CYBERMON

PRODUCT COVERAGE DOCUMENT

Attack Surface Intelligence

Find what you've exposed — including what you forgot you deployed.

What ASI is

Attack Surface Intelligence is the CyberMon product that answers a question most organisations cannot answer from memory: **what of ours is reachable from the public internet right now, and which of it is weak?**

Every domain you register, every server you spin up, every API you publish and every cloud resource a team creates becomes part of your attack surface the moment it is exposed. That surface changes weekly — a marketing microsite, a test environment left running, an API gateway an engineering team stood up without telling IT. An attacker enumerates all of it. Most organisations have an asset inventory that is a spreadsheet, and it is out of date.

CyberMon ASI discovers that surface continuously, from the outside in, the same way an attacker would — then tests what it finds for known vulnerabilities, weak encryption and misconfiguration, and returns a prioritised list with the evidence attached.

> *"We find what you've exposed, including what you forgot you deployed."*
>
> CYBERMON ASI — POSITIONING

Asset types discovered

ASI builds and maintains an external asset inventory across five classes of asset, without requiring you to supply a list first. Discovery is automated and runs on an ongoing basis, so newly created exposure enters the inventory rather than waiting for the next audit.

Domains

Internet-facing domains associated with your organisation, including properties registered outside central IT — campaign sites, regional entities, legacy brands.

IP addresses

Public IP space attributable to your organisation, including hosts standing up outside the ranges your network team maintains.

APIs

Exposed API endpoints — including those published for partner or mobile use that never appeared in an internal inventory.

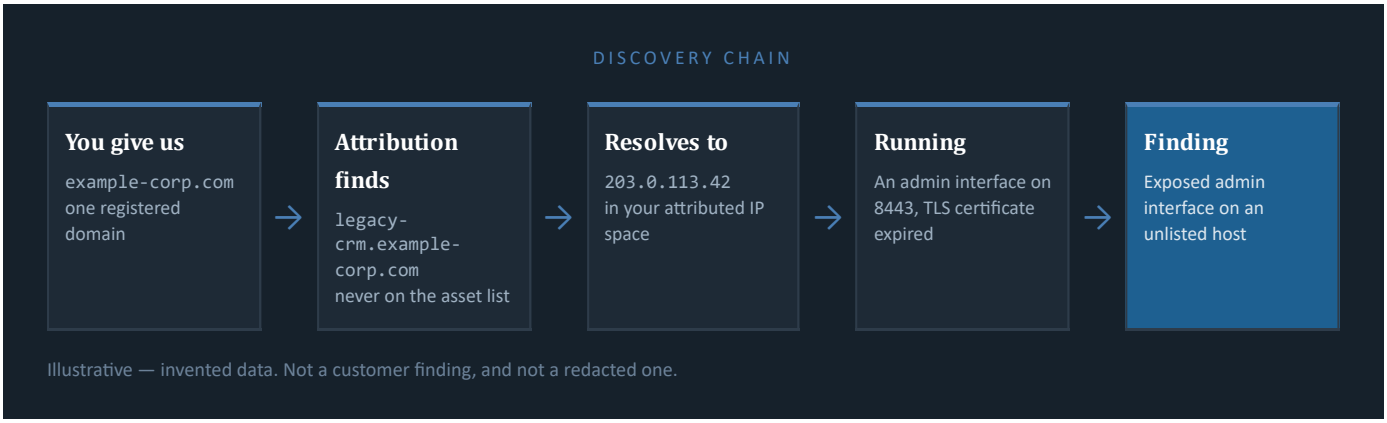
Cloud resources

Internet-reachable resources in your cloud estate, discovered from the outside rather than from a console you have to remember to check.

Shadow IT

Assets that belong to you but that no one in security put there — the single largest source of surprise in a first ASI report.

How an asset nobody listed becomes a finding



Detection surfaces

Discovered assets are continuously assessed across six detection surfaces.

DETECTION SURFACE	WHAT IS CHECKED	WHY A BUYER CARES
CVE detection	Continuous identification of known, published vulnerabilities affecting exposed services and software.	Known CVEs on internet-facing assets are the most commonly exploited route in.
Web vulnerability detection	Continuous testing of exposed web applications and interfaces for exploitable weaknesses.	Web applications change with every release. An annual test describes an application that no longer exists.
TLS / SSL posture	Encryption posture on exposed services — certificate and transport-layer configuration.	Expiring or weak certificates are a routine first flag for regulators and enterprise procurement.
Weak configuration checks	Configuration weaknesses on exposed infrastructure and services.	Most breaches are a default left in place on something nobody remembered was reachable.
AI and LLM endpoint exposure	Detection of exposed AI and large-language-model endpoints attributable to your organisation.	AI endpoints are deployed faster than they are inventoried.
Login / MFA detection	Detection of authentication endpoints exposed to the internet and whether multi-factor authentication is enforced on them.	An exposed login page without MFA is one of the most common single points of compromise, and one of the easiest to miss on a spreadsheet inventory.

A worked example: the host nobody remembered

Invented, but the shape is the one that recurs. Names and addresses are fictional.

