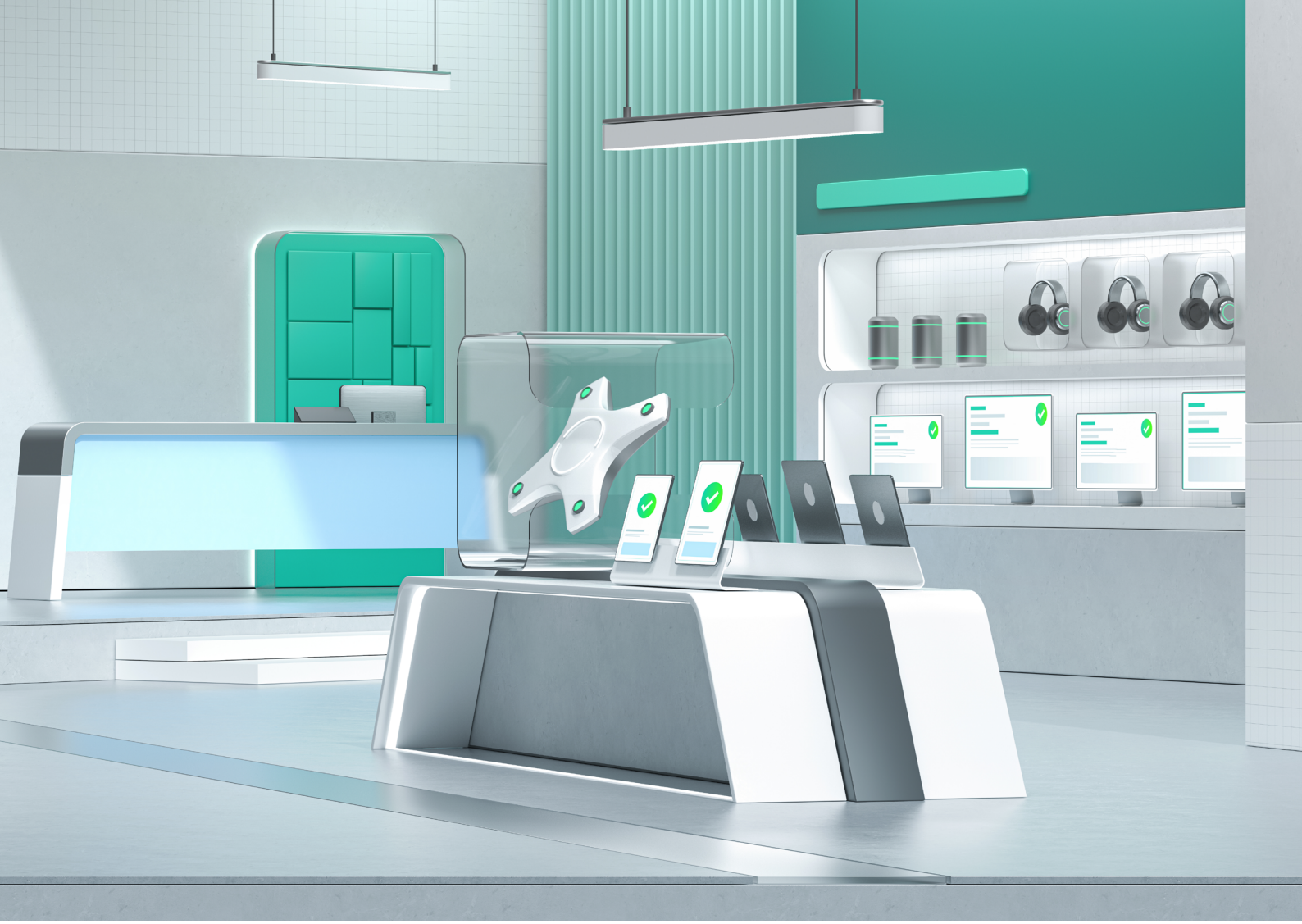


Building a safer future in Retail

kaspersky BRING ON THE FUTURE

go.kaspersky.com/retail 2021

Introduction

If you're a retail leader reading this in 2021, you are automatically a hero.

There is no industry on this planet that has used technology so effectively, and taken such control and command over its destiny, as the retail sector. None at all.

Not only did you **make it**, but you made it yours.

Conditions were far from ideal – not for employees, and not for businesses. Retail sits alongside hospitality and travel as the industries most heavily impacted by public health restrictions.

