csurface

ANNUAL REPORT · CYBER EXPOSURE

State of Digital Exposure

2026 Edition — How the attack surface grows, how the threat accelerates, and why the distance between the two is the real risk. Aggregated and anonymous data from dozens of organizations.

ORGANIZATIONS IN THE BASE **68 + 16 detailed**	EXTERNAL ASSETS MAPPED **122 thousand**	PERIOD **2026**
CLASSIFICATION **Public**	EDITION **1st — Annual**	SOURCE **CSURFACE Platform**

EXECUTIVE SUMMARY

The reading in three parts

What the data in this report says — and the single conclusion toward which it converges.

2026 Edition
CSURFACE

OPERATE ACROSS 2+ CLOUDS

75%

surface dispersed across multiple providers

PUBLIC EXPLOIT AFTER THE FLAW

5 days

average time until attack code exists

VULNERABILITY FOR 5+ YEARS

68%

of the organizations analyzed

This report brings together, in an **aggregated and anonymous** form, what CSURFACE observed while mapping the external attack surface of dozens of organizations — 68 with discovery completed on the platform and 16 submitted to detailed analysis. No company is identified.

First: the surface grows ungoverned. It is not an organized inventory — it spreads across several clouds, across environments provisioned in haste and rarely shut down, across third-party components embedded in every application. Three in four organizations operate assets in two or more clouds; half, in three or more. And what comes in is almost never maintained: 68% carry a vulnerability that has been open for more than five years.

Second: the threat accelerates. A working public exploit appears, on average, five days after a flaw is disclosed; active exploitation, at ninety. The most exploited flaw classes are, for the most part, web application flaws — precisely the layer that 71% of the applications analyzed leave without a WAF.

Third: the risk lives in the distance between the two curves. The defense adds and forgets assets on a scale of years. The attacker weaponizes exploits on a scale of days. The incident is the predictable intersection of these two speeds on the same ungoverned asset — an occurrence of a structural nature, statistically expected wherever the defense falls behind the threat.

The conclusion of this report. Neither of the two curves resolves on its own. Discovering everything without prioritizing overloads the team; prioritizing threats without seeing the entire surface protects only what was already known. Reducing risk requires **continuous discovery of the surface** and **threat intelligence** operating together, without interruption.

Data base

Organizations with discovery completed	**68**
Detailed surface analyses	**16**
Sectors represented	**11**
External assets mapped	**122,095**
Vulnerabilities analyzed	**2,361**
Emerging threats monitored	**2,954**

Sectors of the detailed analyses: automotive, education, government, industry, logistics, professional association, social security, healthcare, services, technology and retail.

All analysis is external and passive. Anonymized data; no organization is identified.

PART 01

The surface grows — and it grows ungoverned

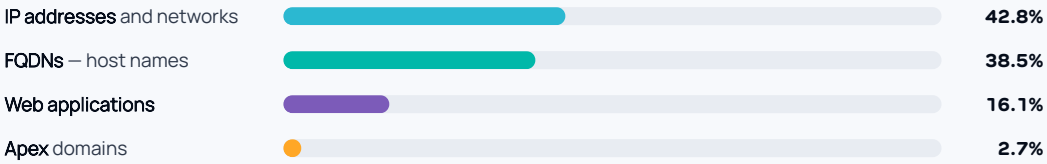
What the external attack surface is made of and why it expands faster than any inventory.

EXTERNAL ASSETS
122 thousand
across 68 organizations

RELATED ORGANIZATIONS
1,068
discovered by the platform

THIRD-PARTY COMPONENTS
2.8×
per exposed owned asset

Distribution of external assets by type



Cloud providers per organization

Analysis

The external attack surface is not an organized inventory. It accumulates. Each product team publishes an application, each business area contracts a SaaS, each acquisition brings the infrastructure inherited from another company — and almost none of it is removed afterward.

The most revealing data point is the cloud one: **three in four organizations** distribute assets across two or more providers, and half across three or more. Each environment adds its own console, its own configuration standard and its own management boundary. Treated in **isolated silos**, with distinct tools, standards and teams per provider, these environments produce partial views that rarely reconcile: the real surface exists fragmented across multiple consoles, and none of the partial views represents the whole.

