# Cybersecurity as a competitive advantage in retail


kaspersky

Retail

# Contents

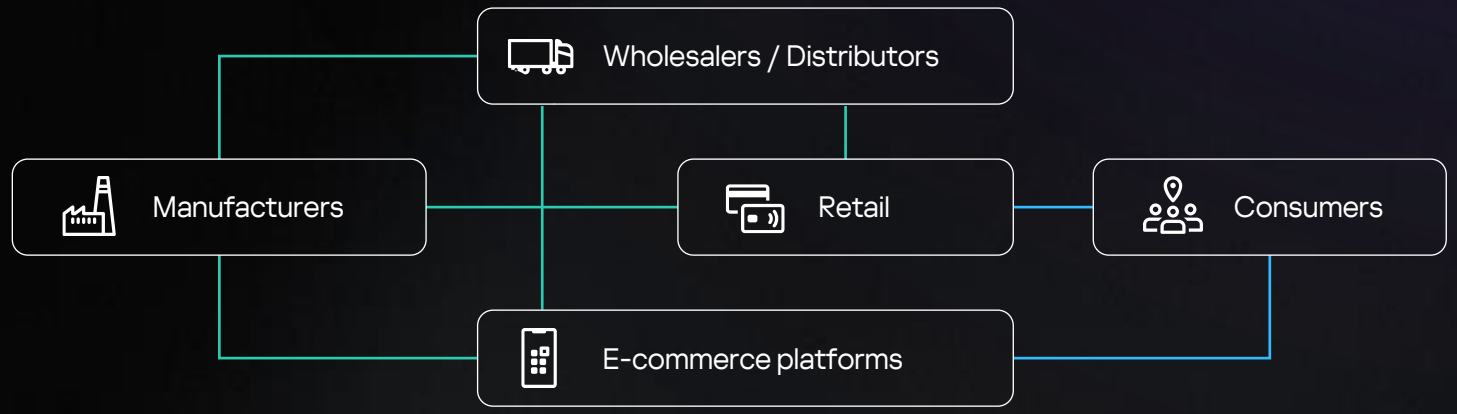
01

# Industry overview

## The trade sector

Involves the distribution of goods and services from the point of production to the point of consumption. Its primary function is to bridge the gap between producers and consumers, who are often separated by time, place and information.

### Value chain




**Types of trade:**

- Wholesale B2B
- Retail B2C

## Retail

The area of trade that involves selling goods and services to consumers through various distribution channels, including physical stores, supermarkets, hypermarkets, online platforms and mobile applications.

## E-commerce

The retail segment defined by buying and selling of goods and services over the internet. It involves transactions that are conducted online, from the initial browse to the final payment.

## Wholesale

Wholesale is the business of selling goods to other businesses, rather than to individual consumers. These businesses then either resell the goods (e.g., retailers) or use them as components in their own products (e.g., manufacturers).

# Priorities

Retail trade is a major source of employment and provides direct contact with consumers, stimulating their demand and shaping their preferences and purchasing behavior.

## **3 top** priorities in retail:

### Customer engagement

Implementing projects to enhance the customer journey, deliver personalized shopping experiences, and create a seamless customer experience

### Resilient infrastructure

Increasing technological flexibility and scalability to optimally support business continuity

### Automating business processes

Automating sales, warehouse and logistics processes, supplier and customer interactions, as well as customer service

# Customer engagement

Implementing projects to enhance the customer journey, deliver personalized shopping experiences, and create a seamless customer experience

## Goals:

1. Develop offline and online commerce channels
2. Adopt a personalized approach to customers
3. Enhance customer support and service

### Short-term plans

- Omnichannel sales (physical commerce)
- Targeted customer offers
- Loyalty program expansion

### Medium-term plans

- Chatbots, augmented reality and AI assistants
- Hyper-personalization and demand forecasting
- Sustainable development and social responsibility

### Long-term plans

- Next-generation product delivery
- Smart stores in offline commerce
- Product purchases via visual search

# Resilient infrastructure

Increasing technological flexibility and scalability to optimally support business continuity

## Goals:

1. Build a resilient e-commerce platforms
2. Leverage cloud services
3. Create a flexible and scalable IT architecture

### Short-term plans

- Resilient and reliable IT systems
- Gradual migration of internal and external services to the cloud
- Online and offline channel integration

### Medium-term plans

- Infrastructure optimization for big data
- Enhanced cybersecurity
- Platform engineering development

### Long-term plans

- Real-time monitoring of applications, warehouses, logistics and workloads
- AI-driven infrastructure monitoring and proactive incident resolution
- API management for connectivity across all devices, apps and data

# Automating business processes

Automating sales, warehouse and logistics processes, supplier and customer interactions, as well as customer service

## Goals:

1. Implement modern warehouse logistics technologies
2. Improve interaction with suppliers and customers
3. Enhance inventory management processes

## Short-term plans

- Increased speed and accuracy of order processing
- Integration of electronic document management (EDM) and EDI systems
- Integration of online and offline channels for enhanced customer experience and real-time offer adaptation

## Medium-term plans

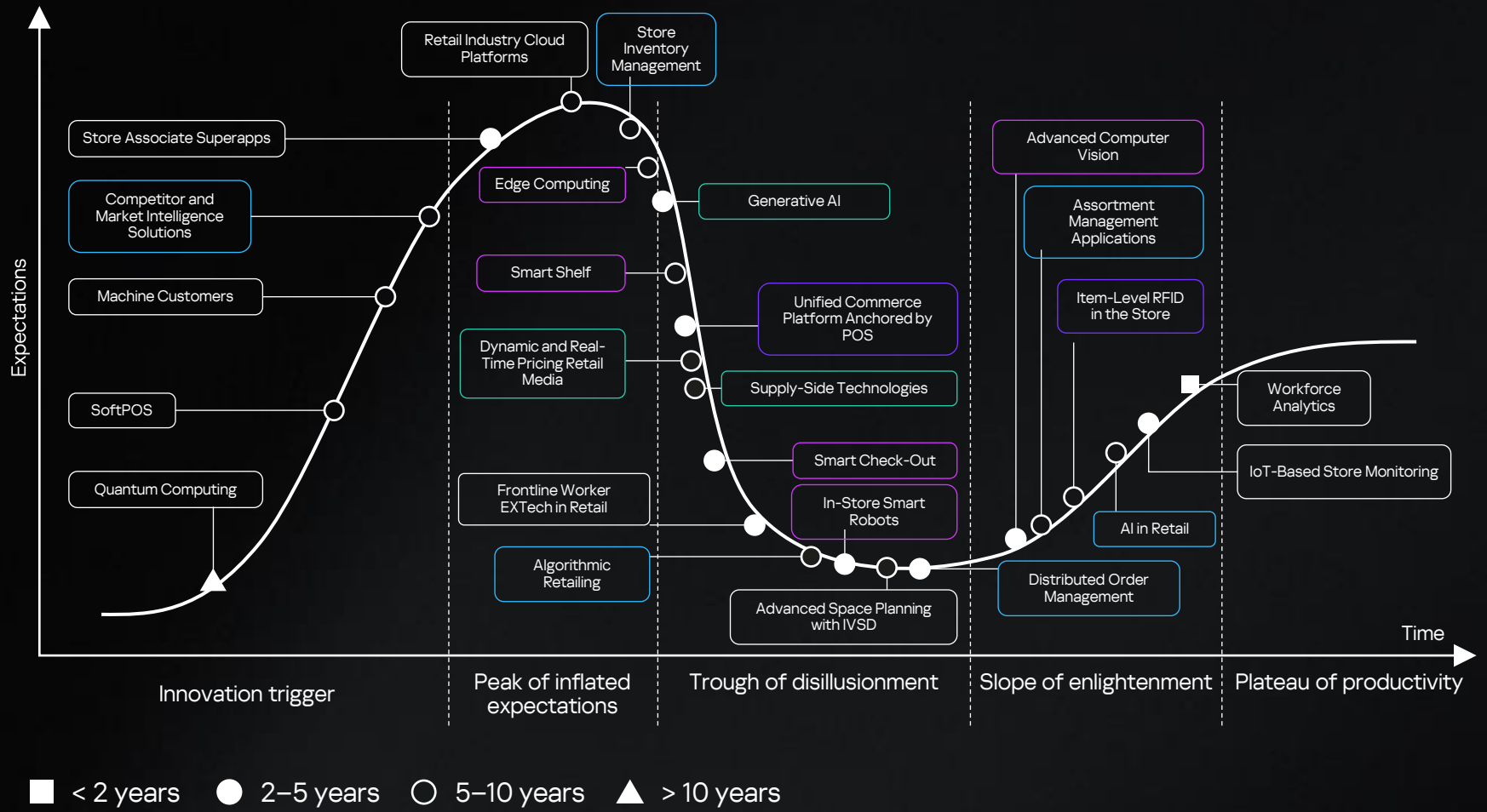
- AI-powered personalized offer creation
- AI tools for dynamic pricing and precise demand forecasting
- Transition from standalone solutions to integrated ecosystems for merchandising, logistics, sales, and analytics management

