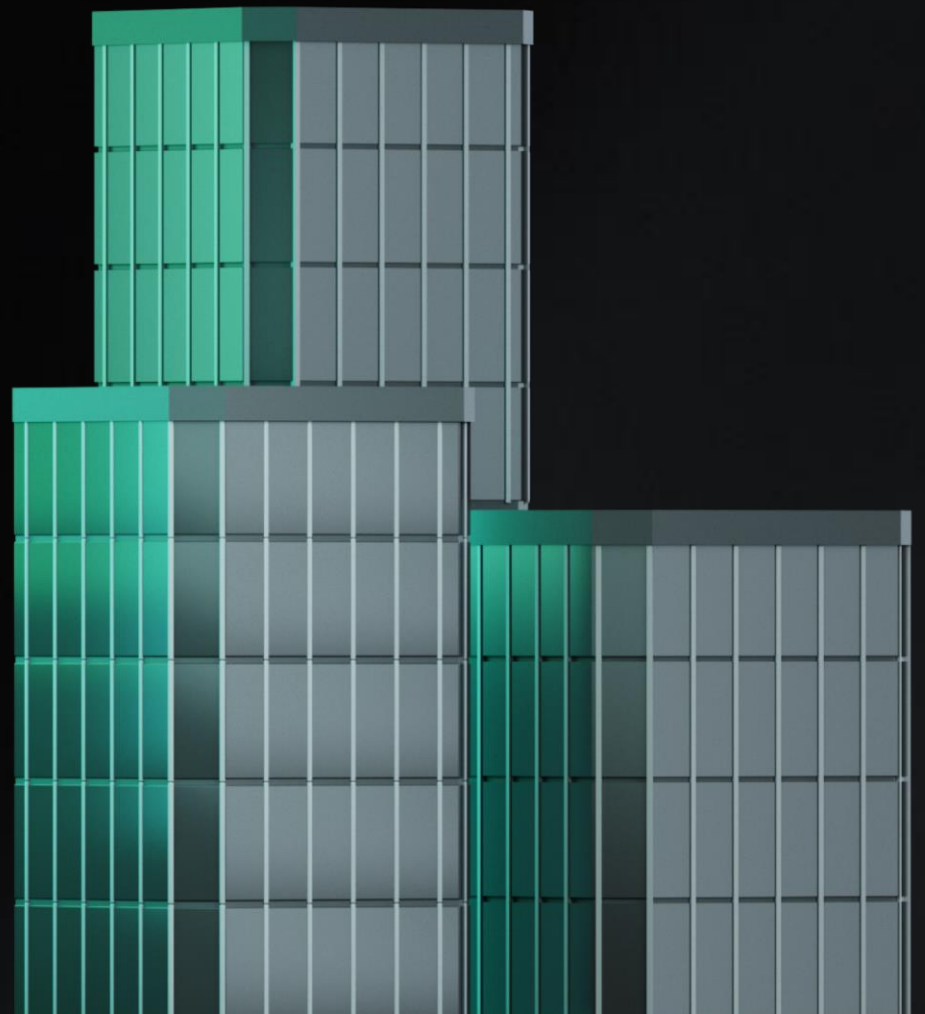
Cybersecurity as a competitive advantage for financial organizations