But we think it's time to turn away from examining our wounds, or trying to piece together what has happened to us.

Everyone is still talking about how we have been 'forced' to evolve and transform. We're not going to do that in this paper. Not because those are clichés, but because they assume that retailers are in a passive position – victims of circumstance. That's not what we see when we look at the way the industry has used technology to transform.

We feel similarly about the term, 'the new normal.' If retail pundits think that the 'normal' was never 'new' before 2019, they haven't been paying attention. And besides, we're not interested in 'normal' – we're interested in momentum.

Are you ready?

That's kind of a complicated question. Ready for what? How can you be ready for a future that cannot be fully scoped?

Most analysts will say that the retail industry was already planning to implement the technologies that have helped it master the tide of the pandemic. The difference was the length of the road map. Five years of digital transformation compressed into 5 weeks, is a common formulation.

But who is to say that this compression (from marathon to sprint) led to an inferior result than the slower timelines envisioned in retail C-suites across the globe? Forgive the platitude, but **necessity is the mother of invention**. And isn't evolution at speed part of the very definition of agile and lean methodologies?

Just do it

These three words helped Nike raise its North American market share from 18% to 43% between 1988 and 1998. It's not just a contender for the most effective slogan of all time – it's also excellent advice. And it's advice that the retail industry took from the very beginning of the pandemic.

The fact that you might have achieved 5 years of digital transformation in 5 weeks should be celebrated – not simply because you achieved it, but because it took place in the leanest, most agile, most focused way possible. Leading, we believe, to a far more positive and effective result.

In this paper you'll find a rundown of the key technology trends that retailers will be turning to within the next 5 seconds to 5 years (and probably are already). We're not plucking anything out of thin air here – everything is based on the best industry research available. If we're talking about it here, it's relevant. This is not sci-fi, not speculation, and we'll do all we can to avoid hype (even though it's exciting).

For every new tech trend we celebrate, we're going to look at how you can use it securely. It's 2021 and we don't believe that anyone – individual, business, or sector – should have to hesitate to adopt essential technologies because of security concerns. That's our business.

Store Inventory Management (SIM)

Digital Supply Chain Transformation

Mixed Reality

Payments

Retail Analytics – AI and algorithmic

Agile Marketing

Trend #1: Store Inventory Management (SIM)

SIM is new to the Gartner Hype Cycle for 2021, with a benefit rating of 'Transformational' and penetration sitting between 5% and 20%. With the pandemic so impressively boosting the rate of online fulfilment growth, SIM is essential for retailers, helping to achieve key business goals, including:

- Meet demand for multiple fulfilment nodes (including curbside, BOPIS)
- Reduce the impact of Inventory on COGS
- Leverage real-time data to make smarter planning decisions
- Reduce the cost of e-commerce fulfilment
- Cut excess inventory load
- Improve employee efficiency in-store and in the warehouse
- Empower true unified commerce by joining the dots between 'brick' and 'click'

When we talk about Store Inventory Management, we're talking about far more than just one technology. It's a complex ecosystem of tech that incorporates IoT, Smart Shelf, Unified Commerce, Smart Check-Out, algorithmic planning, supply chain autonomy, Store-Based Microfulfillment Centers (MFCs), and more.

Perhaps the best way to summarize SIM (and its impact) is by focusing on the value of 'real-time accuracy.' Without this, Unified Commerce (for example) is impossible – the best you can hope for is a sector with two very divergent loci – one online, and one in-store – each desperately trying, and failing, to connect with the other.

Some estimates suggest that traditional store inventory accuracy is as low as 70%. That might work when your business is purely 'brick,' but it won't cut it for 'click' and certainly not for fulfilment nodes that customers now expect, like BOPIS.

How to use SIM securely

In order to leverage maximum ROI on your SIM adoption, you'll need to share sensitive data with your provider. After customer data, your inventory data is a top priority for extra-careful treatment. An attack could expose your stock levels, sales performance, the location of your stock, and any plans you may have for future seasons. The risks are further compounded if you're integrating SIM functionality with customer data to make personalized suggestions, for obvious reasons. The high-profile attack on DSW (Designer Shoe Warehouse) in 2020 proves how critical it is that retailers use SIM technology securely. During a ransomware attack on one of DSW's vendors, the retailer's CEO reported that they "effectively lost a portion of our digital sales capabilities for two weeks during our crucial September selling season."

