CYBERMON

PLATFORM COVERAGE DOCUMENT

The CyberMon Platform

Three products. One risk score.

ASI
Attack Surface Intelligence — what you expose

DRI
Digital Risk Intelligence — what's sold about you

C&C
Compliance & Cloud Security — does it hold up

The platform in one paragraph

> *"CyberMon continuously discovers everything an organisation exposes to the internet, watches what is being said and sold about it outside the firewall, checks its cloud against the frameworks it is held to — and returns one prioritised, evidence-backed risk score."*
>
> CYBERMON — PLATFORM POSITIONING

Three products. One risk score.

Most organisations already own tools that cover parts of this. What they do not own is anything that joins the parts together. An exposed server sits in a vulnerability scanner. A leaked credential sits in a threat feed. A failing control sits in a compliance spreadsheet. Nothing tells the security team that all three describe the same problem — so the team triages three queues and prioritises none of them well.

The three products

PRODUCT 1 · ASI

Attack Surface Intelligence

What you have exposed to the internet, and which of it is weak.

- Discovers domains, IPs, APIs, cloud resources and shadow IT
- Continuous CVE and web vulnerability detection
- TLS/SSL posture and weak configuration checks
- AI and LLM endpoint exposure
- Login and MFA detection on exposed endpoints

> *"We find what you've exposed, including what you forgot you deployed."*

PRODUCT 2 · DRI

Digital Risk Intelligence

What is being said, sold and faked about you outside the firewall.

- Dark web forums, leak sites and paste site monitoring
- Stealer-log credential and corporate email exposure
- Typosquat domains, phishing kits, fake apps on app stores
- Executive impersonation and fake social media handles; takedowns

> *"We watch what's being sold about you. If your employee's credentials are in a stealer log tonight, you know tomorrow — not in two hundred and sixty-three days."*

Sources monitored: data leak sites, dark web forums (including carding forums), paste sites and public code repositories, credential leaks, phishing infrastructure, app stores (Google Play, the App Store and third-party stores), social media impersonation, and Telegram channels. Takedowns are delivered as an analyst-led service; there is no automated takedown workflow today.

PRODUCT 3 · COMPLIANCE & CLOUD SECURITY

Compliance & Cloud Security

Whether your cloud stands up to the frameworks you are held to.

- Cloud misconfiguration and exposed storage detection
- Over-permissive IAM and privilege escalation paths
- Continuous mapping to SOC 2, ISO 27001, GDPR, PCI DSS and DPDP
- Prioritised, step-by-step remediation guidance

> *"We check your cloud against SOC 2 and ISO 27001 continuously, with evidence, so an audit is a report, not a project."*

Frameworks mapped today: SOC 2, ISO 27001, GDPR, PCI DSS and India's DPDP Act. The RBI and SEBI cyber-security frameworks, CERT-In directions and HIPAA are not yet mapped. Unlike the other two products, this one requires read access to the cloud accounts in scope. CyberMon is not an auditor and does not issue certifications or attestations.

The unified risk score

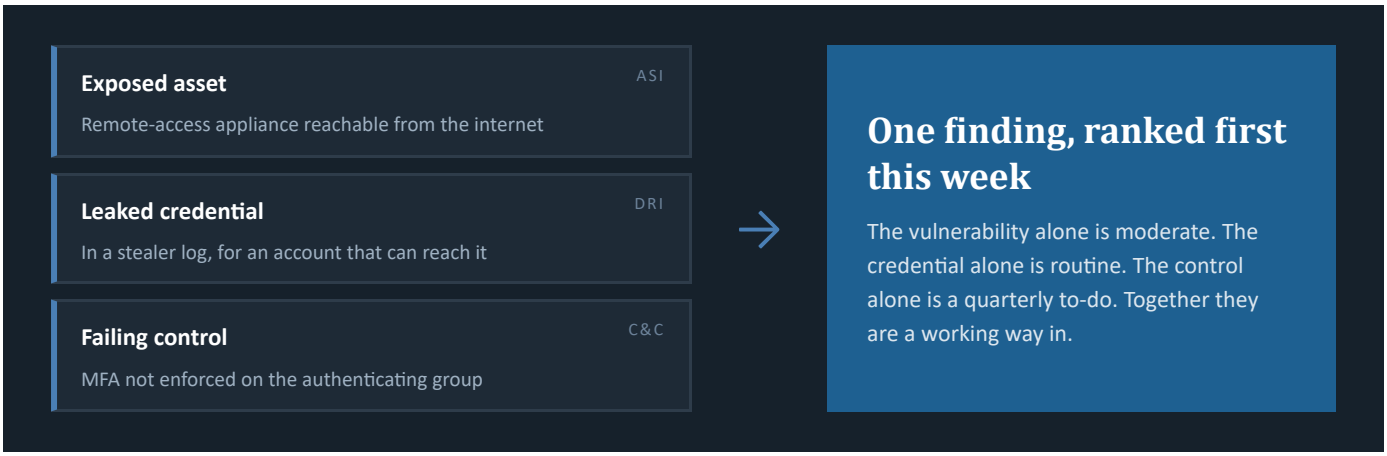
> *"Findings from all three are deduplicated, correlated and scored against business context — so a security team sees the five things that matter this week, with the evidence attached, instead of five hundred alerts with none."*