## Long-term plans

- Automation and robotization of warehouse operations and development of autonomous vehicles
- Introduction of virtual process models and electronic price tags and smart shelves for agile inventory management
- Offline locations equipped with robotics, digital twins, IoT devices, electronic price tags and self-service systems

# Hype Cycle for global trends in the retail industry

Many of these are long-standing market trends, but they are increasingly becoming the new reality.




**Artificial Intelligence (AI):**

- Competitor and Market Intelligence Solutions
- Store Inventory Management
- Algorithmic Retailing
- Distributed Order Management
- Assortment Management Applications
- AI in Retail

**Smart warehouses and stores:**

- Edge Computing
- Smart Shelf
- Smart Check-Out
- In-Store Smart Robots
- Advanced Computer Vision

**Hyper-personalization:**

- Generative AI
- Dynamic and Real-Time Pricing Retail Media
- Supply-Side Technologies

**Seamless user experience:**

- Unified Commerce Platform Anchored by POS
- Item-Level RFID in the Store

*Source: Gartner Hype Cycle of Retail Industry Trends, 2024

# Key trends

New technologies **advance the goals** of retail and e-commerce companies and support business continuity, but they also bring **new risks**.

| | | |
|---|---|---|
| 1 | Seamless user experience | A seamless user experience is when customers can smoothly interact with a brand across different channels and devices without any interruptions or hassle. |
| 2 | Hyper-personalization | Unique, highly personalized offers, dynamic pricing, and marketing campaigns adapted to individual customers. |
| 3 | Smart warehouses and stores | Key elements of digital transformation aimed at automation, increasing efficiency and improving customer experience. |
| 4 | Artificial intelligence | AI is increasingly used for data processing and automating routine operations. IDC predicts that by 2026, 85% of organizations worldwide will use AI and computer vision. |

+

**Additional trends**

- Cloud services
- Self-service
- Internet of Things (IoT)
- Micro-fulfillment centers
- Computer vision
- AR and VR technologies
- Automated delivery

# Advantages and key challenges of retail

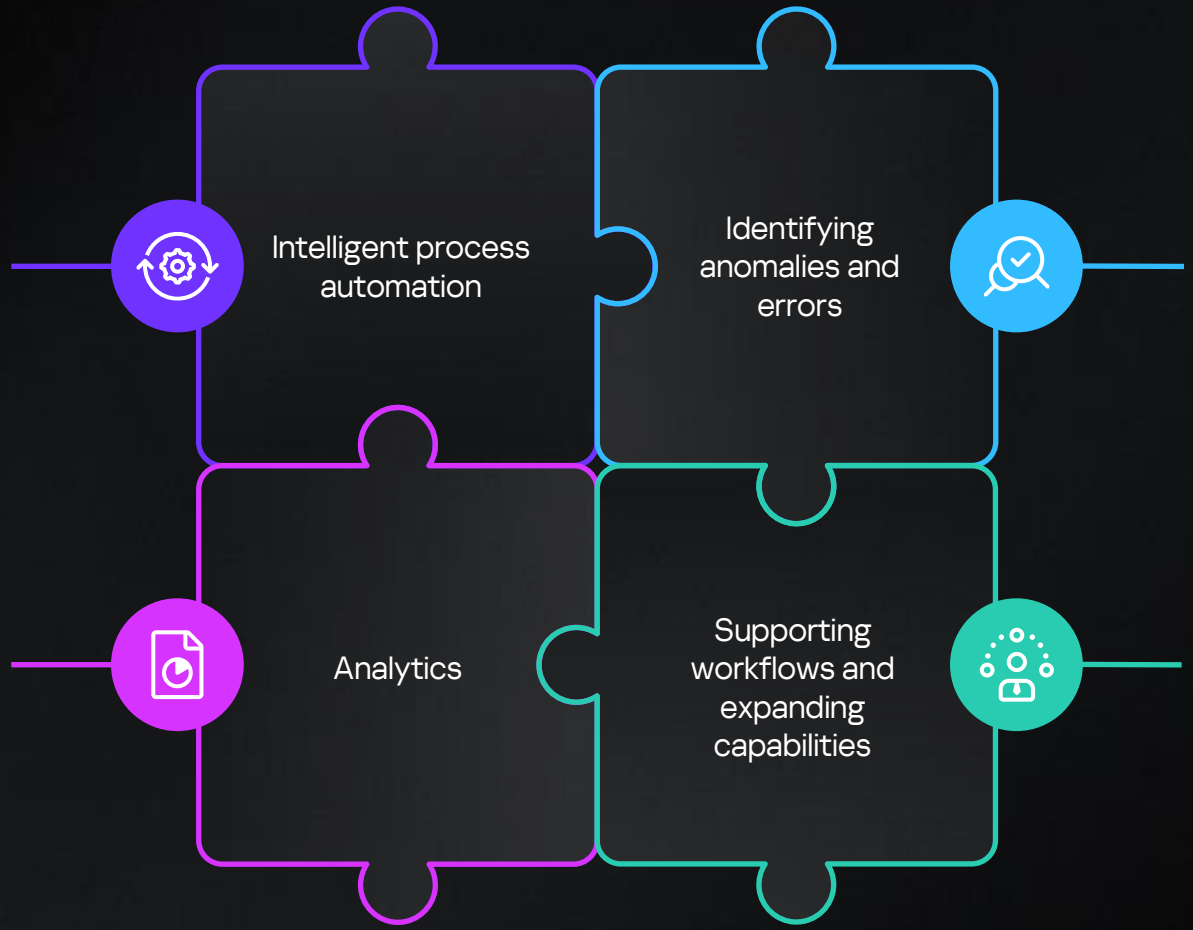
| Priorities | Relevant trends |
|---|---|
| Customer engagement | 1 2 3 4 |
| Resilient infrastructure | 3 4 |
| Automating business processes | 1 3 4 |

| Trends | Advantages | Key challenges |
|---|---|---|
| 1 Seamless user experience | • Increased convenience for customers<br>• Competitiveness and loyalty growth | • **Data and infrastructure security**<br>• Difficulties integrating data and systems |
| 2 Hyper-personalization | • Competitiveness and loyalty growth<br>• Reduced marketing costs<br>• Increased average transaction value | • **Data and infrastructure security**<br>• Collecting, storing and analyzing large volumes of data<br>• Privacy concerns and negative customer reactions |
| 3 Smart warehouses and stores | • Warehouse logistics automation<br>• Improved customer experience<br>• Greater transparency and control of business processes | • **Data and infrastructure security**<br>• Managing complex infrastructure<br>• Significant investments |
| 4 Artificial intelligence | • Optimization of routine tasks<br>• Competitiveness and innovation<br>• Improved customer experience | • **Data and infrastructure security**<br>• High implementation costs |

# Common types of AI use cases in retail

36% of CIOs in retail said their organization is already using AI, and more than 50% plan to implement it by the end of 2025.