kaspersky bring on the future

Contents

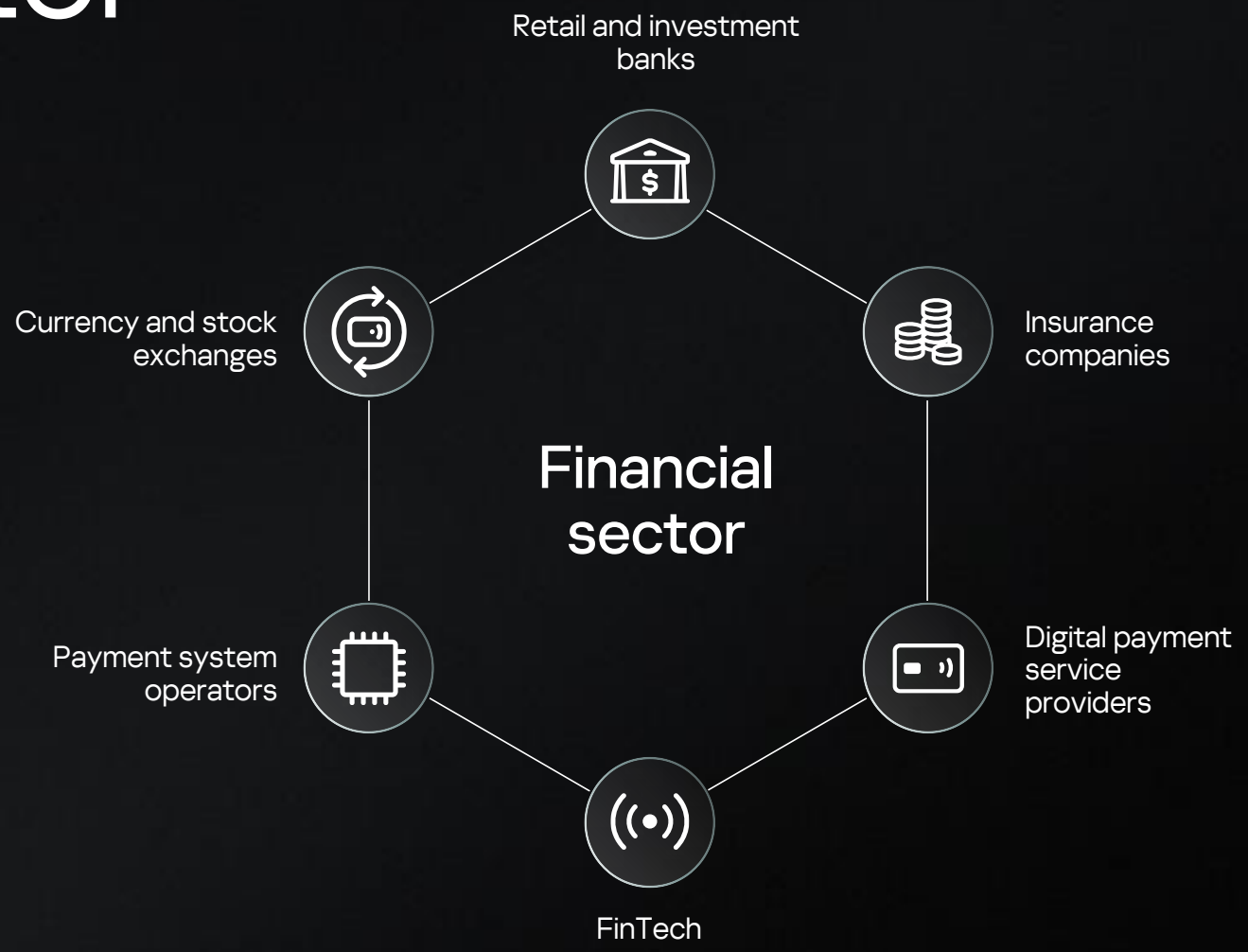


01

Overview of industry priorities, key trends and digitalization challenges

Overview of the financial sector

Key players



Priorities

Financial technologies are fast becoming an integral part of all kinds of financial services, transforming business models and increasing customer focus

3 Priorities of Financial Services organizations:

Customer engagement

Increase revenues through seamless, frictionless customer experiences

Resilient infrastructure

Increase technical flexibility and scalability to support business goals

Digital trust and stewardship

Ensure strong security, risk, and compliance infrastructure to protect customers and support forward-looking business models

Customer engagement

Increase revenues through seamless, frictionless customer experiences

Goals:

1. Improved digital and assisted channels
2. Personalized approach
3. Improved customer experience

Short-term plans

- Enhance mobile banking app and promote the omni-channel experience
- Actionable customer alerts
- Personalized digital offers

Medium-term plans

- AI-powered virtual assistants with Contact Center Management
- Grow revenues by adding value to transactions: offering new services based on data
- Customer value and balance sheet optimization

Long-term plans

- Banking ecosystem
- Lifestyle banking: operations integrated with the customer's lifestyle journey
- Strategic pricing optimization using big data

Digital trust and stewardship

Ensure strong security, risk, and compliance infrastructure to protect customers and support forward-looking business models

Goals:

1. Identifying the ‘modern customer’
2. Enhanced cybersecurity
3. Comprehensive risk management

Short-term plans

- Optimization of the digital identity verification processes
- Incident tracking and reporting
- Operational risk and resilience management

Medium-term plans

- Intelligent Know Your Customer (KYC) / Customer Due Diligence (CDD)
- Advanced anti-money laundering transaction monitoring
- Third-party risk management

Long-term plans

- Real-time monitoring of all applications and workloads
- Use of AI to monitor infrastructure and proactively resolve incidents
- API management to support interconnections between different types of devices, applications and data

Resilient infrastructure

Increase technical flexibility and scalability to better support business goals

Goals:

1. Resilient digital banking platform
2. Active use of cloud services
3. Build a flexible and scalable IT architecture

Short-term plans

- Gradually move business applications to cloud-based infrastructure
- Preparation of a framework for adopting cloud services
- Transforming a monolith app into microservices