Suggestions:

- Order regular security audits, or choose a cybersecurity provider that includes these as part of their offering.
- Adopt the mantra of NIST's 2020 Cybersecurity Awareness Month – "If you connect IT, protect IT." While your SIM provider may hold and process your sensitive data, the IoT sensors you're using to manage inventory are on your premises, and under your control. Make sure you have access to IoT-ready cybersecurity functionality.
- Accept that attacks on third party providers are a certainty, and plan for the possibility that your SIM provider will be attacked – by ensuring you have a rigorous Incident Response system in place.

Trend #2: Digital Supply Chain Transformation

According to Gartner, "nearly all retailers are planning to invest to make their supply chains more agile (96%) and resilient (90%) by 2022." This comes as no surprise – the traditional supply chain model just won't cut it anymore.

It's not only the pandemic that has encouraged retailers to focus on Digital Supply Chain Transformation. The need for a more flexible, lean, responsive, and integrated alternatives to old models was already clear. Multiple fulfilment nodes were already a gaining pace before 2020.

Making a success of Digital Supply Chain Transformation means building a bespoke ecosystem of trusted third-party platforms and providers, to meet the unique needs of your retail business. While many retailers are committed to developing an autonomous supply chain, it's not something that can be done with purely in-house proprietary technology. This reliance on an ecosystem of providers is not unique to Supply Chain, and it's certainly not unique to the retail sector. But, as with any situation where we rely on an external party to meet our needs, it means we have to consider those relationships diligently.

BlueYonder, a Gartner leader in Warehouse Management Systems, has its slogan on point: "Fulfill your potential," promising a supply chain that is 'automated, orchestrated, intelligent and predictive.'

Some words on a word: disruption

Disruption. Say it aloud. Hear yourself say it.

What does it mean to you in 2021? What did it mean in 2019?

Your train doesn't arrive because of service disruption. Disruption is annoying.

Your entire business has to shut for months on end because of pandemic disruption. Disruption is devastating.

But what about the other side of disruption – the side that's been keeping your business leaping further and further into the future, long before 2021?

Technological disruption. We live for it. Pandemic aside, none of the technologies your retail business was engaging with before 2020 would have been possible without disruption:

- Personalization: from marketing through to products
- Voice technology: "Alexa, buy me toilet paper!" (easier said than done in March 2020)
- AI: from chatbots through to analytics
- Mobile: first shopping, then payments
- IoT: supply chain, video analytics, live inventory

Everything in the list above had to break through existing technologies and processes in order to proclaim its promise.
That's what disruption is.

So when we talk about the disruption brought by the worldwide pandemic, we have to focus on the iconoclastic revolutions that will bring previously unachievable revenue and efficiencies to the retail sector. This is not to diminish in any way the particular way that the retail sector has suffered due to seemingly endless lockdowns.
Not at all.

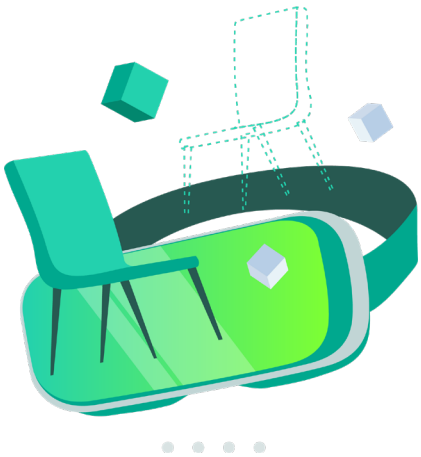
But we have a choice. Do we take ownership of that disruption and celebrate the inexorable momentum it's given the retail sector?
Or do we focus on its chaotic elements?

How to use Digital Supply Chain Technology securely

Digital transformations make every organisation a software company that relies on a multitude of external vendors, adding to difficult-to-manage third-party threats. It might be a sweeping statement, but when it comes to cybersecurity, it's true. Very few retailers (if any) will be in a position to develop their own private ecosystems, and will have to turn to external vendors in order to leverage the technology they'll need to thrive into the future. However, adoption is only the first step: it's those retailers that take the extra steps necessary to ensure they're using Digital Supply Chain technology securely will be the clear winners in the long run.