- Supply chain and inventory management optimization
- Robotization and automation of warehouse operations
- Implementation of autonomous vehicles
- Offers personalization and marketing



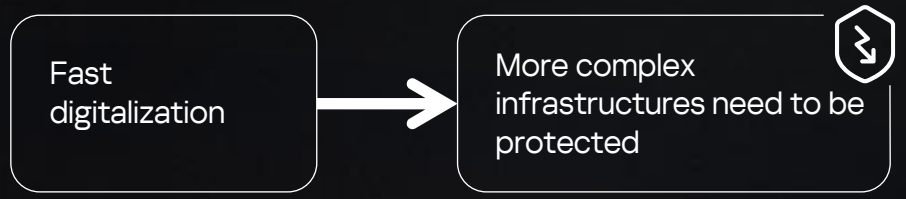

- Optimization of integrated services
- Omnichannel support
- Monitoring of suppliers and logistics processes
- Fraudulent activity analysis

- Scenario and capital expenditure planning
- Big data processing
- In-store customer behavior analysis
- Forecasting (customer demand, inventory and replenishment, sales)

- Intelligent dashboards
- Chatbots and digital assistants
- Decision-making assistance
- Dynamic pricing
- Content generation and marketing automation

*Source: Gartner Hype Cycle of Retail Industry Trends, 2024

# Retail digitalization




## Security challenges

- Attack surface expansion
- New vulnerabilities and threats
- Management and protection of complex infrastructure
- Legacy systems
- Knowledge gaps
- Shortage of specialists
- Budgetary constraints
- Stringent regulations

## Risks

- Targeted attacks could be active in your system right now
- Any disruption of your website or mobile app results in major losses
- Data center attacks can cause massive damage
- Ransomware attacks can lock critical data and devices
- Confidential data loss costs more than just money (reputation, customers)
- Complex logistics processes that affect business efficiency
- Malicious insider activity is widespread and common

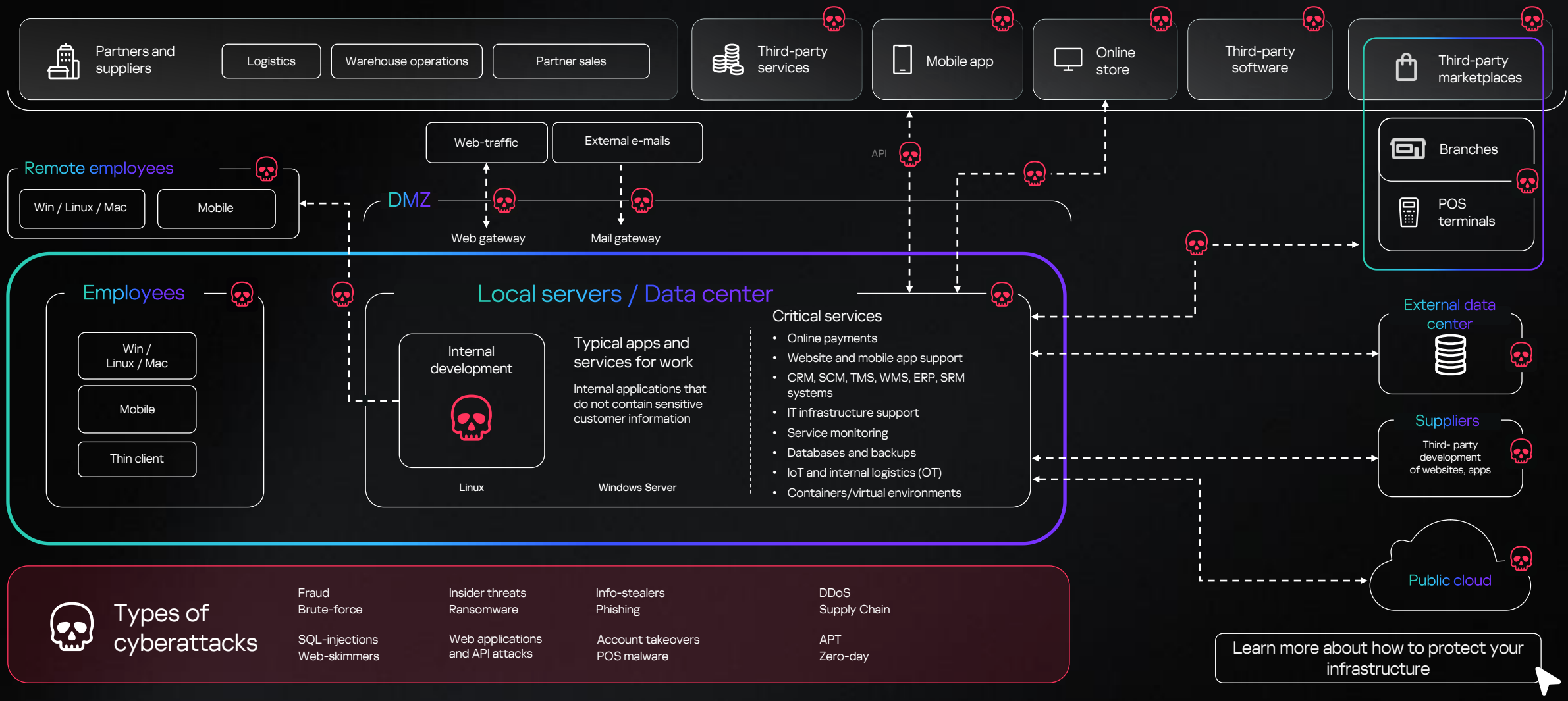
## Required actions

- Overall infrastructure defense
- Website and mobile app protection
- Customer data security against hacking and theft
- Mitigating risks related to third-party vendors, providers and suppliers
- Cybersecurity team training
- Increasing system resilience and reliability
- Monitoring all processes inside the infrastructure and business
- Ongoing security audits and testing

# Contents

02

# Example of an infrastructure with potential attack entry points and threats



# Consequences of cyberattacks for retail

## Retail **ranked first** among all industries **for data breaches** in 2023 and 2024*

- Ransomware
- Web applications and API attacks
- PoS malware
- Web-skimmers
- Fraud
- DDoS
- Phishing
- Insider threats
- APT
- Zero-day
- MITM
- Supply chain
- Info-stealers

