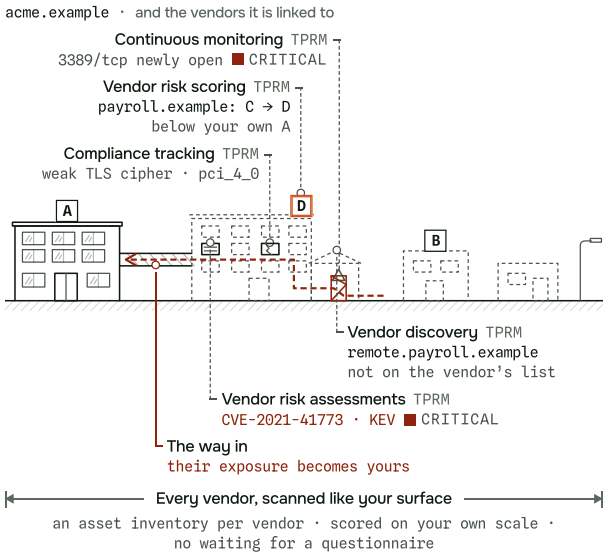
Your Vendors' Exposures Are Yours Too.

Third-Party Risk Management assesses the cyber risk that vendors, suppliers and partners bring into your organization. Deepinfo runs its External Attack Surface Management engine on each third party: every vendor becomes a portfolio with its own asset inventory, scanned and scored like your surface, without waiting for a questionnaire to come back.

Your Vendors' Exposures Are Yours Too.

Third-Party Risk Management assesses the cyber risk that vendors, suppliers and partners bring into your organization. Deepinfo runs its External Attack Surface Management engine on each third party: every vendor becomes a portfolio with its own asset inventory, scanned and scored like your surface, without waiting for a questionnaire to come back.

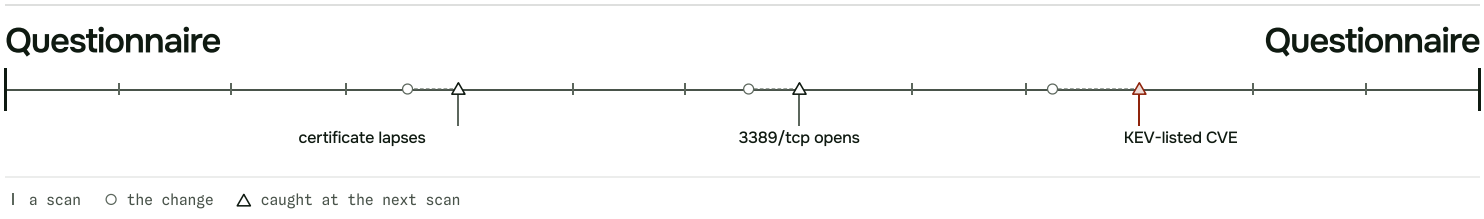


Vendor Risk Changes Between Reviews.

The usual third-party program runs on annual questionnaires and certificates collected in spreadsheets. The answers describe one moment, written by the party being assessed.

Between two reviews a vendor can let a certificate lapse, expose a remote desktop port or fall behind on a CVE that CISA has listed as exploited. None of that waits for the next questionnaire.

A questionnaire tells you what a vendor believes about itself. A scan shows what an attacker sees.



Discovery to Compliance Across Your Vendor Portfolio.

Vendor Discovery

Start from a vendor's primary domain and map what it runs on the internet: the subdomains, IP addresses and related domains no questionnaire lists.

Discovery →

Continuous Monitoring

Scan the assets in each vendor portfolio across the data layers used for yours, and keep each layer's history so you can see what changed.

Monitoring →

Vendor Risk Assessments

Misconfigurations, weak TLS, expiring certificates, exposed services and known CVEs on vendor infrastructure, each with evidence and a severity from Critical to Information.

Assessments →

Vendor Risk Scoring

A security score for each vendor, built like yours, with every CVE ranked by CVSS, EPSS and CISA KEV together.

Scoring →

Compliance Tracking

Vendor findings classified against the frameworks your issues use, from OWASP Top 10 2021 to PCI DSS 4.0 and HIPAA.

Compliance →

Your Vendors on One Scale.

Each third party is its own portfolio, scored by the engine that scores your surface, so a weak vendor stands out against the rest and against you.

acme.example — A
YOURS · YOUR OWN SURFACE

payroll.example — C → D
VENDOR · LINKED TO YOU

`remote.payroll.example` · 3389/tcp newly open CRITICAL · not on the vendor's list

`docs.payroll.example` · CVE-2021-41773 CRITICAL KEV

The way in: payroll.example → acme.example. Their exposure becomes yours.

cloud-hosting.example	A
cdn-provider.example	A
logistics-co.example	B
law-firm.example	C
call-center.example	C
marketing-agency.example	B
subsidiary-eu.example	B
crm-saas.example	A

Your Scan Engine Runs on Vendors Too.