Suggestions:

- Establish a Vendor Risk Management policy and incorporate risk assessments as part of your third party software procurement processes.
- Use a cybersecurity solution that automates vulnerability scans and patching – and make sure your provider is always aware of any Zero-Day vulnerabilities.
- Make data visibility a priority – if sensitive data (including customer data) is sitting in the hands of one of your third party providers, you need to know about it.
- If you're using any kind of Hybrid Cloud infrastructure (and, let's face it, who isn't?), you'll need to understand the limits of the 'shared responsibility' security model. Even if your cloud service provider shares responsibility for data stored there, your first priority always has to be your own data – and your own bottom line.



Trend #3: Mixed Reality

Critics might be unconvinced about the new Space Jam movie, but watching LeBron James turn into a computer game character is a good way to appreciate the impact of Mixed Reality (MR). It's also proof that MR penetration goes far beyond the retail sector, and is an experience that consumers increasingly expect. Your customers are not only comfortable with MR, they're fluent in it.

The merging of AR, VR and the real world that Space Jam 2 represents is proof that MR is yet another example of a technology that was already inevitable for retailers, but whose adoption has been expedited dramatically by the pandemic.

However, pandemic market conditions mean that MR is about far more than just delighting customers with an experience. Just like contactless payments, MR also provides an opportunity for touchless interaction that is now an absolute must. And that's not all. MR empowers retailers to:

- Increase sales and conversion rates
- Reduce return rates (see 'bracketing' below)
- Build relationships with customers, through personalized suggestions
- Tailor products better (sometimes literally – by spotting size misalignments, for example)

The key use case of MR for retail is of course in virtual try-on technologies, such as those offered by platforms like 3DLOOK. And once again, fulfilling the promise of MR means that retailers must again make wise choices about the third party tech providers they engage with.

How to use Mixed Reality securely

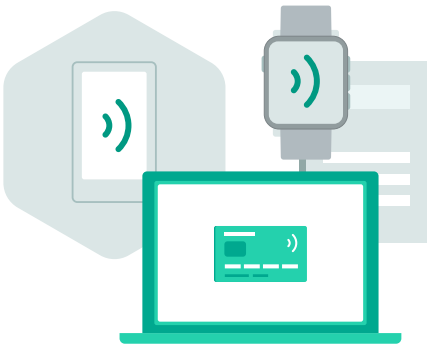
MR: overcoming the challenge of 'bracketing'

The new fitting room is the home, if consumer behavior is anything to go by. Bracketing is the now common practice of 'over-ordering,' with the intention to return any items that don't fit or don't suit. Great for consumers, not so great for retailers who carry the cost of returns. And, when it comes to returns, the growth of BORIS (Buy Online Return In Store) presents a clear example of the need to provide a unified commerce experience between brick and click.

The more immersive the virtual reality experience, the more urgent the need for businesses to use such technology securely. It's easy to see why this matters when it comes to Mixed Reality – after all, you're asking your customers to upload their own faces, bodies, or feet to a platform they trust and to mix that private imagery with images of your products. The platform they're trusting is yours, so the fact that a third party is providing the tech won't make a difference to your customers in the event of a breach. One obvious risk that comes with insecure application of MR is the wrath of regulators – but the picture is more complex than that. Firstly, it goes without saying that regulations vary by region, so it's important to be compliant with your consumers' environments wherever they may be. But the truth about technology regulations is that they are not always able to keep up with the rapid pace of development, leaving businesses forced to look beyond mere compliance in order to provide a secure MR service that consumers can trust.

Suggestions:

- Consider your consumers' **ethical** requirements in parallel with regulatory compliance. Don't just do the minimum viable security option as a box-ticking exercise, but go 'belts-and-braces,' and make it clear to your customers that you're going the extra mile to protect them.
- Remember that your customers will be using the MR functionality **on their own devices**, which lie outside your IT perimeter and could be subject to physical compromise. Choose a cybersecurity provider with industry- and region-specific Threat Intelligence, and the full ability to protect your business against new and unknown threats.
- Make **transparency** your MR watchword – you need to know exactly what's happening with your customers' data at all times – in their eyes, it's **your** reputation that's on the line, not the MR tech provider's.



Trend #4: Payments

Having already made a success of contactless payments (see below), retailers and regulators are making amazing efforts to leverage this – and other – payment technologies to carry the sector through pandemic conditions.

New frontiers include:

- Mobile PoS devices (projected CAGR of 18% between 2021 and 2027)
- Third Party Credit – such as Klarna
- Cashierless
- Biometrics
- Tokens
- Third Party Payment platforms, such as PayPal

Again, effective digital payments transformation necessarily brings retailers into contact with a broad range of third party technology providers. In the case of payments (rather than, say, MR), this partnership with third party providers doesn't only meet a technological need. It's also a business necessity – the only way to do away with friction and drop-out at the check-out.