Data breaches

Disruption of business processes

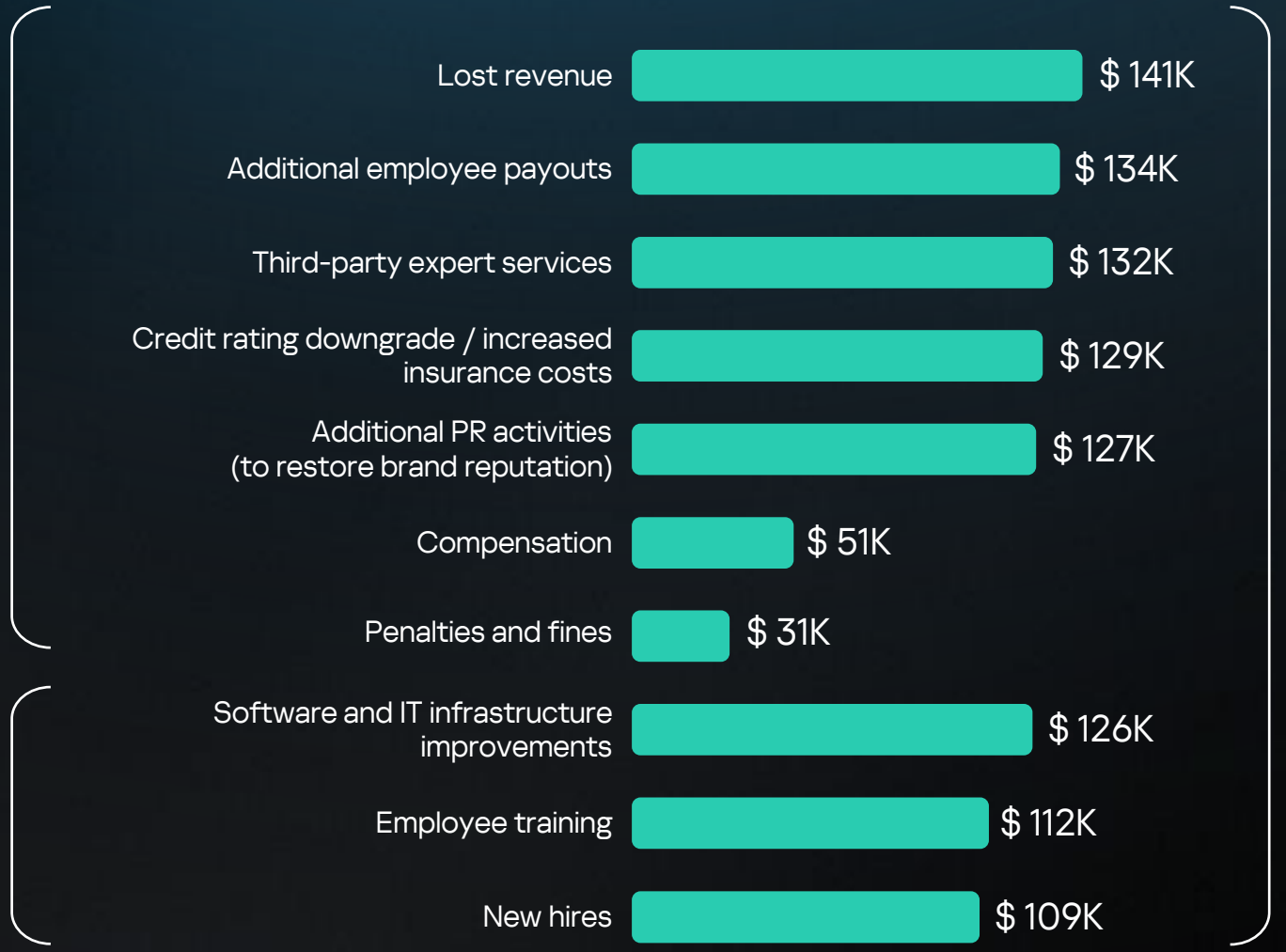
Money theft

Reputational damage

*According to Kaspersky reports

# Data breach

## Breakdown of costs for a major global company following a data breach




**$ 745K**

Initial losses

**$ 347K**

Subsequent costs

**$1.092M**

The total cost incurred by the company as a result of a data breach

Source: Global Emergency Response Team, Kaspersky

# Financial impact of downtime

Retail suffers the **highest downtime losses** of any industry*

**$91M**
**Contractual/legal**
Regulatory fines, SLA penalties, settlement/legal costs

**$76M**
**Lost revenue**

**$38M**
**Security lapse costs**
Ransomware payouts, cyber insurance premiums, extortion payouts

**$38M**
**Staffing/ productivity**
Overtime wages, lost productivity

**$28M**
**Damage control**
Brand trust campaigns, PR/investor relations

**$16M**
**Upgrade needs**
Additional infrastructure capacity, recovering from backups

*According to The Hidden Costs of Downtime report.

# Contents

03

# How can retail protect itself against cyberattacks?

Implement a comprehensive strategy to equip, inform and prepare your in-house experts to deal with cyberthreats.

0

## Preparation

Audit

Review and optimize your processes by inventorying your entire financial infrastructure. This can be done by internal teams or external specialists.

1

## Technologies

Solutions

Give your in-house security team the right tools to detect, investigate, and respond to cyber incidents.

2

## Knowledge

Training and analytics

Keep up with emerging threats and enhance your team's response capabilities through continuous training and up-to-date threat intelligence.

3

## Expertise

Services

Bring in external experts for security analysis, operational assistance, and additional protection and recommendations.

# Defend what matters most and support your priorities with a comprehensive defense

1. Technologies
2. Knowledge
3. Expertise

As cybercriminal activity rises, financial organizations must adopt an ecosystem-based strategy to stay protected.

## 1 Technologies

### Comprehensive protection against different types of threats

#### Essential protection against widespread threats

- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Secure Mobility Management

#### Advanced defense against complex threats

- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Anti Targeted Attack

#### Kaspersky Next EDR

- Kaspersky Next EDR Foundations
- Kaspersky Next EDR Optimum
- Kaspersky Next EDR Expert
- Kaspersky Next XDR Expert

### Tailored solutions for specific industry needs

- Kaspersky Embedded System Security
- Kaspersky Mobile Security SDK
- Kaspersky Fraud Prevention
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky DDoS Protection
- Kaspersky Scan Engine

