Fynd

Insights

Commerce After Free

A three-part series by Farooq Adam on what changes when AI makes software nearly free: why companies still struggle to change, why every change opens new doors to attackers, and what to demand of the partners who lead the change.

Farooq Adam, Founder of Fynd

1 If Software Were Free, Would Anyone Change?
2 The Attack Surface of Change
3 Choose Partners Who Can Defend and React

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Fynd

Insights · Commerce After Free · Article 1 of 3

If Software Were Free, Would Anyone Change?

AI is taking the cost of software toward zero. That will not transform Indian business on its own. The real limit is how much change a company can absorb.

Farooq Adam, Founder of Fynd

3 November 2026 · 4 min read

The true ceiling on adoption is not what customers can pay. It is how much change they can absorb.

1 The Free Test

Here is a simple test for any product. If it were free, would demand become infinite?

Palmer Luckey, who built the Oculus headset, applied this test to virtual reality. The answer was no. Make the headset free, and most people still stop using it within weeks. Make a ticket to the moon free, and most of us still stay at home. The price goes to zero. The cost does not. Risk, effort and fear remain.

This question matters now because AI is doing to software what the internet did to information. A screen that took a team three months to build now takes an afternoon. A workflow that once needed a vendor and a long contract now needs a clear description of what the business wants. Software is on its way to becoming nearly free.

If price were the thing that held companies back, every retailer, distributor and manufacturer in India would transform this year. They will not. A retailer does not rebuild itself because a licence became cheaper. A factory does not change its floor because code became free. Something else is in the way.

After more than a decade of building commerce technology for Indian and global businesses, I see six things in the way. The first is risk: if the store stops, someone takes the blame. The second is the cost of change: the software is cheap, but retraining people and rewiring old systems is not. The third is imagination: many leaders do not know what to ask for. The fourth is proof: nobody wants to go first. The fifth is ownership: if nobody inside the company wins when the project works, nothing moves. The sixth is bandwidth: an organisation can absorb only a few big changes in a year.

The true ceiling on adoption is not what customers can pay. It is how much change they can absorb.

2 What Commerce Will Look Like in 2027

The gap between free software and slow adoption will define the next two years of commerce. Several shifts are already visible.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

The customer will often be an AI agent. A growing share of shopping will start with an agent that compares, negotiates and buys on behalf of a person. That agent does not see a banner. It reads product data, prices, promises and return policies. Brands whose data machines cannot read will not be found.

The storefront will dissolve. Commerce is moving into chat, voice, video and agents. The website becomes one surface among many, and every surface needs the same truth about product, price and stock.

Dashboards will give way to actions. Instead of training managers to read reports, systems will propose specific actions: move this stock, change this price, fix this display. The manager accepts or rejects. Each decision teaches the system.

Customers will pay for outcomes, not logins. When software is nearly free, nobody pays for a seat. Businesses will pay for orders delivered, margin gained and stock-outs avoided.

The store and the factory will move closer to the customer. Every store becomes a warehouse, a showroom and a returns point at once. Demand signals will reach the factory floor in hours, not seasons, and production runs will get smaller.

Content will become infinite, and trust will become scarce. Every product and every customer will get its own images, video and copy. When machines write the content and agents do the buying, verified data and guaranteed outcomes become the premium.

In every one of these shifts, the technology is the easy part. The hard part is the change.

3 Abundance Moves the Scarcity

When software, content and intelligence are nearly free, value moves to what is still scarce: trust, attention, judgment, deep knowledge of a domain, and the human capacity to change.

This changes what businesses should ask of their technology partners. The question is no longer “How cheap is your software?” It is “How much change can you help me absorb, safely?” The partner who does the integration, takes the outcome risk and makes the future visible will matter more than the partner with the lowest price.

There is one more scarce thing that most boardrooms are not yet discussing: security. Every change a company makes in the AI era also opens a new door for attackers who now use AI themselves. That is the subject of my next article.

Price is not the problem. Fear, effort and imagination are. The companies that win this decade will be the ones that remove all three.