The message of consumers is clear – "It's 2021, I shouldn't actually have to get my credit card out in order to buy something!" By careful adoption of third-party payment providers, retailers have a clear pathway to making it as easy as possible to make the purchase once they've reached sight of the finish line.

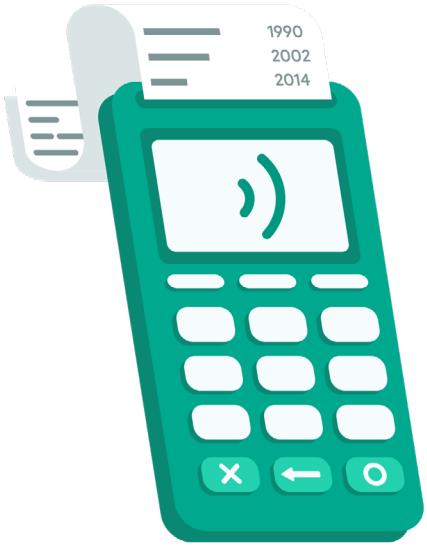
Don't touch me! How retail payments were already positively primed for social distancing

The retail industry was **already** ready for many of the conditions that the pandemic brought. Consider the case of contactless payments in-store.

This technology looks like it was **designed for social distancing**. A technology that allows us to participate in our lives as consumers and retailers without touching the PoS device. And not to put too fine a point on it, these devices can be (as the Daily Mail put it), 'as dirty as public toilets.'

Contactless technology might have been developed for speed, or to remove consumer friction (remembering PINs, having to swipe and sign). Nobody knew back in 2014 (the launch of Apple Pay) that contactless would be the standout social distancing pandemic-busting technology that it proved to be only a few years later.

Retailers, and government regulators, immediately leveraged the possibilities of contactless when the pandemic began. The UK raised payment limits from £30 to £45 in April 2020 (right after the beginning of the country's lockdown on 23rd March). A month later, contactless payments in the UK were up by 44%. A further increase is set for October 15th – with limits of £100.



A brief history of contactless payments

The technology has been available since the 1990s, mostly for specific use cases and merchants (such as gas stations). The joint development of the NFC standard between Phillips and Sony in 2002 opened up urgent possibilities for cross-sector and international adoption.

This led to a procession of key milestones in various regions and markets, and proved the technology's usefulness, and the demand for it.

To locate the global tipping point for contactless payments, we'd probably need to look to 2014 – the birth of ApplePay with the iPhone 6.

Today, Google Pay is available in 40 countries, and Apple Pay in 50. But this is just the beginning – wearables (and more) will follow, extending the liberation of the payment mechanism from the card to the phone and beyond.

Contactless payments prove that the retail sector is more than ready for the digital transformation momentum it is now mining. Readier than anyone outside the industry (or its IT leaders) can possibly imagine.

How to use new payments technology securely

As recently as September 30 2021, researchers discovered a deeply serious iPhone vulnerability that allowed EMV (Europay, Mastercard and Visa) payments to be taken, and contactless limits to be breached (up to £1,000) when the phone was locked and in transit mode. This discovery proved the vital role that security analysts and threat researchers have to play in protecting businesses and consumers alike from the potential cyber risks associated with payment technology. Payment technologies involving biometrics will require similar cybersecurity measures to those outlined in the Mixed Reality section above. Similarly, for retailers turning to external providers for the payment services their customers demand, we suggest looking at the section above on digital supply chain, for hints on how to prevent damage from attacks on third parties in your broader ecosystem.

Suggestions:

- Check that your business' legacy devices (including POS) are protected with appropriate Embedded Systems security technology – the payment software you adopt might not be optimized for any older devices you're still reliant on.
- Conduct regular Vulnerability scans and be absolutely sure that you have relevant Threat Intelligence integrated into your cybersecurity configuration as a matter of course.
- Put customer privacy at the top of your payments security agenda – any leaks of their personal financial data could be devastating for your reputation.
- Take the Payment Card Industry's advice regarding the Data Security Standard (PCI DSS): "PCI compliance is a continuous process," built around an ongoing loop of assessment, remediation and reporting.
- Make sure that any mobile payment devices can be encrypted remotely in the event of theft, loss or compromise.