Third-party dependence amplifies the effect: each exposed web application carries multiple components from the supplier chain — scripts, CDNs and libraries embedded in the code that expand the surface without appearing in any inventory.

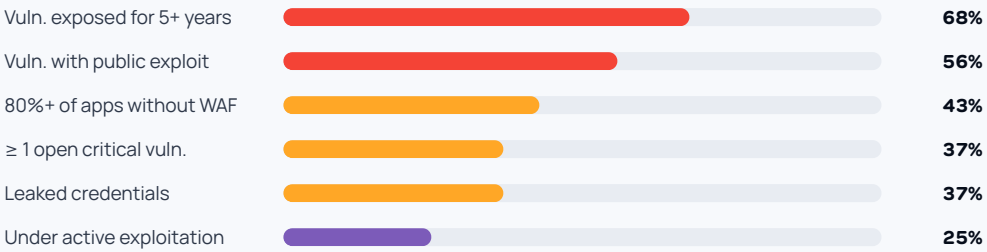
Why this matters. Inventory is the foundation of every security program. Without knowing what exists, every prioritization, every test and every response operates on an incomplete base — and what was left out remains exposed.

PART 02

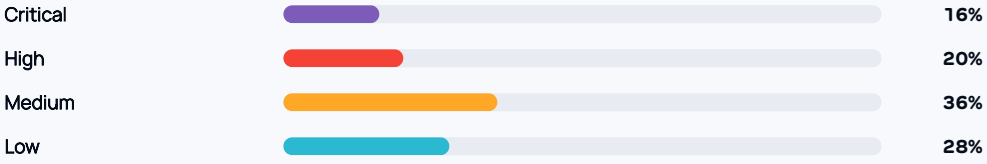
What the surface accumulates

The findings that repeat from company to company — and are almost always old.

Frequency of findings — % of companies analyzed



Distribution of the 2,361 vulnerabilities by severity



Severity is not priority

EXPLOITATION INDICATOR	REPRESENTATIVENESS
With public exploit available	**5.7%** of vulns
Demonstrably exploited	**1.8%** of vulns
Truly priority set	**7.5%** of vulns

Of the 2,361 vulnerabilities, only a fraction has demonstrated exploitation — and it is on that fraction that an attacker begins.

Exposure time is the problem. In 68% of the organizations there is a vulnerability that has been open for more than five years; the oldest one recorded exceeded a decade. The average age of the exposures surpasses six years. This is a silent liability: old vulnerabilities that remained off the radar of inventories and remediation cycles. The remediation backlog, measured in years, is incompatible with the speed of the threat.

Analysis

The same findings repeat from company to company, and they are almost always old. The surface grows and accumulates. What comes in is rarely removed; what fails is rarely fixed.

The volume of vulnerabilities is misleading. What separates a risk inventory from an endless list is exploitation intelligence: knowing which flaws have an exploit, which are being used, which have a real probability of attack. Without that filter, the team addresses what is noisy — not what is dangerous.

PART 03

On the other side, the threat does not wait

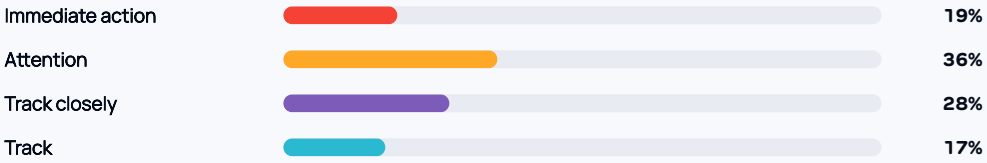
The pace of exploitation observed in the highest-risk cut — a fraction of roughly 1% of the vulnerabilities, selected by threat intelligence, exploit intelligence and Machine Learning.

About the cut. The CSURFACE platform detects the full universe of vulnerabilities on each monitored asset. The numbers in this part refer to the fraction of roughly **1% with the greatest potential to cause an incident** — identified through the cross-referencing of **threat intelligence**, **exploit intelligence** and **Machine Learning** over this base. It is on this prioritized cut that the pace of exploitation in the real world is measured.