Farooq Adam is the Founder of Fynd.

Sources

Palmer Luckey, “Free isn’t Cheap Enough”, 30 October 2018.
https://palmerluckey.com/free-isnt-cheap-enough/

The series

1. If Software Were Free, Would Anyone Change? · current
2. The Attack Surface of Change
3. Choose Partners Who Can Defend and React

Read the series online at secure.fynd.space/insights

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Fynd

Insights · Commerce After Free · Article 2 of 3

The Attack Surface of Change

Attackers now use AI to do most of their work. Every company that transforms with AI opens new doors. Boards must treat security as part of the change, not something added after it.

Farooq Adam, Founder of Fynd

3 November 2026 · 3 min read

What new door does this change open, and who is watching it?

1 The First AI-Run Attack

In September 2025, Anthropic detected something new. A state-sponsored group had turned an AI coding agent into an attack team. The AI ran reconnaissance, wrote exploit code, harvested credentials and pulled out data. It went after about thirty organisations around the world: technology companies, banks, chemical manufacturers and government agencies. A small number of attacks succeeded. By Anthropic's estimate, the AI did 80 to 90 percent of the work. Humans stepped in only at a few decision points.

Anthropic called it the first documented case of a large-scale cyberattack executed without substantial human intervention. It will not be the last.

2 The Attacker's Cost Is Falling Too

In my previous article, I argued that AI is taking the cost of software toward zero. The same is true for attacks. A campaign that once needed a skilled team for months now needs a few operators and an AI agent. Verizon's 2026 Data Breach Investigations Report found that exploited software flaws are now the most common way in, at 31 percent of breaches, for the first time in the report's 19-year history. It also found that AI is shrinking the time defenders have to fix a flaw from months to hours.

India is not a spectator. CERT-In handled more than 29.44 lakh cyber incidents in 2025. IBM's 2026 study puts the average cost of a data breach in India at a record ₹25.5 crore, up 15.9 percent in one year. The same study found that 26 percent of malicious breaches in India were AI-generated.

3 Transformation Widens the Door

Here is the part most boardrooms miss. The attack surface is not only growing because attackers are better. It is growing because of the changes we are making.

Every transformation project adds new doors. An AI agent that can place orders is also an agent that can be tricked into placing the wrong ones. A system that writes its own code can also write a flaw. A new integration between the store, the warehouse and the ERP is also a new path from the internet to the core of the business. Each new supplier connection is another way in: Verizon found that a third party was involved in 48 percent of breaches.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

There is also the AI nobody approved. Verizon reports that the share of employees who use AI tools often rose from 15 percent to 45 percent in one year. IBM found that unapproved "shadow AI" added ₹1.79 crore on average to the cost of a breach in India where it was present.

So every company has two estates to defend. The **existing estate** is the old ERP, the point-of-sale systems in thousands of stores, the factory controllers and the vendor links that were never designed for this threat. The **future estate** is the AI agents, the generated software, the new data flows and the machine customers. Attackers will look for the seam between the two.

4 Security Is Part of the Change

The old habit was to build first and secure later. That habit was costly before. Now it is dangerous, because attackers move at machine speed and an AI agent can do a great deal of damage in the hours before a human notices.

The good news is that the same technology helps defenders. IBM found that Indian companies that used AI and security automation extensively paid ₹21.3 crore per breach on average, against ₹31.6 crore for those that did not. Defence that runs at machine speed is now possible. It must be designed in from the first day of the project, not bolted on after the launch.

For a CEO, this changes the transformation plan. The question is no longer only "What will this change give us?" It is also "What new door does this change open, and who is watching it?"

In my next article, I will set out what businesses should demand of the partners who lead them through this change.

Farooq Adam is the Founder of Fynd.