Trend #5: Retail Analytics – AI and algorithmic

Data analytics is one case where both quantity and quality seem to matter almost equally. Without transforming their use of analytics through AI and algorithmic technologies, retailers will struggle to make real the promise of unified commerce, or supply chain and planning optimization.

The global Retail Analytics market is set to grow from USD 4.3 billion in 2020 to 11.1 billion by 2025. That's a CAGR of 21.2%.

What's different about retail analytics today? That's easy to answer: Algorithmic Retailing. In Gartner's words, "Algorithmic retailing connects big data to results, navigating a journey from descriptive to prescriptive analytics." That switch – from 'descriptive' to 'prescriptive' is one of the biggest changes ever to hit the sector.

From a cultural and organizational standpoint alone, the move towards a prescriptive analytics is hugely disruptive – in a good way. One challenge will be for retailers to attract and retain people who are capable of guiding them in their use of Algorithmic Retailing. It's highly specialized, and must be got right.

With Algorithmic Retailing, the industry finally has access to a technology that will power the IoT use cases (including Inventory) and leverage the potential of AI to new levels. Algorithmic Retailing is currently at 20% to 50% penetration, and a Gartner Benefit Rating of 'Transformational' – no surprise, given the possibilities of cross-business optimization and automation that it provides.

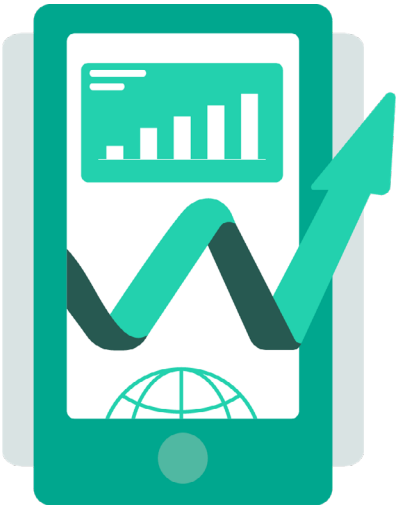
How to use retail analytics technology securely

Successful use of analytics – particularly its emerging AI and algorithmic iterations – requires that you have a sufficiently large (enormous) data set against which the system can test the algorithms it generates. Clearly, aggregating such data – and making it available to an algorithmic analytics system – presents a range of security and privacy risks that must be taken very seriously indeed.

At the same time, any fears about those risks could turn into a risk of their own – if competitors are more boldly adopting AI analytics and seeing profits soar above those of businesses that are more cautious.

Suggestions:

- Use highly proactive EDR functionality to seek out any threats before any breach can be attempted. Threat discovery is not always sufficient, and that's where threat hunting comes in.
- Build cybersecurity awareness training into your standard HR policies to make sure that your employees are empowered to become part of your attack-proof rampart. Even when relying on AI for analytics, there is no substitute for the work of properly trained human beings.
- Consider outsourcing a portion of your cybersecurity burden to a managed services provider to take advantage of highly specialized elite security expertise while liberating your IT staff to focus on tasks that absolutely require their attention.
- Make sure your security configuration and strategy takes a unified approach to the twin loci of your IT estate: your core operational infrastructure (e.g. endpoints) and the devices (e.g. POS) and sensors (IoT) that your business relies on.



Trend #6: Agile Marketing

The line between online and offline retail experiences is now blurred more than ever before, provoking questions that are both basic and highly complex. For example: where are your customers?

Traditional retail marketing – segmented (to varying degrees) by channel or fulfilment node, without significant overlap – is not fit for the world of Unified Commerce or Omnichannel.

You already know that your customers are here, there, and everywhere. The difference today is the speed with which they move between online and offline. And it's not just speed: customers expect that both worlds will operate in alignment and synergy.

Agile Marketing isn't about seeing the customer as a moving target (with your challenge being to 'hit' them while they move between worlds). Marketing – previously seen as a form of administrative function – now sits alongside the functions we typically imagine when discussing the other five trends in this paper.

Agile Marketing means extending the technological promise of AI and Algorithmic Retailing (for example) to prescribe marketing activities, and build automation into the process. There is no sense in leveraging technology to create omnichannel fulfilment or unified commerce, if the same technology does not both gather data from, and inform the activities of, the marketing function.