1. **What you supplied.** One domain, `example-corp.com`, and nothing else. No asset list, no IP ranges.
2. **What ASI attributed.** Forty-one internet-facing hosts, of which nine did not appear on the inventory the customer keeps for their auditor. One was `legacy-crm.example-corp.com` — a CRM stood up for a migration in a previous financial year, never decommissioned.
3. **What was checked.** An administrative interface reachable on port 8443, a TLS certificate expired some months earlier, and a login page with no rate limiting or MFA visible from outside.
4. **What the customer did.** Confirmed the host was theirs, established that the owning team had left, and took it off the internet in an afternoon. It had been reachable for over a year.

The point: no scanner finds this if the asset is not on the list you give it. The finding exists because discovery started from the domain, not from the inventory.

Monitoring scope

- **Continuous, not periodic.** Discovery and assessment run on an ongoing basis rather than as a scheduled engagement. New exposure is found because it appeared, not because an audit was due.
- **External perspective.** Assessment is performed from outside the perimeter, against what is actually reachable — not against what an internal inventory claims exists.
- **Attribution-driven.** The inventory grows as assets are attributed to your organisation, which is what surfaces shadow IT.

Key features

FEATURE	WHAT IT MEANS IN PRACTICE
Evidence with every finding	Every finding ships with proof — the record, the screenshot, the config. Directly usable for incident response, board reporting and DPDP breach notification.
Deduplication and scoring	Findings are deduplicated and scored against business context before they reach you, so the same issue seen on twelve hosts is one item to fix, not twelve tickets.
Correlation across products	An ASI finding is joined to related Digital Risk Intelligence and Compliance findings rather than being reported in isolation.
Built for small security teams	Deduplication and scoring built for teams of two to ten, not a 40-analyst SOC.

How CyberMon differs from the alternatives

Organisations buying external security visibility today choose between three things. Each solves part of the problem.

APPROACH	BREADTH	FREQUENCY	COST PROFILE
Annual VAPT / consultants	Deep but narrow	1–4× a year	A per-engagement fee, repeated
Point-tool stacks	Broad but siloed	Varies by tool	Several subscriptions, plus the integration effort to join them up
Global DRI / ASI platforms	Broad and deep	Continuous	Priced in dollars, for enterprise budgets
CyberMon	**Broad, deep and correlated**	**Continuous**	**Architected for the Indian mid-market, on the same data pipeline**

The correlation difference

"An exposed asset, a leaked credential for it, and a compliance control that covers it are one finding in CyberMon — and three disconnected alerts everywhere else."

This is the practical reason ASI is stronger inside the CyberMon platform than as a standalone scanner. An exposed VPN appliance is a moderate finding. An exposed VPN appliance *with a matching credential in a stealer log* is an incident — and only a system that sees both can tell you which one you are looking at.

On cost

"Global equivalents price in dollars for enterprise budgets. CyberMon is architected to serve an MSME at a fraction of that cost on the same data pipeline." CyberMon's defensibility is that data pipeline and its India-specific sources — app stores, regional phishing infrastructure and Telegram channels that global vendors under-index on.

Who ASI is for, and the problem it solves

Target sectors: BFSI · Healthcare · Energy & Infrastructure · Government & Telecom · Retail & E-commerce · Technology & SaaS.

ASI is bought by the security or IT leader who owns external exposure and cannot currently prove what it consists of. It is most valuable where the asset estate changes faster than the inventory that describes it.

The questions ASI is bought to answer

- How many internet-facing assets do we actually have, and how does that compare with the list we gave our auditor?
- What did engineering expose last quarter that security was never told about?
- Which of our exposed systems has a known, published vulnerability on it today?
- Are any certificates about to expire, or any login pages exposed without MFA?
- Have any AI or LLM endpoints been exposed under our name?

Where an annual penetration test leaves a gap

A VAPT engagement is deep and valuable, and CyberMon does not replace it. But it tests a defined scope at a point in time. It cannot find the asset that was created three weeks after the scope was agreed, and it says nothing about the eleven months between engagements. ASI covers that interval.

What you need in place to get value from this

Someone who can act on a finding. CyberMon finds, prioritises and evidences; it does not remediate. A finding lands with the person who owns the affected asset. That can be one part-time person, but it cannot be nobody.

Delivery

What is built and running today

Automated asset discovery and ingestion pipelines; risk scoring, deduplication and correlation engine in production; analyst alert queue, evidence capture and customer reporting workflow; live platform at cybermon.co.in.

Onboarding & reporting

Onboarding begins with attribution — establishing which internet-facing assets belong to your organisation — after which automated discovery and ingestion run on an ongoing schedule. Because discovery is external, ASI does not require agents on your infrastructure to begin. Findings reach you through the analyst alert queue and the customer reporting workflow, cadence and notification target agreed at scoping.

How it is bought

Attack Surface Intelligence is sold as an annual subscription, scoped per engagement against the customer's attack surface, exposure level and industry. Pricing is quoted per engagement — speak to CyberMon, or to your CyberMon partner, for a scoped quote. ASI is most effective purchased alongside Digital Risk Intelligence, where correlation between an exposed asset and a leaked credential for it becomes available.

CyberMon

Three products. One risk score.

CyberMon LLP · Bengaluru, India · LLPIN ACZ-2481 · cybermon.co.in

Free leak-and-exposure reporting is available on the live platform.