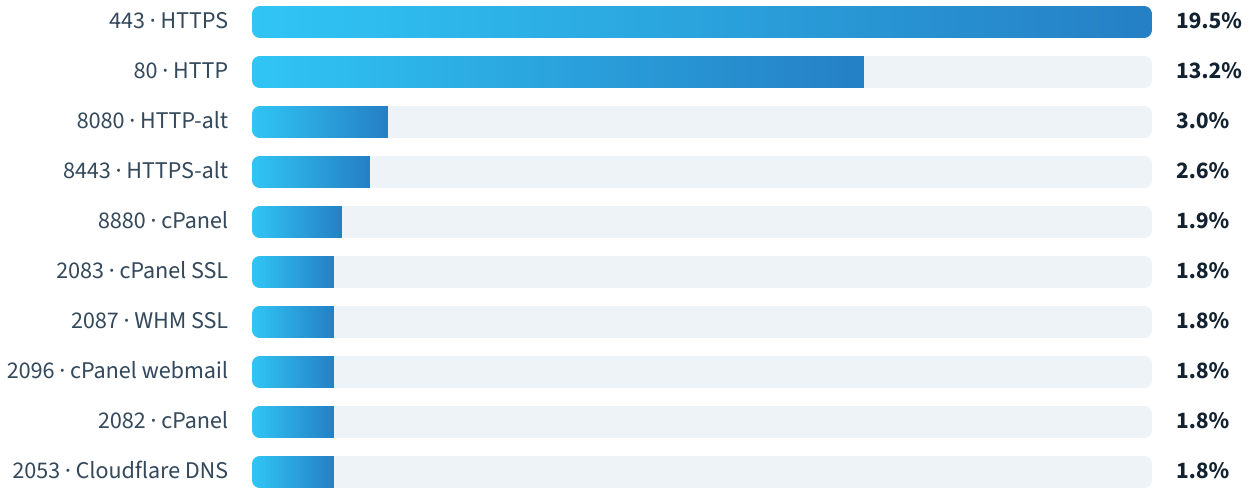
ASSESSING EXPOSURES: PORTS

# Half of all exposure listens **outside the standard playbook**

An **exposure** is a single service on a single port on a single IP — what an attacker actually sees. The median IP has 2 open ports; the 90th-percentile IP has 13; the most-exposed has 197. Across all organizations, 15,992 unique port numbers were observed open.

### Top 10 ports by exposure count

HTTP + HTTPS (standard and alternative ports) account for roughly 38% of all observed port exposures.




| 15,992 | 97.7% | 50.8% | 197 |
|---|---|---|---|
| unique port numbers observed open | of unique open ports are above 1024 | of all instances of open ports are above 1024 | max open ports observed on a single IP |

ASSESSING EXPOSURES: SERVICES

# Web dominates — and over half is **intentionally obscured**

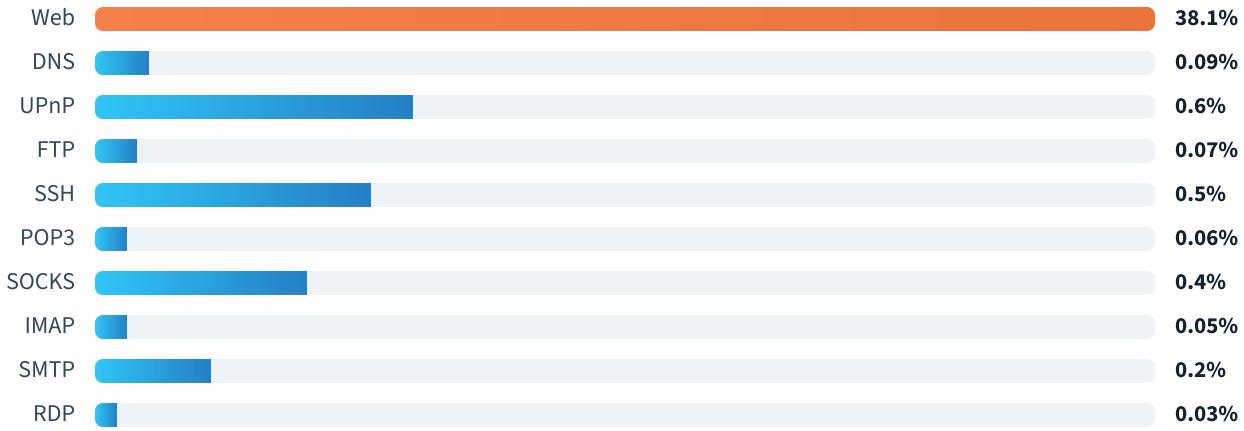
Beyond ports, SixMap fingerprints the service running behind each open port — the actual software an attacker would interact with. Across nearly a million service exposures, the profile is striking: web services dominate everything that can be identified, while the majority of exposures reveal nothing about themselves at all.


| | |
|---|---|
| Web (HTTP + HTTPS) | **38.1%** |
| Other identified services | **7.4%** |
| Unidentifiable (intentionally obscured) | **54.5%** |

Roughly 55% of exposures respond to scans without advertising what they are — typically firewalls or reverse proxies. These services are intentionally obscured and not identifiable without active techniques that would require permission from the target organization.