EMERGING THREATS MONITORED	PUBLIC EXPLOIT IN	ACTIVE EXPLOITATION IN	UNDER REAL EXPLOITATION
2,954	**5 days**	**90 days**	**809**
prioritized cut · high severity	average time after disclosure	average time until real-world attack	confirmed exploited in the wild

Most exploited flaw classes (CWE)

Real priority — SSVC categorization



Analysis

While the surface accumulates in silence, the threat on the other side moves at an **industrial pace**. A working public exploit appears, on average, five days after a flaw is disclosed. In some cases the exploit comes before the notice: among the critical threats monitored there are hundreds exploited as zero-day.

The attacker's aim is precise. Five of the six most exploited flaw classes are **web application** flaws — injection, path traversal, file upload. It is exactly the layer that, in Part 02, appears without a WAF in 71% of the applications analyzed. The threat curve points to the most unprotected point of the defense.

And severity is not priority: even in a set where every flaw is serious — average CVSS 9.0 — the SSVC categorization classifies only **19% as immediate action**. Any team can read exploitation indicators; the hard part is cross-referencing that intelligence with the real surface and knowing, week by week, which threats reach its own assets.

The list never stops growing. The catalog of demonstrably exploited vulnerabilities is updated every week — a single recent week recorded 12 new entries. A quarterly scan misses the entire window. Only continuous monitoring detects the flaw in the week it becomes a confirmed threat.

THE CONCLUSION

The encounter — where the incident is born

What the volume of threats has to do with the surface reports.

THE THREAT ATTACKS

5 days

average time between a flaw being disclosed and a working public exploit existing for it.

×

THE DOOR STAYS OPEN

5+ years

time that the oldest vulnerability remains exposed in 68% of the companies analyzed.

The analysis

Everything. That is the answer to what the volume of threats has to do with the surface reports. Each ungoverned asset from Part 01 — a forgotten cloud environment, a third-party component, an application without a WAF — is a door. Part 03 says that doors are found and attacked within days. The reports in Part 02 say that these doors stay open for years.

Side by side, the two datasets converge on a single conclusion. The defense adds assets faster than it can inventory them, and removes or fixes almost nothing — exposure time is measured in **years**. The attacker weaponizes an exploit in **days**.

An incident, therefore, is the predictable intersection of two curves: a surface that grows disorderly and never shrinks, and a threat that only accelerates. The incident is merely the time when the two cross on the same asset — almost always an asset absent from the inventory.

What closes the distance between the two curves

A surface that is not seen cannot be fixed, and the speed of the threat is not beaten by manual effort. Closing that distance requires two capabilities operating together and without stopping:

Continuous discovery — which finds every door, including the cloud environments, the shadow IT and the assets absent from the inventory.

Threat and exploit intelligence — which says which doors are being attacked now, and reorders the priority queue as the threat evolves.

One without the other leaves the window open. It is the continuous combination of the two — discovery and intelligence in the same data model — that turns exposure into manageable risk.

csurface

CONTINUOUS EXPOSURE MANAGEMENT

From disorderly exposure to prioritized action.

CSURFACE is a single platform for external attack surface management. It brings together, under one data model, the two capabilities this report shows to be inseparable: discovering everything that is exposed and knowing, in real time, what the threat will exploit first.

Continuous discovery
Maps the entire external surface from the root domain — cloud, shadow IT, third-party chain and forgotten assets. No agents, no lists to provide.

Machine Learning classification
Attributes each asset to the organization, eliminates the false positive of ownership and classifies by business criticality. An inventory with context.

Threat and exploit intelligence
Cross-references each exposure with indices of active exploitation and emerging threats — the priority queue reflects the real risk and reorders itself.

Exploitability validation
Confirms what is in fact exploitable, with active external testing where there is coverage and passive detection across the rest of the surface.

Credential monitoring
Tracks corporate credentials leaked in breaches and on the dark web, with alerts in hours — not in months.

Risk quantification
Capability under development: it will translate technical risk into financial value, so that the board decides based on numbers, not on technical alerts.

See where your company stands in this picture.

Get my company's preliminary analysis →