This is the output of the platform, and the reason the three products are sold as one system rather than three subscriptions. Findings arrive deduplicated against each other, correlated where they describe the same underlying risk, and ranked against what that risk means for the business.

The differentiator

Correlation

"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."



What one correlated finding looks like

RANK 1 OF 6 · CM-00412 · OPEN · ANALYST REVIEWED

Internet-facing remote-access appliance with a leaked credential and no MFA on the authenticating group

ASSET	`vpn-uat.example-corp.com`	discovered by attribution — not supplied by you
CREDENTIAL	`r.menon@example-corp.com`	present in a stealer log; the account can reach this service
CONTROL	`MFA not enforced`	mapped to SOC 2 and ISO 27001 access controls

Suggested action: reset the credential · enforce MFA on the group · patch or restrict the appliance

Illustrative — invented data. Password material is never reproduced in reporting: the matched fields are shown, the secret is not.

Evidence, and teams sized right

“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 built for teams of two to ten, not a 40-analyst SOC. The output is an action, not a feed.” This is a design constraint, not a limitation. A platform that assumes a large analyst bench produces volume; a platform that assumes a team of four has to produce ranking.

How CyberMon differs from the alternatives

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**

“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.”

The defensibility is the data pipeline itself and the India-specific sources feeding it — app stores, regional phishing infrastructure and Telegram channels that global vendors under-index on. For an organisation whose customers, brand exposure and regulatory obligations are in India, that coverage difference is the one that changes the findings.

What is built and running today

The following is the correct basis for what a client can contract for now.

CAPABILITY
Automated asset discovery and ingestion pipelines across all three products
Risk scoring, deduplication and correlation engine in production
Threat-source normalisation across leak sites, forums, paste sites and app stores
Analyst alert queue, evidence capture and customer reporting workflow
Live platform at cybermon.co.in, including free leak-and-exposure reporting

What is not being claimed

CyberMon has a funded roadmap beyond the capabilities above. Nothing on that roadmap is represented in this document as available. Items on the roadmap — including a self-serve tier for smaller organisations, an automated takedown workflow, and expanded India-specific collection — are available for discussion, but are not part of what is being sold today.

What these attacks actually cost, sector by sector

Independent, third-party research — not a CyberMon claim about any customer. Included to size the problem CyberMon is built to close: the gap between when a breach happens and when it is found and priced.

$4.44M
Global average cost of a data breach, 2025

$7.42M
Healthcare — highest of any sector, 14th year running

279 days
Average time to identify and contain a healthcare breach

SECTOR	AVERAGE COST OF A BREACH (2025)
Healthcare	**$7.42M**
Financial services	**$5.56M**
Industrial	**$5.00M**
Energy	**$4.83M**
Technology	**$4.79M**
Global average, all sectors	**$4.44M**
Education	**$3.80M**
Retail	**$3.54M**
Public sector	**$2.86M**

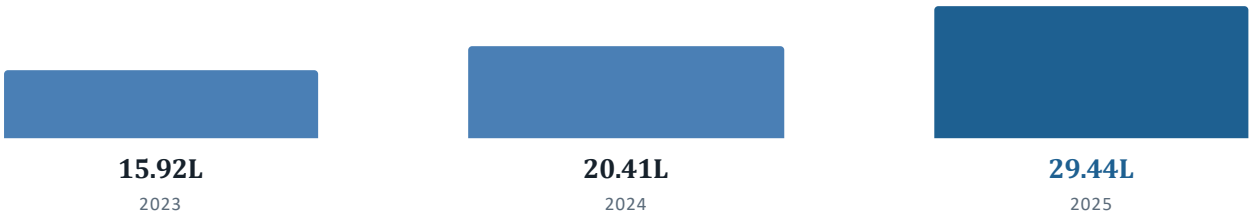
Two trends stand out. First, the sectors CyberMon targets — BFSI, healthcare, energy and infrastructure, government — sit at or above the global average, not below it. Second, the **public sector recorded the sharpest year-on-year increase of any industry, up 10.8%** (roughly $310,000 per breach), even though its absolute cost is the lowest — the direction of travel matters as much as the current number. In the United States specifically, the average breach cost reached a record **$10.22M**, up 9% year-on-year, underlining how quickly this figure moves in a regulated, high-scrutiny market.