### Top 10 identified services by exposure count

Web services dominate the identified profile. All other services combined account for under 2% of observed exposures.



THE BROAD SURFACE IS HEALTHY

# The first finding is **reassuring**

**99.63%**

of service exposures have **zero known CVEs**

**98.46%**

of internet-facing IPs have **no detected vulnerabilities**

The data does not support a “the perimeter is extremely insecure” narrative. The assets organizations actively manage are, by and large, well-protected — the product of continuous patching, hardening of exposed services, and the operational discipline to keep millions of services running cleanly across the globe.

Across the 100 organizations, that proportion holds with remarkable consistency — independent of industry, size, or geography. The well-managed perimeter is the rule, not the exception.

The interesting question is what makes the remaining **1.54%** different — and what implications that small population carries.

VULNERABLE HOSTS ARE EXTREMELY HIGH-RISK

# Not a cleaner version of the rest — **categorically different**

The 1.5% of hosts that carry any vulnerability are not a slightly-worse version of the healthy majority — they are categorically different. On these hosts, CVEs cluster densely, and the same concentration recurs across nearly every organization in the sample.

### CVE density: single random service vs. single vulnerable service

Mean CVEs per service exposure, comparing the average across all exposed services to the average across all exposed services that are known to have at least 1 published CVE. The vulnerable cohort runs roughly 270 times higher.

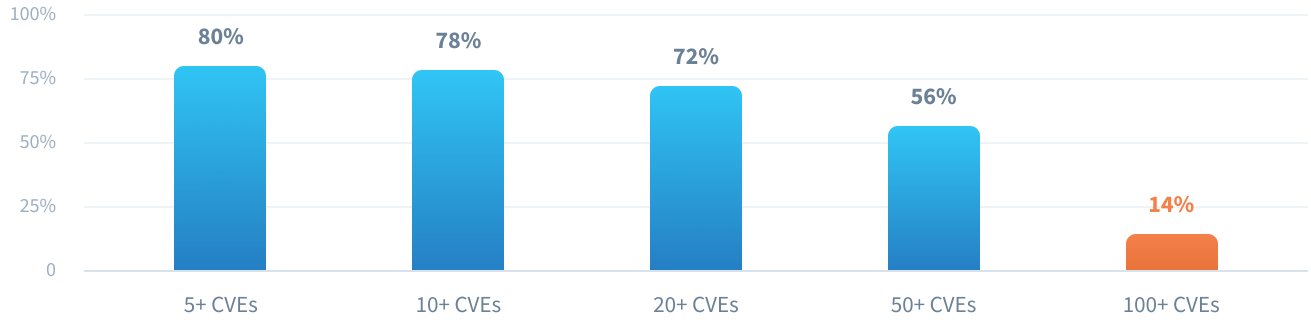
| | |
|---|---|
| Average service exposure | **0.15 CVEs per service across all services** |
| **Average vulnerable service** | **39.68 CVEs per service across vulnerable services** |

**272× difference in CVE density**

| | | | |
|---|---|---|---|
| 23 | 36.0 | 277 | 1.54% |
| median CVEs / vulnerable host | mean CVEs / vulnerable host | CVEs on the worst host | of IPs are vulnerable (2,711) |

### Organizations with at least one host carrying many CVEs

Four out of five organizations have a host with five or more CVEs. The split is bimodal — no populated middle.