How to use Agile Marketing securely

Regulation of Agile Marketing

Ever since the EU's GDPR, the marketing function has been under pressure from regulators to protect customer privacy. It's not that the marketing function is the only one to deal with private customer data; but unlike the finance function, it hasn't always been accustomed to the pressures regulatory compliance. Technologies like MR will bring new levels of regulatory pressure to the marketing function. It's one thing to know a customer's name, email address and social handles, and quite another to have access to their behavior via technologies such as MR. Yet data gathered from MR (for example) is a source that marketing departments will not want to be without, particularly as the evolution towards agile approaches continues to accelerate.

Two words: Total Experience. The wonderful thing about the marketing department from 2021 onwards is that it is already in a perfect position to work with other functions in a truly 'joined up' way. The concept of Total Experience (an evolution of the principle that consumers don't buy products, they buy 'experiences') has been around for a few years now, but technologies such as MR and the extreme growth of mobile e-commerce have now made it a reality. The good news is that analysts, such as Gartner, recommend that Management Experience and Employee Experience must be unified with Customer Experience and User Experience. In short, shrewd marketing departments know that in order to deliver the Total Experience that customers now expect, they have to work in concert with other business departments – and that includes IT. That collaboration obviously works both ways, presenting new opportunities for cross-departmental understanding and cooperation – hopefully eliminating security and data siloes, and making it easier than ever to bring everyone on board with the company's security strategy and practices.

Suggestions:

- Build a highly cyber-positive culture in which all employees are encouraged to take pride in the role they have to play in keeping the business – and its customers – safe. Make cybersecurity skills training available as needed, and include security as a personal KPI for employees where relevant in annual appraisals.
- Always remember that even though AI-driven agile marketing tools such as Black Swan may hold immense promise for retail marketers, the role of the human being's gut instinct will continue to be a rich well of marketing inspiration, not to mention a crucial source of 'checks and balances' for the security of any automated marketing tool, no matter how agile.
- Bear in mind that the more AI you leverage for marketing activities, the more customer data you will necessarily have to expose. It's not worth forging ahead without appropriate cybersecurity measures to protect your customer's financial and other personal data. The rule is safety first, always. A short-term marketing win is not worth sacrificing your long-term reputation.

Summary

In 2020, the retail sector managed to compress about 5 years of digital transformation into the space of just a few weeks, proving itself as a true agility leader among industries. As we move towards the end of 2021, the task is to build on that heroic momentum, consolidating gains, and taking even greater strides forward into the immense possibilities offered by innovative retail technologies. As always, retailers must have total confidence that their digital transformation is secure. The good news is that Kaspersky can help you evolve and adapt to whatever tomorrow brings, by making it easy to protect your business – and your customers – while transforming boldly, and confidently into the next decade and beyond.

Helping global retailers transform means offering solutions that fit. While all retailers are heroes, no business is alike. We meet our retail clients right where they are, placing business continuity and fear-free innovation first at all times.

Everything we do is backed by Kaspersky's legendary Threat Intelligence; fortifying our enduring quest to protect data, customers, and business continuity 24/7 against advanced threats and targeted attacks.

Browse Kaspersky's perfectly engineered enterprise portfolio to find award-winning solutions and services that will help you innovate without putting your business (or your customers) at risk. To help you find the perfect fit, we've organized our portfolio into a step-by-step framework. Because wherever you are in your innovation journey, Kaspersky will help you push boldly into tomorrow with total conviction.

Kaspersky's step-by-step cybersecurity approach

1

Kaspersky Security Foundations – essential core of cloud-based, automated protection for all devices, VDI and hybrid server infrastructures, before organizations advance seamlessly to ...

2

Kaspersky Optimum Security - for organizations requiring more specialized security against new and evasive threats, before effortlessly implementing our third tier ...

3

Kaspersky Expert Security – for organizations with established mature IT security teams combatting the most complex targeted attacks.