Source: IBM, *Cost of a Data Breach Report 2025* (600 breached organisations across 17 industries, published 2025). Figures are global averages in USD and are not specific to CyberMon customers or to India; they are cited here to frame the cost of late detection, not as a claim CyberMon has measured them itself.

The Indian market: incidents, losses, and the gap they are buying to close

A separate section because the Indian threat and market picture does not track the global one directly — incident volume, the sectors hit hardest, and reported losses all come from Indian regulatory and industry sources.

Incidents tracked by CERT-In, by year



Lakh (1L = 100,000) cyber incidents tracked by CERT-In — roughly an 85% increase over two years. In 2025, unauthorised network scanning and probing alone accounted for about 83% of everything CERT-In handled.

~22%
of tracked attacks hit healthcare in 2025 — up 8 points from 2023, the largest single-sector share

₹36,014 Cr
Indian banking-system fraud losses, FY2024–25 (RBI) — includes ₹18,674 Cr from reclassified legacy loan-fraud cases

$4.46B
Revenue of India's cybersecurity product industry, 2025 — 34% CAGR since 2020 (DSCI)

> BFSI, healthcare, telecom and government platforms are named repeatedly across CERT-In, RBI and DSCI reporting as the sectors under the most sustained pressure — the same sectors CyberMon targets with DRI and Compliance & Cloud Security.

What it means for a buyer

Incident volume is rising faster than headcount in most Indian security teams, and a meaningful share of reported financial loss traces back to the same root causes CyberMon watches for: credentials traded before they are used, cloud controls that quietly stop holding, and exposure nobody re-checked after the last audit. India's broader cybersecurity market (products and services combined) is estimated at roughly $8.6–12 billion in 2025 depending on methodology, and is forecast to keep growing at 14–15% a year — the spend is accelerating alongside the incident count, not ahead of it.

Sources: CERT-In / PIB India (cyber incident volumes, 2023–2025); Data Security Council of India, *India Cyber Threat Report 2025* and *Cybersecurity Product Landscape Report 3.0* (sector share, product-industry revenue); Reserve Bank of India annual report on bank fraud, FY2024–25 (fraud losses, via RBI reporting reproduced in Indian financial press). Market-size range synthesises multiple independent analyst estimates published in 2025; figures vary by scope and are not CyberMon's own data.

Who the platform is for

Target sectors: BFSI · Healthcare · Energy & Infrastructure · Government & Telecom · Retail & E-commerce · Technology & SaaS. These are the sectors CyberMon targets and is built to serve, not a claim of live deployment.

SECTOR	WHAT DRIVES THE PURCHASE
BFSI	Regulated exposure, customer-facing phishing and fake apps, credential theft, and an evidence requirement a spreadsheet cannot satisfy.
Healthcare	Patient data on leak sites, ransomware targeting providers and suppliers, cloud estates that grew faster than their controls.
Energy & infrastructure	Large, old and partly undocumented external surface; high consequence of a single exposed system.
Government & telecom	Supply-chain scrutiny, demonstrable continuous monitoring, impersonation of public-facing services.
Retail & e-commerce	Cloned storefronts, fake apps, impersonating social accounts, payment-card obligations under PCI DSS.
Technology & SaaS	Rapidly changing asset estate, customer-driven SOC 2 and ISO 27001 obligations, access to tenants traded on dark web forums.

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

Onboarding establishes attribution — the domains, IP space, cloud accounts, brands, executives and corporate email domains belonging to your organisation. Automated discovery and ingestion then run on an ongoing schedule across all three products. External discovery does not require agents on your infrastructure; Compliance & Cloud Security requires read access to the cloud accounts in scope.

Reporting reaches you through the analyst alert queue and the customer reporting workflow, every finding carrying its proof. Reporting cadence, alert channel and the critical-finding notification target are agreed at scoping.

How it is bought

The three products are sold as annual subscriptions, 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.

CyberMon — three products, one risk score

ASI — what you have exposed to the internet, and which of it is weak.

DRI — what is being said, sold and faked about you outside the firewall.

Compliance & Cloud Security — whether your cloud stands up to the frameworks you are held to.

Bengaluru, India · cybermon.co.in

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