Sources

Anthropic, "Disrupting the first reported AI-orchestrated cyber espionage campaign", 13 November 2025.
https://www.anthropic.com/news/disrupting-AI-espionage
Press Information Bureau, Government of India, "CERT-In: India's Frontline Defender against Cyber Threats", 23 January 2026.
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2217537&lang=1&reg=3
IBM India, "India Records its Highest Average Cost of a Data Breach 2026", 3 August 2026.
https://in.newsroom.ibm.com/India-Records-its-Highest-Average-Cost-of-a-Data-Breach-2026
Verizon, 2026 Data Breach Investigations Report, 19 May 2026.
https://www.verizon.com/about/news/breach-industry-wide-dbir-finds

The series

1. If Software Were Free, Would Anyone Change?
2. The Attack Surface of Change · current
3. Choose Partners Who Can Defend and React

Read the series online at secure.fynd.space/insights

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Fynd

Insights · Commerce After Free · Article 3 of 3

Choose Partners Who Can Defend and React

In the AI era, a technology partner must do more than ship software. It must carry the change, protect the old estate and the new one, and respond at machine speed when something goes wrong.

Farooq Adam, Founder of Fynd

3 November 2026 · 3 min read

Software is becoming free. Change is not. Safety is not. Choose the partner who can deliver both.

1 Two Arguments, One Conclusion

In the first two articles of this series, I made two arguments. First, free software will not transform a business on its own. The real limits are risk, the cost of change and a lack of imagination. Second, every change a company makes with AI also opens new doors to attackers who now use AI themselves.

Put these together and one conclusion follows. The most important decision in a transformation is not which software to buy. It is which partner to trust with the change.

2 The Old Way of Choosing

For twenty years, enterprises chose technology vendors with a familiar list: features, price, references, the quality of the demo. Security was a questionnaire that procurement sent near the end. The vendor shipped the software, and the customer's team owned everything after that.

That model does not survive the AI era. When software is nearly free, features and price stop separating one vendor from another. When attackers move at machine speed, a questionnaire at the end protects nobody. And when the hard part of a project is the change itself, a vendor that hands over the code and leaves has handed over the risk.

3 Five Questions to Ask a Partner

I suggest that every board ask five questions before it chooses a partner for AI transformation.

Will you own the change, not only the code? The partner should do the integration with the old systems, redesign the process and stay accountable for the result. A partner that is paid for outcomes has every reason to make the change succeed and to keep it safe.

Can you secure the estate I already have? Most attacks will not come through the shiny new AI system. They will come through the old ERP, the store devices, the factory controllers and the supplier links. A good partner maps these, closes the gaps and watches them, before it connects anything new.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

Is security designed into the future estate from day one? AI agents need limits on what they can do, which data they can see and which actions need a human to approve them. Generated code must be tested before it runs. Every new integration needs an owner and a log. Ask to see how this is built, not only a policy document.

Do you understand how AI is used to attack? Prompt injection, AI-written phishing, deepfake voices, automated scans that find a flaw within hours of its release. A partner that has not studied these will not defend against them. Ask what they saw last quarter and what they changed because of it.

When something goes wrong, how fast do you react, and who answers the phone? Breaches will happen. What matters is detection in minutes, containment in hours and a clear plan for who does what. The partner must be able to switch off an agent, roll back a change and keep the business running while the problem is fixed.

4 Trust Is the Product

In my first article I wrote that, when software becomes abundant, value moves to what is still scarce. Trust is the scarcest of all. A customer will let an AI agent buy for them only if they trust it. A retailer will let a system change prices in a thousand stores only if it can see, approve and reverse each change. A board will approve a transformation only if it believes the company will be safer at the end, not more exposed.

This is why the partners who win this decade will be different from the vendors who won the last one. They will carry the change. They will defend both the estate you have and the estate you are building. They will react at machine speed when it matters.

Software is becoming free. Change is not. Safety is not. Choose the partner who can deliver both.

Farooq Adam is the Founder of Fynd.

The series

1. If Software Were Free, Would Anyone Change?
2. The Attack Surface of Change
3. Choose Partners Who Can Defend and React · current

Read the series online at secure.fynd.space/insights

© 2026 Shopsense Retail Technologies Limited. All rights reserved.