Fynd

Customer guide · November 2026 · Early access edition

Fynd Secure

The AI-native security command center for brands on Fynd

Protect the commerce you run on Fynd. Connect the rest of your estate. Let AI agents do the first work, with your team in control of the decisions that matter.

8	8	24x7
Fynd Guards for commerce properties	AI agents across your estate	Managed security team option

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Fynd Secure at a glance

Security for the commerce you run

Fynd Secure protects what runs on Fynd and brings the rest of your estate into one security command center.

29 min
average attacker breakout time in 2025[1]

8
Fynd Guards for commerce properties

8
AI agents for detection, investigation and response

24x7
managed security team option

Fynd Secure is a paid security product for Fynd enterprise and mid-market customers. Turn on extra Fynd Guards for storefronts, apps, checkout, APIs, OMS, Store OS devices, Kaily AI agents, Boltic workflows and the Fynd console. There is nothing to install for Fynd properties.

Then connect the rest of your estate: AWS, GCP, Azure, on-prem systems, Google Workspace, Microsoft 365, Okta, Entra ID, laptops and stores. One command center brings the signals together. Eight AI agents explain what is happening and take action within the policy you set.

Protect

Enterprise guards for everything you run on Fynd.

Command

One AI view across clouds, on-prem, SaaS, identity, endpoints and stores.

Managed

Fynd's 24×7 security team works with the agents when you want a service.

Built for decisions, not alert queues

Fynd Secure turns security signals into a plain-language story, shows the possible impact, and makes the next safe action clear. You stay in control of high-impact decisions.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Why now

Attackers move at machine speed

AI is making reconnaissance, social engineering and attack execution faster, while retail stays a direct path to money.

CrowdStrike reports that average interactive eCrime breakout time fell to 29 minutes in 2025, with the fastest observed breakout at 27 seconds. It also reports an 89% year-on-year increase in attacks by AI-enabled adversaries. A security team that reads alerts one by one can miss the window to contain an attack.[1]

In November 2025, Anthropic described a campaign in which AI carried out reconnaissance, wrote exploit code, harvested credentials, moved data and documented the operation across about 30 organisations. Anthropic estimated that AI performed 80% to 90% of the work, with people making only a few critical decisions. This is a vendor report and attribution, but it shows how the operating model is changing.[2]

Deepfake fraud does not need a software breach. The World Economic Forum reported that an Arup employee transferred 25 million US dollars after a video call with deepfake versions of senior managers. No Arup system was hacked. The control has to cover people, identity and approvals as well as code.[3]

27 sec
fastest recorded breakout in 2025[1]

80% to 90%
of one reported espionage campaign done by AI[2]

$25m
deepfake-enabled transfer reported at Arup[3]

The practical answer

Detection and response need to run together. Fynd Secure watches, explains, and acts within your rules, while keeping a human in the loop where the impact is high.

What is at stake for retail brands

Every sale day is an operating day for attackers

Retail attacks can change conversion, inventory, payment trust, customer accounts and store operations in the same incident.

Imperva found that automated traffic made up 51% of web traffic and bad bots made up 37% of all internet traffic in its 2025 report. Account takeover attacks rose 40% in 2024. For a retail brand, that can mean scraped prices, hoarded inventory, fake sign-ups, stolen loyalty points and card testing, not just slow pages.[4]

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Account takeover

Stolen passwords are tested at scale. A successful login can expose addresses, order history, saved payment tokens or loyalty value.

Payment-page skimming

An unapproved script can capture payment data without changing the page a shopper sees.

Ransomware and disruption

A third party or admin account can become the path into stores, cloud systems and supply-chain operations.

Business-logic abuse

Coupon, refund, inventory and API actions can be abused even when the software has no known vulnerability.

The 2025 M&S incident disrupted online and store operations and was expected to reduce annual profit by about 300 million pounds. IBM's 2025 India study put the average cost of a data breach in India at 22 crore rupees. These figures are not a forecast for your business, but they show why security belongs with commerce leadership.[5,6]

Protect the business outcome

Fynd Secure connects a technical signal to the business context: which checkout flow, store, admin, customer group or order process could be affected.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

India rules, explained simply

Know the clock before an incident starts

The right preparation is a clear incident process, retained evidence, and a human owner for every notification.

