CYBERMON

PRODUCT COVERAGE DOCUMENT

Compliance & Cloud Security

So an audit is a report, not a project.

SOC 2 | ISO 27001 | GDPR | PCI DSS | DPDP

What Compliance & Cloud Security is

Attack Surface Intelligence looks at what you have exposed. Digital Risk Intelligence looks at what is being sold about you. Compliance & Cloud Security looks inward at the one estate that changes fastest and is audited hardest: **your cloud — and whether it stands up to the frameworks you are held to.**

Most cloud problems are not attacks. They are a storage bucket someone opened for a migration and never closed, a role granted broad permissions during an incident and never revoked, a default that was fine at ten engineers and is not fine at eighty. None of it triggers an alert. It sits there, quietly, until an auditor finds it — or until someone else does.

And when the audit comes, the work is not usually the fixing. It is the evidence: proving what the configuration was, when, and that the control was operating. Teams spend weeks assembling screenshots for a report that describes a cloud estate which has already moved on.

> *"We check your cloud against SOC 2 and ISO 27001 continuously, with evidence, so an audit is a report, not a project."*
>
> CYBERMON COMPLIANCE & CLOUD SECURITY — POSITIONING

Detection surfaces

The product assesses your cloud estate across two classes of finding: how resources are configured, and who can reach them.

DETECTION SURFACE	WHAT IS CHECKED	WHY A BUYER CARES
Cloud misconfiguration	Configuration weaknesses across cloud resources, assessed continuously rather than at audit time.	Configuration drifts constantly. A control that passed last review may not be passing now.
Exposed storage	Detection of storage that is reachable when it should not be.	Open storage is the most common single cause of large data exposure.
Over-permissive IAM	Identity and access roles carrying more permission than the job requires.	Permissions accumulate and are almost never withdrawn, so blast radius grows quietly.
Privilege escalation paths	Chains through which a lower-privilege identity could reach higher privilege.	Individually defensible permissions can combine into a route to administrator.

Framework mapping

Findings are mapped continuously to the control frameworks the organisation is assessed against, so a configuration finding arrives already carrying the control it affects.

FRAMEWORK	STATUS
SOC 2	Continuous mapping — current capability
ISO 27001	Continuous mapping — current capability
GDPR	Continuous mapping — current capability
PCI DSS	Continuous mapping — current capability
DPDP	Continuous mapping — current capability

Scope, stated precisely

India's **DPDP Act is now a mapped framework**, alongside SOC 2, ISO 27001, GDPR and PCI DSS — that is the complete list of what is mapped today. The **RBI and SEBI cyber-security frameworks, CERT-In directions and HIPAA remain outside current scope**, and nothing in this document should be read as covering them.

Every CyberMon finding also ships with evidence that is directly usable for DPDP breach notification — distinct from, and now in addition to, DPDP control mapping itself.

One finding

A storage bucket holding customer records is readable without authentication. Detected on an ongoing check, not at audit time.

SOC 2	logical access controls over stored data
ISO 27001	Annex A access control and information handling
GDPR	security of processing, where EU personal data is held
PCI DSS	protection of stored account data, where card data is present
DPDP	reasonable security safeguards for personal data

Illustrative. The control families named are indicative of where a finding of this class maps; exact control identifiers are confirmed per framework at onboarding.

Remediation guidance

Findings are returned with prioritised, step-by-step remediation guidance rather than a bare statement that a control is failing. The output is intended to be actionable by the team that owns the cloud account, not only by a specialist.

A worked example: remediation, step by step

Invented. This is the shape of the guidance attached to a finding, not a real customer's configuration.

1. **The finding.** Object storage container `ec-customer-exports` permits unauthenticated read. Public access block is disabled at the container level.
2. **Establish exposure first.** Check access logs for reads from outside your own ranges before changing anything — if the data has been read, that is an incident, and the evidence pack supports the notification.
3. **Re-enable public access blocking** at the container level, then at the account level so a future container cannot repeat the mistake.
4. **Replace the access path.** If anything legitimately needed to read the container, move it to a scoped role or a signed URL with an expiry rather than reopening public access.
5. **Confirm on the next assessment.** The finding is re-checked on the following cycle. If the condition is gone it closes; if it returns, it re-opens against the same record rather than arriving as a new one.

What CyberMon does not do: make the change. Guidance is guidance — cloud access is read-only by design, and your team performs the remediation.

Assessment scope

- **Continuous, not point-in-time.** Assessment runs on an ongoing basis, which is what allows an audit to be a report rather than a project.
- **Evidence-first.** Findings carry the proof with them, so the evidence pack is a by-product of monitoring rather than a separate exercise before an audit.
- **Correlated with the other two products.** A failing control is joined to the exposed asset it applies to and any leaked credential that reaches 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.
Continuous framework mapping	A configuration finding arrives already carrying the SOC 2, ISO 27001, GDPR, PCI DSS or DPDP control it affects, instead of being translated into control language later by hand.
Prioritised remediation	Findings are ranked and returned with step-by-step guidance, so the team fixes the control that matters rather than working down an alphabetical list.
Correlation across products	A failing control is joined to related Attack Surface Intelligence and Digital Risk Intelligence 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. The output is an action, not a feed.

Who it is for, and the problem it solves

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

BUYER	THE PROBLEM IT IS BOUGHT TO SOLVE
Technology & SaaS	Customer-driven SOC 2 and ISO 27001 obligations arriving faster than the team can evidence them, against an estate that changes with every release.
BFSI	Regulated exposure and a standing requirement to demonstrate control operation with evidence, not assertion.
Retail & e-commerce	PCI DSS obligations on a cloud estate that expands around every peak season.
Healthcare	Sensitive personal data in cloud storage, and GDPR obligations where the organisation handles EU data subjects.
Government suppliers	Demonstrable continuous control monitoring as a condition of participation, with an evidence trail that survives scrutiny.

The questions it is bought to answer

- Is anything in our cloud storage reachable that should not be?
- Which of our IAM roles carry more permission than the job needs, and can any of them reach administrator?
- Which SOC 2, ISO 27001 or DPDP controls are failing in our cloud right now — not at the last review?
- If our auditor asks for evidence next week, do we have it, or do we have to go and build it?

What this product is not

CyberMon is not an auditor and does not issue certifications, attestations or audit opinions. Compliance & Cloud Security provides continuous checks, control mapping and evidence to support your assessment; the assessment itself remains the work of your certification body or assessor.

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

Unlike Attack Surface Intelligence and Digital Risk Intelligence, which assess from outside the perimeter, this product requires **read access to the cloud accounts in scope**. Onboarding establishes that access and the framework or frameworks you are to be assessed against, after which checks and mapping run on an ongoing schedule. Findings reach you through the analyst alert queue and the customer reporting workflow, every finding carrying its proof. Cadence, alert channel and the critical-finding notification target are agreed at scoping.

How it is bought

Compliance & Cloud Security 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. The product is most effective purchased alongside Attack Surface Intelligence and Digital Risk Intelligence, where a failing control can be correlated with the exposed asset it covers and any leaked credential that reaches it.

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.