### Beyond traditional cybersecurity

- Kaspersky Container Security
- Kaspersky SD-WAN
- Kaspersky Thin Client

## 2

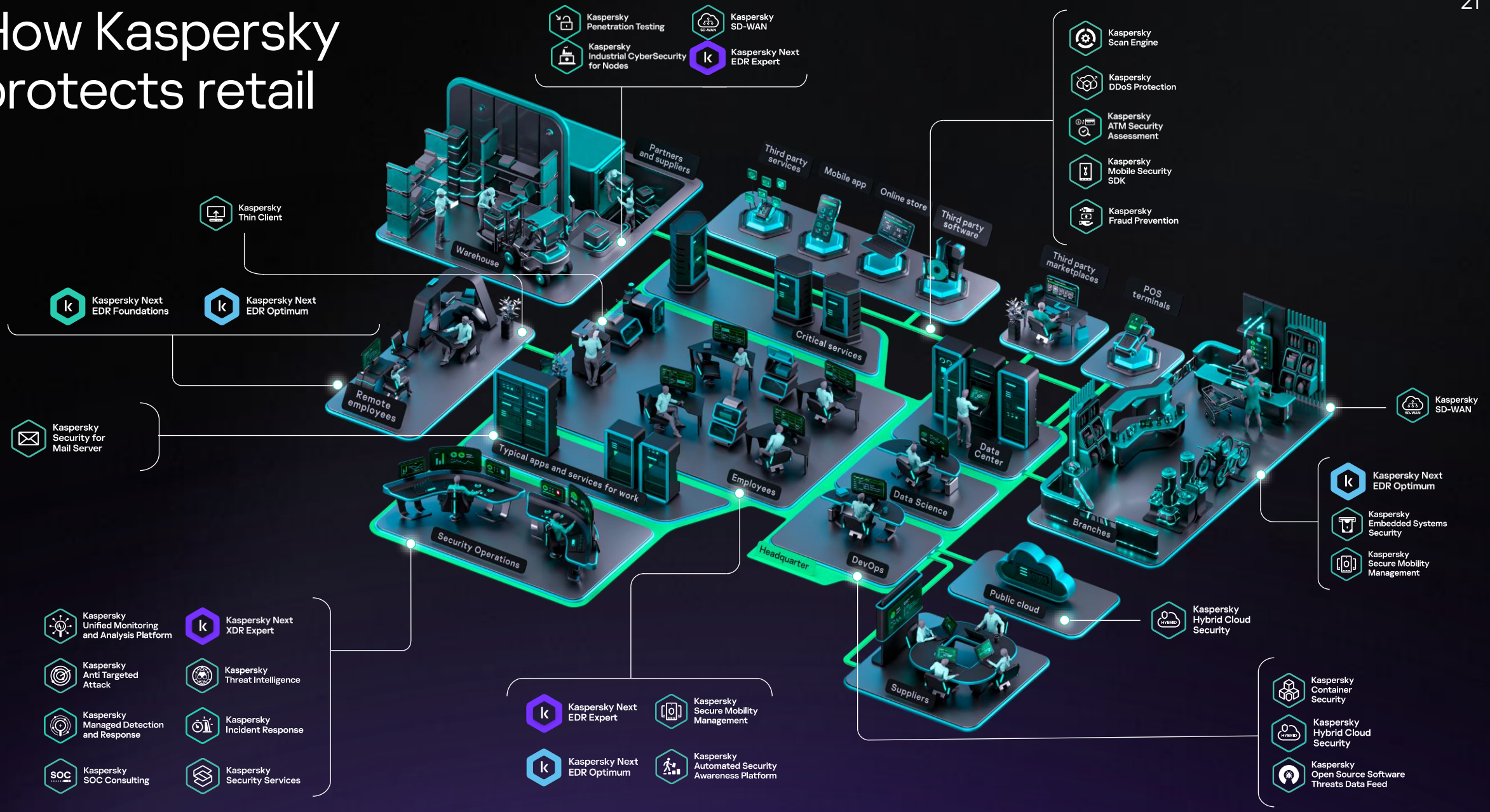
- **Awareness**: Kaspersky Security Awareness
- **Threat Intelligence**: Kaspersky Threat Intelligence
- **Trainings**: Kaspersky Cybersecurity Training

## 3

- **Assessment**: Kaspersky Security Assessment; Kaspersky Payment Systems Security Assessment; Kaspersky Penetration Testing
- **Managed security**: Kaspersky Managed Detection and Response
- **Response**: Kaspersky Incident Response
- **Compromise assessment**: Kaspersky Compromise Assessment
- **SOC Consulting**: Kaspersky SOC Consulting
- **Professional Services**: Kaspersky Professional Services

* Main product and service groups are presented

# How Kaspersky protects retail



# Key IT and cybersecurity challenges

- Protecting infrastructure from sophisticated attacks
- Managing complex and distributed infrastructure
- Protecting the perimeter from supply chain attacks
- Protection against insider attacks
- Supporting payment transaction continuity
- Protecting customers' personal data

Between 2023 and 2025, the number of security incidents and data breaches in retail increased by over 100%*

* According to Data Breach Investigations Report by Verizon (2023-2025)

# Protecting infrastructure from sophisticated attacks

## Technologies
Solutions

Comprehensive protection against all types of threats
**Kaspersky Next XDR Expert**

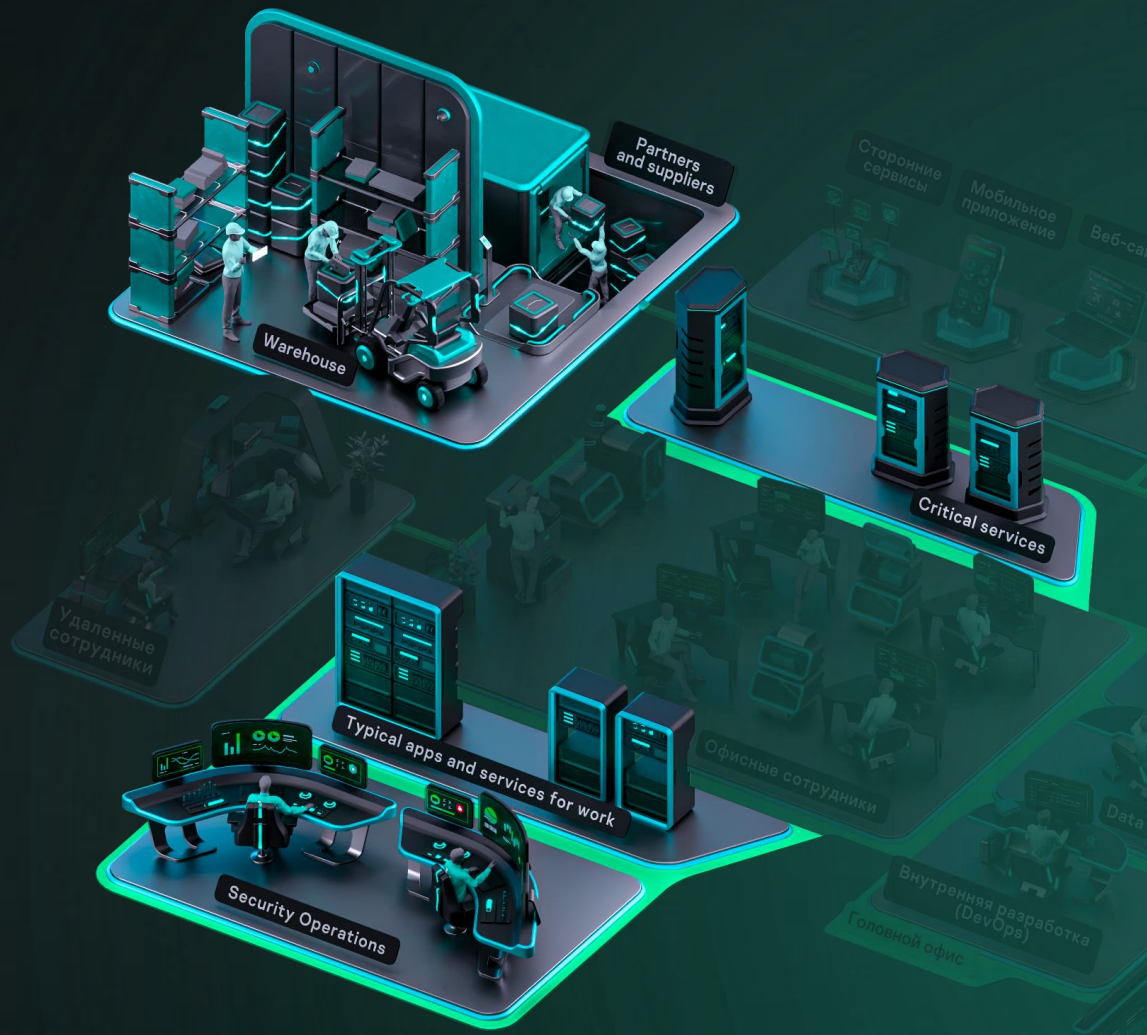
- APT and other advanced cyberthreat protection
  **Kaspersky Anti Targeted Attack**
- Analysis and monitoring of the entire infrastructure
  **Kaspersky Unified Monitoring and Analysis Platform**
- Protection of warehouses and production facilities
  **Kaspersky Industrial CyberSecurity**

## Knowledge
Training and analytics

- Threat information services
  **Kaspersky Threat Intelligence**
- Practical cybersecurity training
  **Kaspersky Cybersecurity Training**

## Expertise
Services

- Incident response and recovery from cyberattacks
  **Kaspersky Incident Response**
- Services for information security monitoring centers
  **Kaspersky SOC Consulting**
- Managed protection against cyberthreats and sophisticated attacks
  **Kaspersky Managed Detection and Response**