Rule or standard	What it means in plain words
CERT-In Directions	Covered entities report specified cyber incidents within six hours of noticing them, keep ICT logs securely for a rolling 180 days in India, and synchronise clocks to a trusted time source.
DPDP Rules 2025	The Rules were notified on 13 November 2025. Security safeguards and the breach process in Rules 6 and 7 apply from 13 May 2027. Tell affected people without delay, and send the Data Protection Board a detailed report within 72 hours.
DPDP Act	The maximum penalty for failing to take reasonable security safeguards to prevent a personal-data breach is 250 crore rupees.
PCI DSS 4.0.1	Requirements 6.4.3 and 11.6.1 address payment-page script inventory, approval, integrity and detection of unauthorised changes.
Global expectations	GDPR uses a 72-hour supervisory-authority window where feasible. SOC 2 and ISO 27001 are assurance and management frameworks, not replacements for incident law.

The DPDP Rules phase obligations in over time. A rule being notified is not the same as every obligation being enforceable today. Your counsel should map the exact scope, role and date for your business, including any RBI or SEBI requirements.[7,8,9,10,11,12,13]

This is a summary, not legal advice

Confirm obligations, reporting duties and deadlines with your counsel. Fynd Secure helps you prepare evidence and drafts. A human reviews and submits every regulator report.

How Fynd Secure works

Two ways in, one timeline out

Start with the Fynd properties you already run, then add the systems that make up the rest of your business.

Protect

1. Switch on the Guards

Turn on extra protection for storefronts, apps, checkout, APIs, OMS, Store OS devices, Kaily, Boltic and the Fynd console. There is nothing to install.

Command

2. Connect the estate

Add cloud, on-prem, SaaS, identity, endpoints and stores. Start read-only. Add response permissions only when you choose.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

You decide

3. Set the policy

Choose what agents can do automatically, what they can do with notice and undo, and what must wait for approval.

Everything lands in one command center and one incident timeline. Triage removes duplicate alerts. Investigator builds the story. Responder proposes or runs the next action. Compliance keeps the clock and evidence visible. You can ask questions in plain language instead of learning another security vocabulary.

- A single attack can be followed from storefront to identity, cloud, endpoint and store.
- Actions show who or what made the decision, why it was safe, and how to undo it where possible.
- New customers begin in shadow mode, so you see what would happen before enforcement.

The eight Fynd Guards

Protection for the paths attackers use

Each Guard covers a commerce surface and explains the control in words your team can act on.

Bot and abuse

Stops scraping, inventory hoarding, fake sign-ups, card testing and coupon abuse with behaviour scoring, device signals and targeted challenges.

Account takeover

Stops credential stuffing, password spraying and session hijacking with breached-password checks, velocity limits, OTP step-up and session binding.

Checkout integrity

Stops payment skimmers and changed payment-page scripts with an approved script inventory, tamper detection and a managed content security policy. Supports PCI DSS 6.4.3 and 11.6.1.

API shield

Stops API abuse, token theft and data scraping with schema checks, per-token rate limits and anomaly detection.

Admin and insider

Stops risky admin actions, bulk exports, price and coupon tampering with SSO, just-in-time access, allowlists and two-person approval.

Data vault

Reduces data leakage with field-level encryption, tokenisation, masking, customer-managed keys and consent and erasure records.

AI agent guard

Stops prompt injection, data leaks and tool misuse in Kaily and your agents with input and output filters, tool policies and scoped identities. Uses OWASP Agentic Applications guidance.

Store device guard

Stops tampered POS terminals, rogue apps and stolen store devices with health checks, app allowlisting and remote lock and wipe through Store OS.

Essentials is included for every Fynd customer

Essentials includes DDoS and edge protection, managed TLS, standard WAF rules, MFA for admin users, and a monthly security score. Protect adds the eight enterprise Guards and their deeper controls.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Connect your whole estate

Start read-only. Add response when ready.

Fynd Secure connects the systems that hold your business together without asking for broad permissions on day one.

Group	Examples	How it connects
Fynd properties	Storefront, app, checkout, APIs, OMS, Kaily, Boltic, console	Native. Nothing to install.
Clouds	AWS, GCP and Azure	Read-only roles first. Optional response permissions after you opt in.
SaaS and identity	Google Workspace, Microsoft 365, Okta and Entra ID	OAuth apps and API connectors.
On-prem	Servers, Active Directory, firewalls, VMware and ERP	Fynd Collector, a small virtual appliance that forwards logs securely.
Endpoints	Laptops and desktops	Your existing EDR, or one connected through Fynd.
Stores	Store OS devices, POS terminals and store networks	Native Store device Guard plus network logs through the Collector.