A portfolio holds one organization's assets: its own inventory, its own scans, its own issues and its own score. Adding a vendor works like adding a new part of your surface.

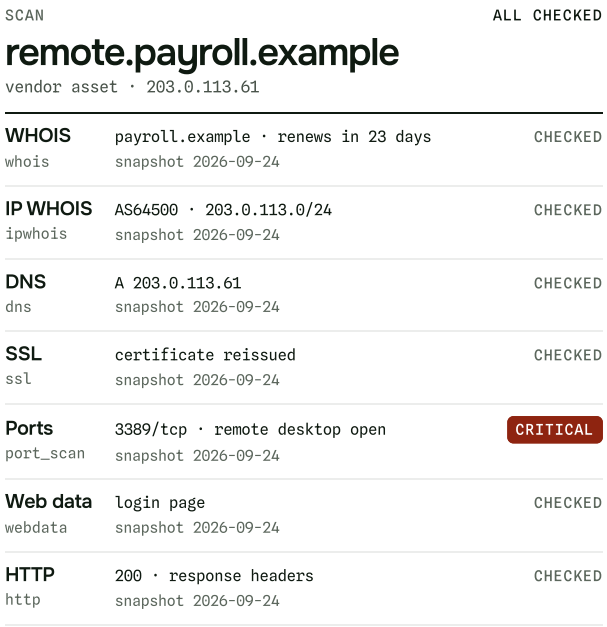
Because the engine is shared, a vendor finding looks exactly like one of your own. The severity scale, the issue states, the evidence and the CVE ranking are identical, so the two can be compared line by line.

DATA LAYERS	WHOIS to HTTP, per vendor asset
ISSUE STATES	The lifecycle your issues use, with the history of each change
SEVERITY	Critical, High, Medium, Low, Information
FRAMEWORKS	OWASP, PCI DSS 4.0 and 3.2, HIPAA, CWE, CAPEC, WASC

Scan Layers Read as Vendor Risk.

The layers are the ones EASM scans on your assets. What changes is the question you ask of them.

- **WHOIS**: which registrar holds the vendor's domains, and when each registration expires
- **IP WHOIS**: which networks, owners and countries the vendor's services run on
- **DNS**: how its name servers and mail exchangers are set up, and when records change
- **SSL**: expired and expiring certificates, their issuers, and the host names each one reveals
- **Ports**: services open to the internet over TCP and UDP, such as remote access or databases
- **Web data**: technologies in use, login pages and screenshots
- **HTTP**: response headers and status codes for each host it exposes



What Each Source Can Tell You.

Questionnaires still matter for what only the vendor knows. External scanning covers what anyone on the internet can already see, and keeps covering it between reviews.

	External scanning	Questionnaire
VISIBLE FROM THE INTERNET		
Expired or expiring certificates	✓	Self-reported
Open ports and exposed services	✓	Self-reported
Known CVEs on internet-facing technology	Ranked by CVSS, EPSS and KEV	Self-reported
Changes between review cycles	✓	–
Needs the vendor to take part	No	Yes
KNOWN ONLY INSIDE THE VENDOR		

	External scanning	Questionnaire
Security awareness training	–	✓
Incident response procedures	–	✓
Internal access controls	–	✓

Where It Fits in Your Vendor Program.

BEFORE SIGNING

Onboarding

Add a prospective vendor's primary domain as a portfolio and review its external posture before the contract is signed.

DURING THE CONTRACT

A Continuous Watch

The notification rules that watch your assets cover vendor assets too: new and reappeared issues, score drops, certificate, WHOIS and DNS changes, new open ports. Instant, or as an hourly to monthly digest.

AT REVIEW TIME

Evidence on Record

Each vendor issue keeps its evidence, its state history and its framework classification, so a review starts from records instead of a request for answers.

Query This Data Through the API

Vendors are discovered and scanned from the index that holds your assets. Your tools can look up any vendor's domains through the API. The index holds 400M+ domains, 2B+ subdomains, 200B+ DNS records and 30B+ SSL certificates.

Domain Detail API	API →	Subdomain Finder API	API →
Associated Domain Finder API	API →	Domain WHOIS API	API →

See Your Own Exposure, From the Outside.

REQUEST A DEMO

www.deepinfo.com/request-demo

PRICING

www.deepinfo.com/pricing

API DOCUMENTATION

docs.deepinfo.com

OFFICES

Istanbul (HQ)
Paris
Kuwait City

CONTACT

www.deepinfo.com/contact

SECURITY

security@deepinfo.com

© 2026 DEEPINFO