# Managing complex and distributed infrastructure

- Wide geographical coverage
- Shortage of IT specialists
- Internet issues in branches
- Complex logistics chains
- Distance between branches and central office
- Uneven levels of cyber protection

Growing attack surface and entry points

**40%**

of distributed-network companies face network issues at least twice a month*

**82%**

of companies need more than an hour to restore network connectivity*

* According to «Managing geographically distributed businesses: challenges and solutions» by Kaspersky, 2024

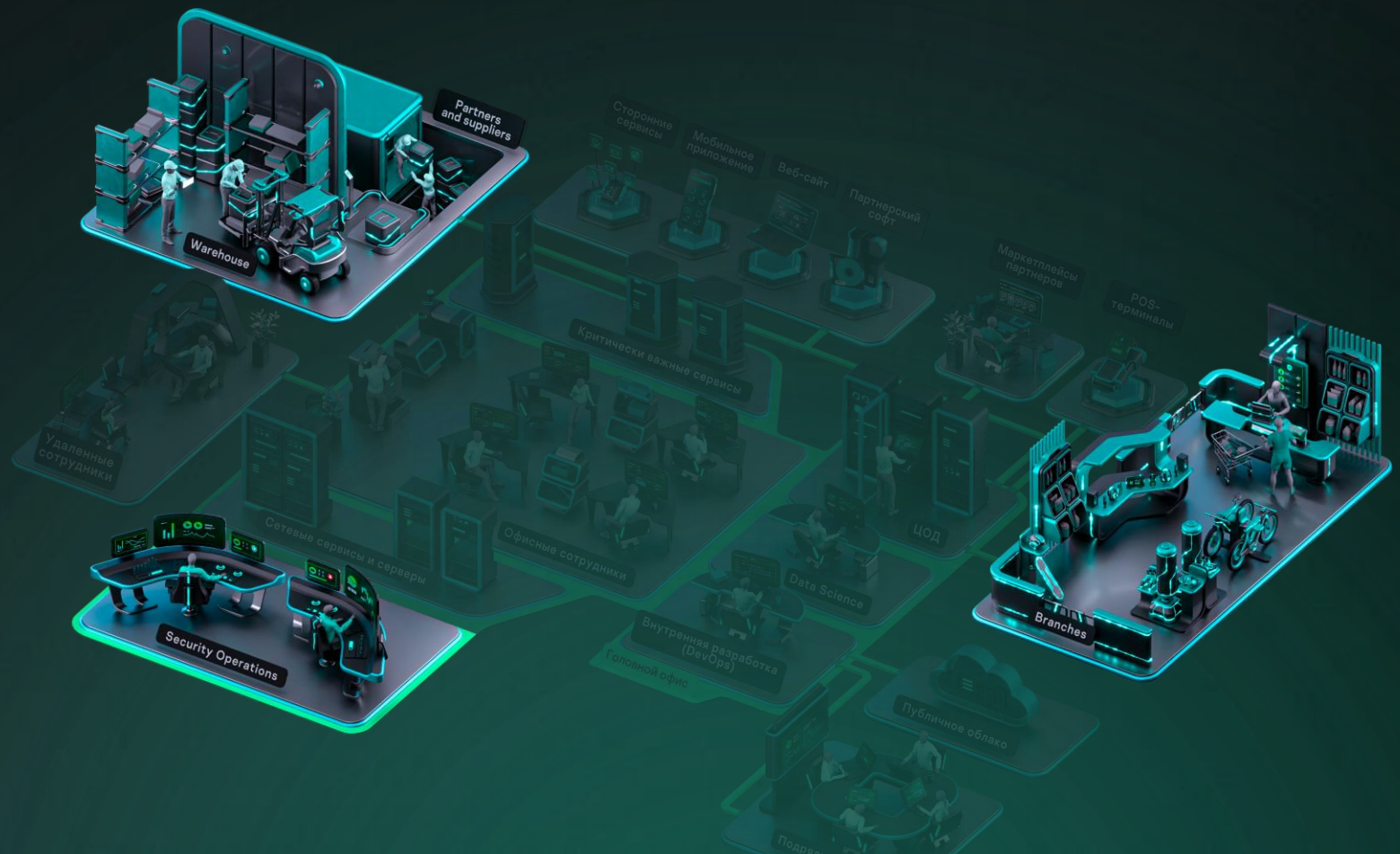
# Centralized IT and security systems are essential for managing complex distributed infrastructures of warehouses and branches

## Technologies
Solutions

- Distributed corporate network
  **Kaspersky SD-WAN**
- Protection of warehouse nodes and production facilities
  **Kaspersky Industrial CyberSecurity for Nodes**
- Warehouse pentesting
  **Kaspersky Penetration Testing**
- Analysis and monitoring of the entire infrastructure
  **Kaspersky Unified Monitoring and Analysis Platform**

## Expertise
Services

- Managed protection against cyber threats and sophisticated attacks
  **Kaspersky Managed Detection and Response**



# Protecting the perimeter from supply chain attacks

## Third-party threats

In 2024, trusted relationship attacks ranked among the top three attack vectors*

30%

of retail attacks in 2024 involved third parties (partners and suppliers)**

## Third-party software threats

Supply chain attacks

Vulnerabilities in e-commerce CMS platforms:

- CMS OpenCart
- WordPress
- Magento

75

zero-day exploits used in the wild were recorded by Google Threat Intelligence Group (GTIG) in 2024***

* According to Kaspersky Incident Response 2024
** According to 2025 Data Breach Investigations Report. Retail Snapshot. Verizon
*** According to Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis

# Supplier/partner systems are often less secure than the targeted retailers themselves, making them prime targets for attackers

## Technologies
Solutions

Comprehensive protection against all types of threats
**Kaspersky Next XDR Expert**