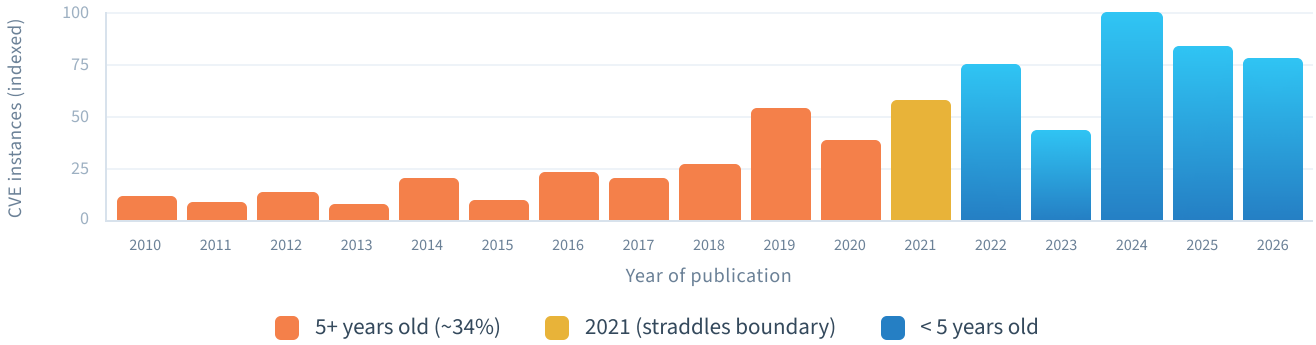
ALL TOO COMMON: OLD, EXPLOITABLE CVES

# Old vulnerabilities, with a **high probability of exploitation**

Age and exploitability are where the vulnerable cohort turns dangerous. The CVEs concentrated on these hosts are rarely fresh zero-days. Rather, a large share of the CVEs detected are known, often have publicly available exploit code, and in some cases are known to be exploited in the wild.

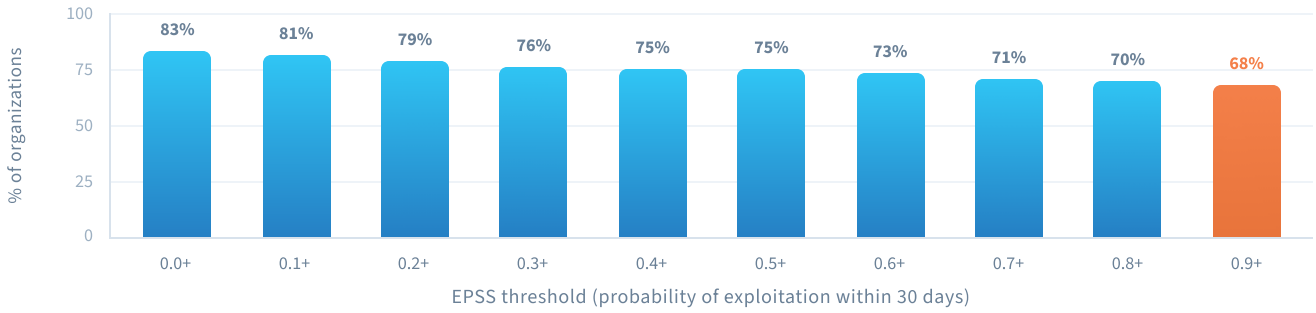
### Age distribution of observed CVE instances

Indexed volume of CVE instances by publication year (peak year = 100). Roughly a third were published five or more years ago (2020 and earlier, shown in orange).




### Organizations with a CVE above each EPSS threshold

Share of organizations with at least one CVE above each EPSS exploitation-likelihood threshold. About two-thirds carry one rated very high.




**68%** of organizations have a host with at least one CVE with an EPSS score of 0.90 or higher, indicating a very high likelihood of exploitation within 30 days. **63%** have a CISA KEV-listed CVE, already actively exploited in the wild.

IMPLICATION: SHADOW IT REMAINS A CHALLENGE

# The shape of a population that is **not being managed**

Small in proportion, unusually concentrated, distributed across nearly every organization, and dominated by old vulnerabilities with a disproportionately high probability of exploitation. Concrete fingerprints recur throughout the dataset:

| | |
|---|---|
| **Apache HTTP Server — CVE-2024-38475 (KEV)** — path traversal → RCE | **849 IPs** 57 organizations |
| **Apache HTTP Server — CVE-2021-40438 (KEV)** — SSRF, patched 5 years ago | **736 IPs** 55 organizations |
| **Microsoft Exchange — ProxyShell cluster (KEV)** — 5 CVEs, 2018–2021, exploited at scale | **11 IPs** 6 orgs, full bundle |
| **OpenBSD OpenSSH 4.x / 5.x** — legacy product released 15–20 years ago | **55 CVEs** on one OpenSSH 4.3 host |
| **Telnet on port 23** — plaintext credentials over the public internet | **3,128 IPs** 26 organizations (~1 in 4) |
| **Oracle Sun ONE Web Server** — end-of-life; vendor defunct since 2010 | **EOL** still internet-facing |

> The ASM category promised to close exactly this gap — then most providers were acquired and folded into broader suites. The problem was addressed at the marketing level. **What remains is the problem itself**, now at the scale this report documents.

