We Index the Internet.
Your External Security Runs on It.

Deepinfo indexes the whole internet: 400M+ domains, 2B+ subdomains, 200B+ DNS records and 30B+ SSL certificates, with their IP addresses and their WHOIS and HTTP records. Your assets, your vendors and the lookalikes built to copy you are already in it. We bring them to light.

PLATFORM

Every Module. One Index. One Place to Act.

The Deepinfo Platform is a Continuous Threat Exposure Management platform built as modules, each reading a different part of the internet, from the hosts you expose to the credentials that have already leaked. All of them run on Deepinfo's own internet index, with one engine, one scoring scale and one API.

THE MODULES

What Each Module Reads.

EASM	**External Attack Surface Management**	Discovers the domains, subdomains and IPs tied to your organization, scans each one layer by layer, from WHOIS and DNS to open ports and web data, and ranks what it finds with CVSS, EPSS and CISA KEV. Each issue stays on record until a rescan confirms the fix.
CTI	**Cyber Threat Intelligence**	Reads breach data, infostealer logs and dark web sources for your domains, employees and customers, and profiles the threat actors that target your region and industry. Each finding points to an account, a device or a person your team can act on.
BRP	**Brand Risk Protection**	Matches domains across the index against your brand keywords: exact, inside a longer name, one typo away, or spelled with characters from other alphabets that read as your own. Each lookalike your team approves is then monitored across DNS, MX, SSL and HTTP, with a risk score timeline. Social media, app store and search engine monitoring cover where customers meet your brand away from your domains, and Managed Takedown handles removal.
TPRM	**Third-Party Risk Management**	Runs the EASM engine on a portfolio for each third party, with its discovery, scanning and scoring. A vendor's score and yours sit on one scale.
DSI	**Deep Search & Insights**	Opens the index to your analysts and developers: domain search and reverse lookups, WHOIS and DNS history, vulnerability search and live lookups. It is the data the other modules run on.

IN USE

10,000+

organizations work from Deepinfo data, on the platform and through the API. Banks, airlines, telecom operators, defense manufacturers, public institutions and security vendors among them.

TURKISH AIRLINES	TURKCELL	aselsan	BITSIGHT	WILEY	alBaraka
Invicti	TÜRKSAT	HAVELSAN	beko	Istanbul Airport	Tüpraş

THE INDEX

Under Every Module Is an Index We Built.

Many platforms rent their view of the internet. We collect ours, resolve it and keep it with its history. That data powers each module, and your analysts and developers can query it directly.

DATA & API

API reference
docs.deepinfo.com/reference/

Build on the Data Under the Platform.

The index behind the platform is open to your code: API services answer one question per call, and data feeds hand over whole datasets as files.

API SERVICES

Ask the Index, One Call at a Time

REST endpoints for one target or one query per request: live lookups, DNS and WHOIS history, pivots from an IP, mail server, name server or registrant email to every domain behind it, and CVE search with EPSS and CISA KEV.

DATA FEEDS

Take the Dataset With You

Files for teams that load the data into their own systems: all the domains and subdomains Deepinfo knows about, plus daily files of registered, updated and deleted domains and newly discovered subdomains.

Customer Stories

Each one covers the problem, the modules the team runs and what changed.

EDUCATION · TÜRKİYE

A Leading Research University

Continuous discovery across decentralized departments, research labs and student-organization infrastructure.

HEALTHCARE · TÜRKİYE

An International Humanitarian Foundation

Fraudulent donation domains caught and taken down, and field-program infrastructure monitored at the depth of headquarters.

GOVERNMENT · TÜRKİYE

A Metropolitan Municipality

Lookalikes of citizen-facing services watched through tax, permit and enrollment seasons, and removed through Managed Takedown.

WHY WE EXIST

No organization should be blindsided by something that was observable all along.

Organizations have more internet-facing assets than their security teams can name. Subsidiaries register domains, partners stand up infrastructure, and acquisitions arrive with systems nobody has inventoried.

Attackers look for exactly what defenders lose track of. Deepinfo gives security teams that same outside view, kept current, with a next step attached to everything in it.