The first connection creates a shared view of assets, identities, permissions and data. That makes one attack visible across the estate. For example, a risky login in Microsoft 365 can be linked to a Fynd admin session, a cloud access change and a store device event instead of appearing as four unrelated alerts.

One attack, one story

You can connect a system without giving Fynd permission to change it. Response permissions are separate, explicit and logged.

AI agents, with you in control

Automation that shows its work

Eight focused agents share context, follow your autonomy policy and ask for approval when the blast radius is high.

Triage

Reads every alert, removes noise and groups related signals into one incident.

Investigator

Builds the full story: who, what, how and how far the activity spread.

Responder

Runs playbooks within policy and asks you when an action needs approval.

Fraud and bot

Watches shopper behaviour across storefront, app and checkout in real time.

Exposure

Finds misconfigurations, open services, risky permissions and attack paths.

Hunter

Searches for hidden attackers using fresh intelligence and shared attack patterns.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Compliance

Keeps evidence, tracks reporting clocks and drafts regulator reports.

Red team

Safely tests your estate and AI agents so weaknesses are found before an attacker finds them.

Level	What happens	Examples
Level 1, automatic	The agent acts within a narrow, reversible policy.	Block attack traffic, add a challenge, rate-limit a token, roll back a changed checkout script.
Level 2, automatic with notice and undo	The agent acts, tells you, and gives you a one-click undo.	Lock a compromised shopper account, rotate a leaked API key, end sessions, isolate one laptop.
Level 3, human approval	The agent shows the blast radius first. Critical actions need two approvers.	Disable an admin, isolate a production server, block a country, change cloud access roles.
Never automatic	Only a human can do it.	Delete data, pay or negotiate a ransom, turn off logging, or submit a regulator report.

New customers start in shadow mode for the first weeks. Agents show what they would have done without changing anything. Approvals can arrive in the Fynd Secure app or approved messaging channels on your phone. Ask Fynd Secure questions such as: Are we under attack now? What changed in checkout this week? Draft my board update.

Hard safety limits

Fynd's safety limits cannot be loosened. Every action has an explanation, a policy level and an audit record. You control the policy inside those limits.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

A real attack, end to end

Vastra & Co. keeps its festive sale open

This illustrative, fictional scenario shows how the Guard, agents and human approvals work together in six minutes.

Vastra & Co. is a fictional fashion brand. During a festive sale, attackers use credential stuffing against the shopper login. Fynd Secure sees the signal, confirms the pattern, protects shoppers, and then follows the same proxy pool into the admin path.

21:02:10 — **The spike starts**

Login failures jump from 40 to 9,000 a minute from 14,200 residential proxy addresses.

21:02:50 — **The pattern is confirmed**

Triage groups the alerts. 62% of tried passwords appear in known breach lists.

21:03:05 — **Low-risk actions run**

A challenge and OTP step-up are added to risky logins. The proxy network is blocked at the Fynd edge.

21:04:30 — **Accounts are protected**

312 accounts that logged in before the block are locked. Shoppers are asked to reset passwords and saved payment tokens are frozen.

21:05:40 — **The trail widens**

Hunter links the same proxy pool to three other Fynd brands and to an admin login at Vastra two days earlier.

21:06:10 — **The high-impact action waits**

A request to suspend the admin and rotate six API keys is sent to two approvers on WhatsApp and the app. The blast radius is shown first.

21:08:05 — **Two people approve**

Responder completes the action in 40 seconds. The attack is contained in six minutes with zero checkout downtime.

21:20 — **The human reporting step begins**

CERT-In and DPDP drafts are ready for review. The agents do not submit them.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

40 sec
to detect the credential-stuffing pattern

6 min
from first signal to containment

0 min
checkout downtime during the sale

Illustrative scenario

The Vastra & Co. story is a fictional example based on the live demo. Results in a real incident depend on the signals available, your policy and the decisions your team makes.

Compliance built in

Evidence ready when the clock starts

Fynd Secure helps your team keep the evidence, track the deadline and prepare the report without handing the decision to an agent.

Clocks

See the CERT-In six-hour clock, DPDP 72-hour detailed-report clock and other customer-defined deadlines in the incident view.