CASE STUDY · FORTUNE GLOBAL 500 PHARMA

# An exceptionally healthy surface — **and 7 deeply broken hosts**

A European-headquartered Fortune Global 500 pharmaceutical company, ~70,000 employees, operations across 100+ countries. Only 7 of its 2,353 internet-facing IPs (0.30%) carry any CVE — roughly 5× cleaner than the dataset average. But those 7 are exactly the shape this report describes.

| 2,353 | 9,557 | 23,201 | 343 |
|---|---|---|---|
| internet-facing IPs | service exposures | distinct domains | unique ports observed |

| 235 | 133 | 5 | 2 |
|---|---|---|---|
| CVE instances on 7 hosts | distinct CVEs | CVEs at EPSS ≥ 0.9 | CISA KEV-listed CVEs |

**The 7 vulnerable hosts**

| Host | Software detected | CVEs |
|---|---|---|
| Host A | OpenSSH 4.3 (released 2006) | **55** |
| Host B | OpenSSH 5.3 (released 2009) | **43** |
| Host C | Apache HTTP Server 2.4.58 | **35** |
| Host D | Apache HTTP Server 2.4.x | **33** |
| Host E | Apache HTTP Server 2.4.x | **33** |
| Host F | Apache Tomcat 9.0.113 | **16** |
| Host G | Sun ONE Web Server 6.1 (defunct 2010) | **4** |

If a 70,000-person Fortune Global 500 enterprise with mature security investment still runs OpenSSH from 2006 and a web server from a vendor defunct 15 years ago, this pattern almost certainly repeats across most large enterprises. These are not slow-patched assets — they are assets nobody appears to know are still owned.

FOCUS ON THE FUNDAMENTALS

# In an AI era, **double down on the basics**

Speeding patch velocity on already-clean hosts does not move the needle when 98% already have no detected vulnerabilities. The breach starts on infrastructure that was never in the management plane to begin with. Four capabilities matter most:

### Complete, up-to-date asset inventories

Ongoing identification of what an organization actually owns and exposes — including infrastructure from acquisitions, line-of-business deployments, and cloud accounts outside central IT.

### Continuous monitoring & exposure assessment

Ongoing analysis of how each asset is configured: which ports it presents, which services it runs, which software versions are exposed, and how posture changes over time.

### Fast, accurate detection & response

Surfacing meaningful risk signals — active exploitation, new KEV additions, EPSS changes — within hours of disclosure, routed to the team that owns the affected asset.

### An agile vulnerability management function

A practice that takes action on prioritized findings within compressed timeframes — measured in hours and days, not weeks and quarters.

> Asset inventory is **foundational** among the four. Without it, every subsequent capability runs against an incomplete view of what an organization actually owns.

OVERVIEW OF THE SIXMAP SOLUTION

# Continuous attack surface monitoring, **built around the four**

SixMap discovers external assets, assesses their exposure, and detects risk in priority order — operating continuously rather than at point-in-time intervals.

MAP · DISCOVER

### Continuous External Discovery

Identifies the internet-facing assets an organization owns — including infrastructure absent from internal inventories — at scale across the full IPv4 and IPv6 space. Every asset carries documented attribution evidence.

ASSESS

### Continuous Exposure Assessment

Fingerprints what is running on each asset: which ports are open, which services and software versions are exposed, and how posture changes over time. The same logic that built this report runs continuously against every customer's surface.

PRIORITIZE

### Continuous Risk Detection

Surfaces the exposures that matter most by combining CVE severity, EPSS scoring, CISA KEV tagging, and threat-actor association — routing the signal immediately to the team that owns the affected asset.

ACT

### Accelerated Mitigation & Remediation

Because customers already know what they own, who is responsible, and where each threat applies, teams move directly to action. Risk mitigation shifts from a multi-week investigation to a same-day response.

Talk to SixMap about finding the vulnerable hosts that have fallen out of sight on your perimeter — and preparing your security program for a world in which threat actors wield the most powerful AI tools available.

ABOUT SIXMAP

# Know thyself. **Preemptively reduce risk.**

SixMap delivers the most complete and accurate external view of any public or private organization, showing security teams who they are, what they own, and what they must protect. By closing the gap between what security teams monitor and what adversaries find through reconnaissance, SixMap helps customers mitigate risks before attacks occur. Born out of national defense and deployed to protect some of the nation's most sensitive networks, SixMap now brings military-grade capabilities to public and private organizations to preemptively stop cyberattacks.

BOOK A DEMO

SixMap Research · June 2026

6731 Columbia Gateway Dr, Suite 100, Columbia, MD 21046 · sixmap.io

SIXMAP