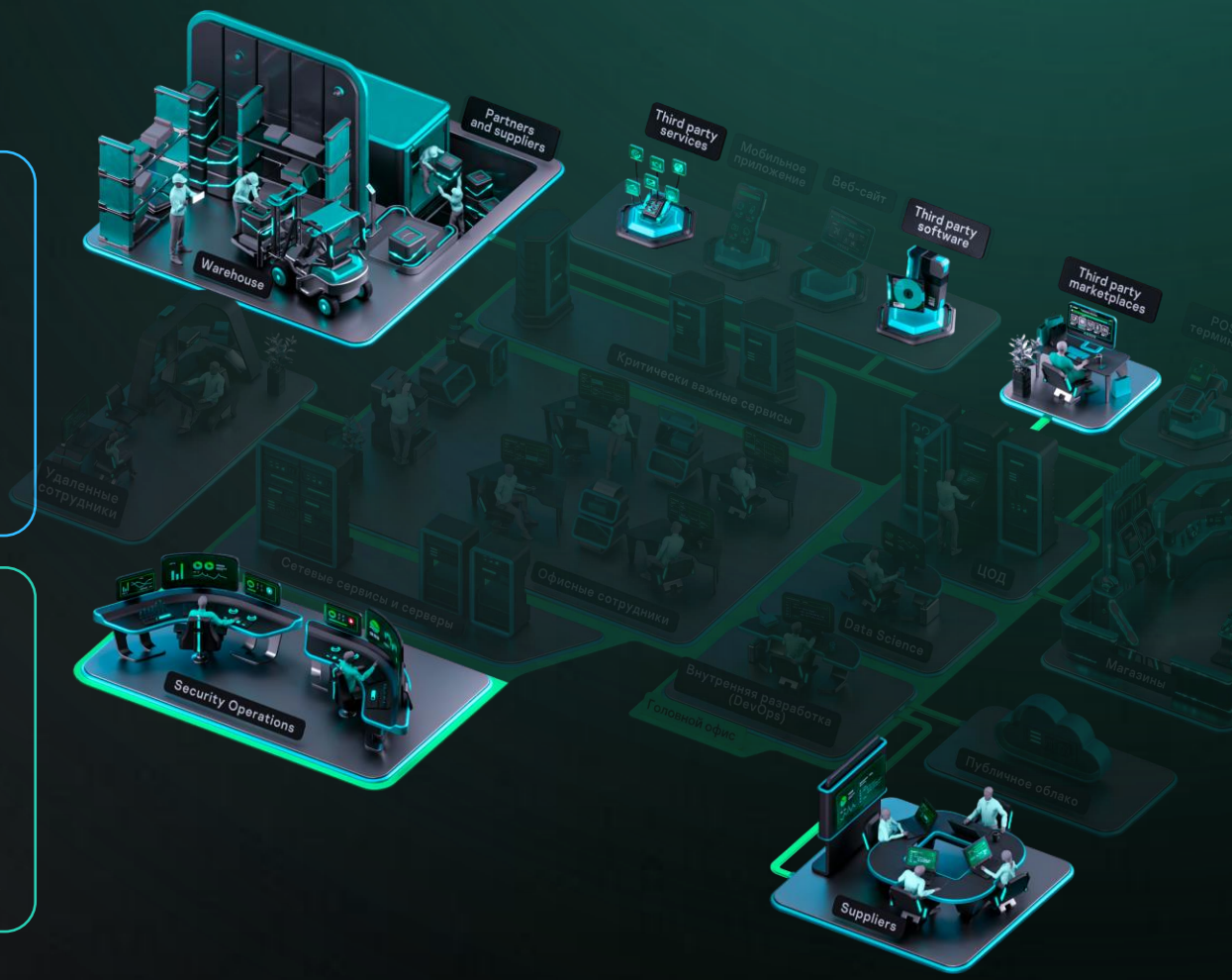
- Analysis and monitoring of the entire infrastructure
  **Kaspersky Unified Monitoring and Analysis Platform**
- APT and other advanced cyberthreat protection
  **Kaspersky Anti Targeted Attack**

## Knowledge
Training and analytics

- Threat information services
  **Kaspersky Threat Intelligence**

## Expertise
Services

- Incident response and recovery from cyberattacks
  **Kaspersky Incident Response**
- Managed protection against cyberthreats and sophisticated attacks
  **Kaspersky Managed Detection and Response**



# Protection against insider attacks

## What did employees do to cause the incident?*


**64%**

of all cyber incidents in 2022–2023 were caused by the human factor*

**17%**

of retail attacks in 2024 were related to social engineering**

**16%**

of retail attacks in 2024 started with phishing**

* According to Kaspersky
** According to 2025 Data Breach Investigations Report. Retail Snapshot. Verizon

# Employees themselves are often the source of cyberthreats, which is why regular cybersecurity training to help ensure comprehensive infrastructure protection is essential

## Technologies
Solutions

Comprehensive protection against all types of threats
**Kaspersky Next XDR Expert**

- Secure workplace connection
  **Kaspersky Thin Client**
- Checking document uploads to internal systems
  **Kaspersky Scan Engine**

## Knowledge
Training and analytics

- Threat information services
  **Kaspersky Threat Intelligence**
- Online training in information security basics
  **Kaspersky Automated Security Awareness Platform**

## Expertise
Services

- Security assessment of your organization
  **Kaspersky Security Assessment**

# Ensuring uninterrupted payment transactions

## Malware for PoS terminals

- Neutrino
- BlackPOS
- Alina
- MalumPOS
- Multigrain
- PoSeidon
- Prilex
- Backoff

## DDoS-as-a-service

From $90
for a 24-hour attack against an unprotected website

from $200
for a 24-hour attack against a DDoS-protected website

**$20 000 per hour**
Losses from a successful DDoS attack

* According to Kaspersky

# It's necessary to adopt international security standards such as PCI DSS and PSD2, and to deploy specialized security solutions to support payment transaction continuity

## Technologies
Solutions

- Securing containerized applications
  **Kaspersky Container Security**
- Protection of stationary PoS systems
  **Kaspersky Embedded Systems Security**
- DDoS attack protection
  **Kaspersky DDoS Protection**
- Creating a secure environment in a partner's mobile application
  **Kaspersky Mobile Security Software Development Kit (SDK)**
- Analysis and monitoring of the entire infrastructure
  **Kaspersky Unified Monitoring and Analysis Platform**
- PoS terminal security and management
  **Kaspersky Secure Mobility Management**

## Expertise
Services

- Analysis of payment system security
  **Kaspersky ATM Security Assessment**
- Managed protection against cyber-threats and sophisticated attacks
  **Kaspersky Managed Detection and Response**

# Protecting customers' personal data

## **Data breach:** direct losses

GDPR

Up to **€10m** or **2%** of global turnover
Up to **€20m** or **4%** of global turnover

LGPD

Up to **$10m** or **2%** of turnover

PIPL

Up to **$7m** or **5%** of turnover

DPDPA

Up to **$30m**

## **Data breach:** indirect losses

~15% (depends on region and age)
of consumers changed retailer or product due to a data leak*

How to calculate indirect losses:

**Average ticket**
**x**
**(number of customers x 0,15)**

* According to YouGov

# Data breaches often occur as a result of employee actions and insufficient cyberthreat protection

## Technologies
Solutions

Comprehensive endpoint protection
**Kaspersky Next EDR Foundations**
or **Kaspersky Next EDR Optimum**

- Online fraud protection
  **Kaspersky Fraud Prevention**
- Analysis and monitoring of the entire infrastructure
  **Kaspersky Unified Monitoring and Analysis Platform**
- Corporate device management
  **Kaspersky Secure Mobility Management**

## Knowledge
Training and analytics

- Data breach detection
  **Kaspersky Digital Footprint Intelligence**

# Contents

04

# Kaspersky's track record in the retail industry

We help retailers minimize risk through proven technologies and deep expertise.
Our solutions follow global best practices.

**>15** years

**122** countries

**>12 300** retailers around the world

| | | | | |
|---|---|---|---|---|
| ~9580 in CIS | ~550 in APAC | ~1430 in Europe | ~720 in the Americas | ~170 in META |

# Success stories

Some of the world's largest retail companies trust us to protect their business

## Magnit

Magnit, one of Russia's largest retailers, implemented a comprehensive cybersecurity system as part of its digital transformation strategy – and has relied on Kaspersky solutions for over 15 years.

> 32 500 branches

386 000 employees

Kaspersky solutions have become central elements of the company's security system, strengthening defenses against cyberattacks.

- Kaspersky Anti Targeted Attack
- Kaspersky Endpoint Detection and Response Expert
- Kaspersky Secure Mail Gateway
- Kaspersky Web Traffic Security
- Kaspersky Container Security
- Kaspersky Fraud Prevention
- Kaspersky Private Security Network
- Kaspersky Embedded Systems Security

> We've been using Kaspersky solutions to protect endpoints since 2008. Over this time, we have come to appreciate their reliability and effectiveness. Kaspersky specialists provided invaluable support in rebuilding our cybersecurity system to modern one. We plan to continue expanding our cooperation.
>
> Alexander Vasilenko,
> CISO

MAGNIT

# Success stories

Some of the world's largest retail companies trust us to protect their business

## Grupo Corripio

Kaspersky delivered a high-quality, scalable and competitively-priced solution so comprehensive that Grupo Corripio has been able to block thousands of endpoint threats, including phishing, ransomware and Trojans.