Evidence

Keep the relevant logs, decisions, affected systems, actions and approvals together with the incident.

Drafts

Generate a plain-language CERT-In, DPDP or customer notice draft for a human to check, edit and submit.

Framework mapping

Map evidence and controls to CERT-In, DPDP, PCI DSS, ISO 27001 and SOC 2 expectations.

- India logs can be retained for the 180-day CERT-In requirement when that option is selected.
- Payment-page script checks support PCI DSS 4.0.1 requirements 6.4.3 and 11.6.1.
- The command center shows what is covered, what is missing and who owns the next task.
- Fynd Secure is designed to help you meet obligations. It is not a legal opinion, audit report or certification.

Human review stays mandatory

Agents prepare the facts and drafts. Your authorised people confirm accuracy, decide whether to notify, and submit reports to regulators.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Trust and data

Useful context without giving up control

Fynd Secure is designed to make security data useful while keeping access narrow, actions explainable and customer policy in charge.

India by default

Customer data is stored in India, Mumbai by default. Data location options are discussed for your estate and contract.

Least privilege

Connections start read-only. Response permissions are optional, scoped and logged.

Encryption and isolation

Data is encrypted in transit and at rest, with customer-managed key options and tenant isolation.

Explainable action

Every agent action shows the evidence, policy level, reason, blast radius and audit record.

Your policy

You choose autonomy levels inside Fynd's hard safety limits. You can export your data and review access.

Shared learning, not shared data

Threat signals can be anonymised for cross-brand protection. Shopper and customer personal data is not shared as threat intelligence.

Fynd Secure is built to support security, privacy and compliance work. Fynd Secure does not by itself make your organisation compliant, and no claim is made here that Fynd holds a certification. Confirm controls, data flows, retention and contractual terms with your counsel and auditor.

The simple promise

You should always be able to answer three questions: What happened? What did the system do? Who approved the next step?

Plans

Start with protection, expand when ready

Choose software, managed service, or a path from one to the other. Pricing is shared in a conversation with Fynd and depends on usage.

Included

Essentials

For every Fynd customer: DDoS and edge protection, managed TLS, standard WAF rules, MFA for admin users and a monthly security score.

Fynd properties

Protect

The eight Fynd Guards for storefronts, apps, checkout, APIs, OMS, Store OS devices, Kaily, Boltic and the Fynd console.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Whole estate

Command

The AI command center across clouds, on-prem, SaaS, identity, endpoints and stores, with eight agents, exposure management and compliance automation.

Fynd team

Managed

Fynd's 24×7 security team behind the agents, with monitoring, threat hunting, incident support and reporting assistance.

Optional add-ons include brand protection and takedowns, continuous AI red teaming, endpoint protection licences, email and collaboration security, deepfake and impersonation drills, third-party risk monitoring, and cyber insurance through partners. Availability depends on region and rollout phase.

No public price list

Pricing is shared in a conversation with Fynd and depends on the properties, assets, data volume, retention and service level you choose.

Getting started

Early access, in phases during 2027

Start with what runs on Fynd, learn what the agents see, then expand into the rest of your estate.

1 **Request access**

Tell us about your Fynd properties, stores, security team and the systems you want to connect.

2 **Have a discovery call**

Agree the first Guard set, data location, owners, reporting needs and response boundaries.

3 **Connect read-only**

Start with native Fynd signals and read-only connections. Add the Fynd Collector for on-prem systems if needed.

4 **Run in shadow mode**

Review findings and see what each agent would do before any enforcement action.

5 **Switch Guards to enforce**

Turn on the controls that fit your business, with clear owners and a rollback path.

6 **Set your autonomy policy**

Choose automatic actions, notice and undo actions, approval actions and human-only actions.

Fynd Secure is in early access and will roll out in phases during 2027. Protect comes first, followed by Command, then Managed. Features, connectors and service coverage may change as the rollout progresses.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Request early access

Use Get early access on the Fynd Secure website, or ask your Fynd account team. We reply within one working day.

Try the live demo

Open the live demo from the Fynd Secure website. It runs on sample data, so you can approve actions and simulate attacks safely.

Frequently asked questions

Straight answers

The most common questions from leaders evaluating Fynd Secure.

Do we need to install an agent on Fynd properties?