Cybersecurity maturity level	Solution
IT Smaller organizations without a specialized IT security team	**What** **Kaspersky Security Foundations** **How** Implement fundamental security for organizations of any size and infrastructure complexity, delivering cloud-managed automatic prevention of commodity cyberthreats on any devices, VDI and hybrid server infrastructures. ▸ **Endpoints:** Protect every endpoint in your organization with **Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security** ▸ **Cloud:** Benefit from borderless security with **Kaspersky Hybrid Cloud Security** ▸ **Network:** Secure your perimeter with **Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway** ▸ **Data:** Safeguard valuable and sensitive data with **Kaspersky Security for Storage** ▸ **Security Management:** Access expertise with **Kaspersky Premium Support; Kaspersky Professional Services**
IT security Organizations in need of advanced defenses, but with limited specialist IT security resources	**What** **Kaspersky Optimum Security** **How** Combat evasive threats with effective endpoint detection and response and continuous security monitoring – but without prohibitive costs or complexity ▸ **Advanced detection:** Boost ML behavior analysis, sandboxing, threat intelligence and automated threat hunting* with **Kaspersky Sandbox, Kaspersky Threat Intelligence Portal and Kaspersky Managed Detection and Response Optimum** ▸ **Analysis and investigation:** Enhance threat visibility and simplified investigation process with **Kaspersky Endpoint Detection and Response Optimum** ▸ **Rapid response:** Deploy automated in-product response options, as well as guided and managed response scenarios* with **Kaspersky Endpoint Detection and Response Optimum and Kaspersky Managed Detection and Response Optimum** ▸ **Security awareness:** Equip employees with automated tools at all levels and develop key cybersecurity skills with **Kaspersky Security Awareness Training** *Supported by Kaspersky experts

Mature and fully formed IT security team and/or dedicated SOC

- Have a complex and distributed IT environment
- Are a highly likely target for complex and APT-like attacks
- Have a low risk appetite due to high costs of security incidents and data breaches
- Are concerned about regulatory compliance

What

Kaspersky Expert Security

How

Complete mastery over the most complex and targeted cyberattacks

- **Equipped:** Equip your in-house experts to address complex cybersecurity incidents. Benefit from a unified cybersecurity solution. **Kaspersky Anti Targeted Attack Platform with Kaspersky EDR** at its core empowers your team with XDR capabilities.
- **Informed:** Enrich your knowledge pool with threat intelligence and upskill your experts to deal with complex incidents:
  - Integrate actionable, immediate threat intelligence into your security program. **Kaspersky Threat Intelligence** gives you instant access to technical, tactical, operational and strategic threat Intelligence.
  - Develop your in-house team's practical skills, including working with digital evidence, analyzing and detecting malicious software, and adopting best practices for incident response, with **Kaspersky Cybersecurity Training**.
- **Reinforced:** Call upon external experts for security assessment, immediate support and back-up:
  - Take advantage of immediate support from the **Kaspersky Incident Response** team of highly experienced analysts and investigators to fully resolve your cyber-incident, fast and effectively.
  - Bring in a second opinion and managed threat hunting expertise from a trusted partner with **Kaspersky Managed Detection and Response**, so your in-house IT security experts have more time to spend reacting to the critical outcomes requiring their attention.
  - Understand just how effective your defenses would really be against potential cyberthreats, and whether you're already the unwitting target of a long-term stealth attack, through **Kaspersky Security Assessment**.

Targeted Solutions

What	How
 **Kaspersky Embedded Systems Security**	A multi-layered solution delivering unequalled protection to Windows-based embedded devices – even those with limited system resources and running discontinued OSs. Opt-in security layers including application and device controls, exploit prevention and anti-malware mean protection can be optimized for lower-powered devices - including vulnerable older PCs running unsupported OSs such as Windows XP.
 **Kaspersky Fraud Prevention**	Advanced Authentication allows for frictionless and continuous authentication, cutting the costs of second factor processes for legitimate users, while keeping fraud detection rates high in real time. Automated Fraud Analytics thoroughly analyzes events that occur during the entire session, transforming them into valuable pieces of data. Protects the external perimeter of any business, ensuring safety and protection for clients.
 **Kaspersky DDoS Protection**	Covers a bandwidth of up to 2Gbps, with extensive service coverage, including attack analysis reports and anti-DDoS capability assessments. Optional automatic always-on DDoS mitigation, fortified by Kaspersky engineers running parallel checks to optimize defense according the nature of each DDoS attack.
 **Kaspersky Payment System Security Assessment**	Uncovers any vulnerabilities in your POS infrastructure that are exploitable by different forms of attack, outlines the possible consequences of exploitation, evaluates the effectiveness of your existing security measures, and helps you plan further actions to fix detected flaws and improve your security.

Cyberthreats News: www.securelist.com

IT Security News: www.kaspersky.com/blog

Threat Intelligence Portal: opentip.kaspersky.com

Technologies at a glance: www.kaspersky.com/TechnoWiki

Awards and recognitions: media.kaspersky.com/en/awards

Interactive Portfolio Tool: kaspersky.com/int_portfolio

kaspersky BRING ON THE FUTURE