50+ companies | 12 000 employees | 2 data centers

Kaspersky solutions have become central elements of the company's security system, strengthening defenses against cyberattacks.

Learn more

- Kaspersky Anti Targeted Attack
- Kaspersky Endpoint Detection and Response Expert
- Kaspersky Hybrid Cloud Security
- Kaspersky Total Security for Business
- Kaspersky Managed Detection and Response

> Over the years, Kaspersky has been our strategic ally and has been an important part of our history. Kaspersky's centralized monitoring and management through intuitive, user-friendly interfaces have allowed us greater visibility and control over our cyber security infrastructure.

**Radhames Mendez,**
Senior Business Continuity Manager, Grupo Corripio

GRUPO CORRIPIO

# Contents

05

# Why Kaspersky

Our unique team of cybersecurity experts defends against the world's most complex and dangerous threats. Their deep knowledge continuously strengthens our solutions and services, delivering unmatched quality.

**>27 years**

building a safer world

**>467,000**

new malicious files detected by Kaspersky every day

**>4,9 billion**

cyberattacks detected by Kaspersky in 2024 alone

**>220,000**

corporate customers worldwide choose our protection

**>900**

active groups and operations associated with APT are monitored by us

**5**

unique Centers of Expertise

# Technology leadership built on world-class expertise

## Research and investigation

World-leading expertise in threat research and incident investigation are at the core of our portfolio

Unparalleled global expertise keeps our customers ahead of threats and supported throughout the incident response cycle with our product and services

## Secure AI-powered approach

Secure approach to Artificial Intelligence – built-in to our solutions

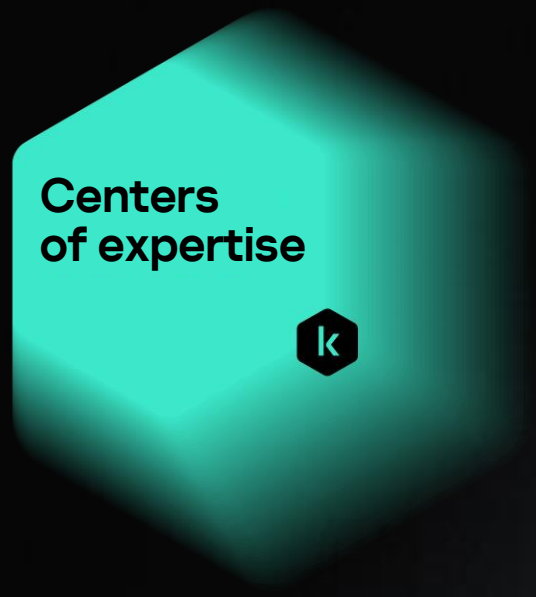
From AI-enhanced threat discovery and alert triage to GenAI-driven Threat Intelligence – we've been doing it for years, and we're leading the way

## Secure Software Development

From Secure Software Development Lifecycle to secure-by-design

Secure development is a guiding principle in our product design processes, enabling us to create completely secure systems that keep our customers safe

# Unmatched expertise




## The unmatched power of expertise: The core of our cybersecurity portfolio

Learn more

Threat Research  Incident Investigation

### Kaspersky Global Research and Analysis Team

- Research of the most complex threats: APTs, cyber espionage campaigns, global cyber epidemics, etc.
- Security of future focused technologies
- Investigation of sophisticated financial cybercrime

### Kaspersky Threat Research

- Safe development and constructive security
- Online threats analysis and content filtering research
- Threat research from malware to APTs and detection logic development

### Kaspersky AI Technology Research

- AI cybersecurity
- GenAI research
- AI-powered threat detection / strengthening information security solutions with AI algorithms

### Kaspersky Security Services

- MDR
- Incident Response
- Security Assessment
- SOC Consulting
- Compromise Assessment
- Digital Footprint Intelligence

### Kaspersky ICS CERT

- Threat Analysis in industrial infrastructure
- ICS vulnerability research and assessment
- Technology associations, analytics and standards

# Transparent & independently recognized

**Proven.**
**Transparent.**
**Independent.**

**The Kaspersky Global Transparency Initiative** is built on concrete, actionable measures that allow stakeholders to validate and verify the trustworthiness of our products, internal processes and business operations.

**13**

Transparency Centers across the world

Regular independent assessments

- SOC 2 audit
- ISO 27001 certification

Bug bounty program

## Recognition that matters

Kaspersky products undergo regular independent assessments by leading research institutes, with our cybersecurity expertise consistently recognized by top industry analysts.

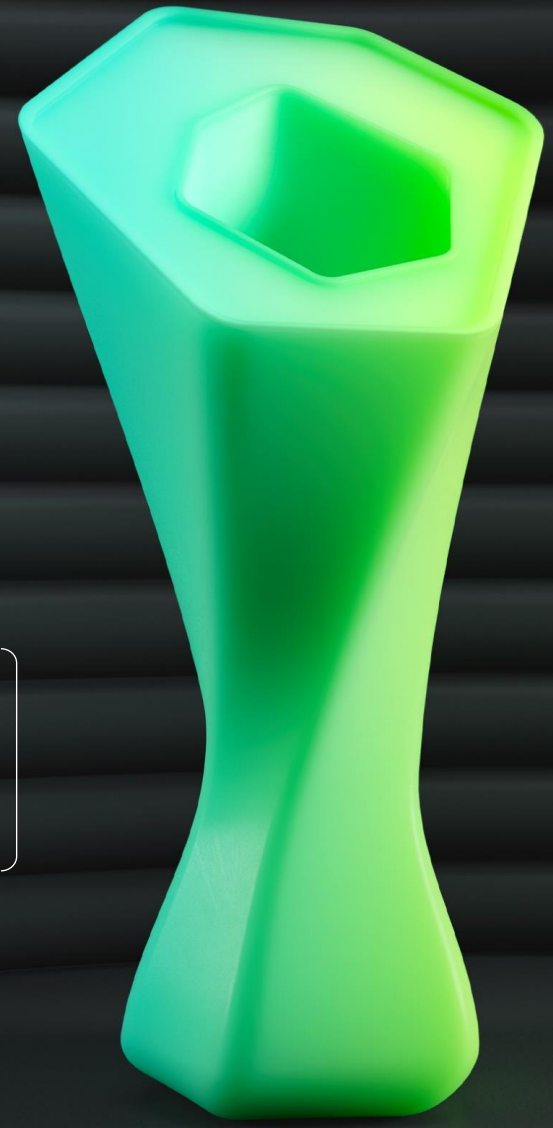
## Most tested. Most awarded.

For over a decade, Kaspersky products have participated in 1022 independent tests and reviews, earning 771 first place results and 871 top-three finishes - testament to our industry-leading protection.

In 2024

| 95 | 91 | 97% |
|---|---|---|
| Tests & reviews | First places | TOP3 places |

Learn more



# Active industry contributor

As a key and active player in global threat intelligence, we work closely with the wider cybersecurity community to combat cybercrime worldwide

INTERPOL

PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE 11 • 12 • 2018

industrial internet CONSORTIUM

AFRIPOL

Coalition Against Stalkerware

We work alongside international organizations such as INTERPOL, law enforcement agencies, CERTs and the global IT security community on joint cybercrime investigations and operations.

MITRE | ATT&CK®

We contribute critical cyberthreat intelligence to global initiatives, including MITRE, to enhance the accuracy of the ATT&CK framework.

Our work is guided by the ethical principles of responsible vulnerability disclosure.

Kaspersky strengthens security across the industry by identifying and helping to fix zero-day vulnerabilities for global brands such as Adobe, Microsoft, Google, Apple, and others.

kaspersky

2025

www.kaspersky.ru



#kaspersky
#bringonthefuture