No. Fynd Guards are native to the Fynd properties you already run. For systems outside Fynd, the connection method depends on the source. On-prem systems can use the Fynd Collector virtual appliance.

Can we connect AWS, GCP and Azure without giving response access?

Yes. Connections start with read-only roles. Response permissions are optional and can be scoped to the actions and systems you approve.

Will the AI agent make changes without our approval?

Only for actions your autonomy policy allows at Level 1 or Level 2. Level 3 actions wait for approval and show the blast radius first. Deleting data, turning off logging and submitting regulator reports are never automatic.

What happens if the agent is wrong?

Every action includes its evidence and reason. Level 2 actions include a one-click undo where possible. Shadow mode lets you test the policy before enforcement, and hard safety limits restrict what agents can do.

Can Fynd Secure replace our existing EDR or SIEM?

It can connect to existing EDR and security tools and bring their signals into the same timeline. Whether you replace a tool depends on your coverage, contracts and operating model.

Does Fynd Secure guarantee compliance?

No. It is built to support your compliance work by collecting evidence, mapping controls and drafting reports. Your organisation remains responsible for its obligations, decisions and submissions.

Where is our data stored?

Customer data is stored in India, Mumbai by default. Discuss data location, retention, encryption keys and any cross-border flows with Fynd during the discovery process.

Can a human review every regulator report?

Yes. Agents can prepare CERT-In, DPDP and customer-notice drafts, but an authorised human must review, decide and submit them.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

How does Fynd learn from attacks on other brands?

Fynd Secure can use anonymised indicators such as attack patterns and infrastructure signals to improve cross-brand protection. It does not share shopper or customer personal data as threat intelligence.

When can we buy Fynd Secure?

Fynd Secure is in early access. Rollout is planned in phases during 2027: Protect first, then Command, then Managed. Request access on the Fynd Secure website or through your Fynd account team.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

References

Sources for the facts in this guide

Publisher sources used for the threat, retail and regulation facts cited throughout the guide.

Reference numbers appear next to the relevant facts. Product descriptions, plans and illustrative scenarios are Fynd Secure product information and are not external claims.

1 CrowdStrike, 2026 Global Threat Report, 2026
https://www.crowdstrike.com/en-us/global-threat-report/

2 Anthropic, Disrupting the first reported large-scale AI-orchestrated cyber espionage campaign, 13 November 2025
https://www.anthropic.com/news/disrupting-AI-espionage

3 World Economic Forum, How deepfakes are fuelling cybercrime, 4 February 2025
https://www.weforum.org/stories/emerging-technologies/deepfake-ai-cybercrime-arup

4 Imperva, 2025 Bad Bot Report, 14 April 2025
https://www.imperva.com/blog/2025-imperva-bad-bot-report-how-ai-is-supercharging-the-bot-threat/

5 BBC, M&S cyber attack expected to cost about 300 million pounds, 10 June 2025
https://www.bbc.com/news/articles/c0el31nqnpvo

6 IBM India, India records highest average cost of a data breach, 7 August 2025
https://in.newsroom.ibm.com/2025-08-07-India-Records-Highest-Average-Cost-of-a-Data-Breach-IBM

7 CERT-In, Directions under section 70B of the Information Technology Act, 28 April 2022
https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

8 Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 13 November 2025
https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

9 Ministry of Electronics and Information Technology, Digital Personal Data Protection Act, 2023
https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

10 PCI Security Standards Council, Important updates for merchants validating to SAQ A, 30 January 2025
https://blog.pcisecuritystandards.org/important-updates-announced-for-merchants-validating-to-self-assessment-questionnaire-a

11 European Union, General Data Protection Regulation, 27 April 2016
https://eur-lex.europa.eu/eli/reg/2016/679/oj

12 AICPA, System and Organization Controls SOC suite of services, undated, accessed November 2026
https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

13 International Organization for Standardization, ISO IEC 27001:2022, October 2022
https://www.iso.org/standard/27001

14 OWASP GenAI Security Project, Top 10 for Agentic Applications for 2026, 9 December 2025
https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Fynd

Fynd Secure

Get early access

Protect your Fynd properties first. Then bring the rest of your estate into one command center.

Request access on the Fynd Secure website, or ask your Fynd account team.

Try the live demo on the same site. It runs on sample data, so press anything.

fynd.com

© 2026 Shopsense Retail Technologies Limited. All rights reserved.