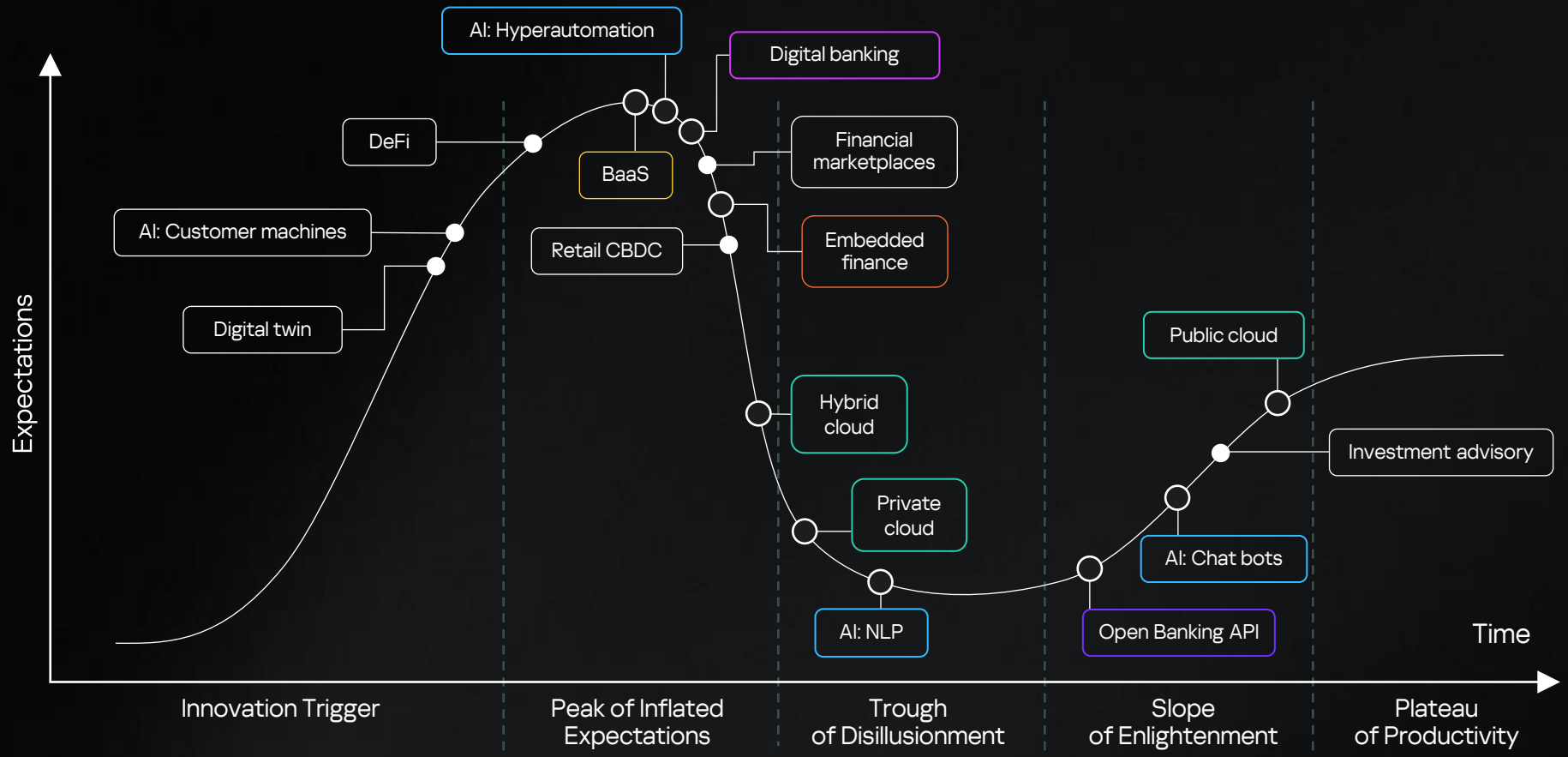
Medium-term plans

- Prioritize specific workloads to begin transforming to the latest development methodologies
- Workload selection for cloud migration
- Streamline workflows to speed up application output

Long-term plans

- Real-time monitoring of all applications and workloads
- Using AI to monitor infrastructure and proactively resolve incidents
- API management in order to support interconnections among all manner of devices, applications, and data

Hype Cycle for global trends in the financial industry



Cloud services

- Hybrid cloud
- Private cloud
- Public cloud

AI

- Hyperautomation
- Chat bots
- NLP

Many of these trends have been present in the market for some time, but they continue to grow and are increasingly becoming the new reality.

* Based on Gartner Hype Cycle

Widespread use of AI in finance

AI remains one of the most dominant emerging technologies in the banking and investment services industry, with **77%** of CIOs reporting that their enterprise has deployed or is planning to deploy AI in the next 12 months.

中國銀行 BANK OF CHINA

2019: Bank of China implemented iAM Smart technology to verify identities using facial recognition when opening mobile banking accounts.

Nordea

2017: Nordea Life & Pension launched a robot named Liv—a "virtual employee" for customer service in Sweden.

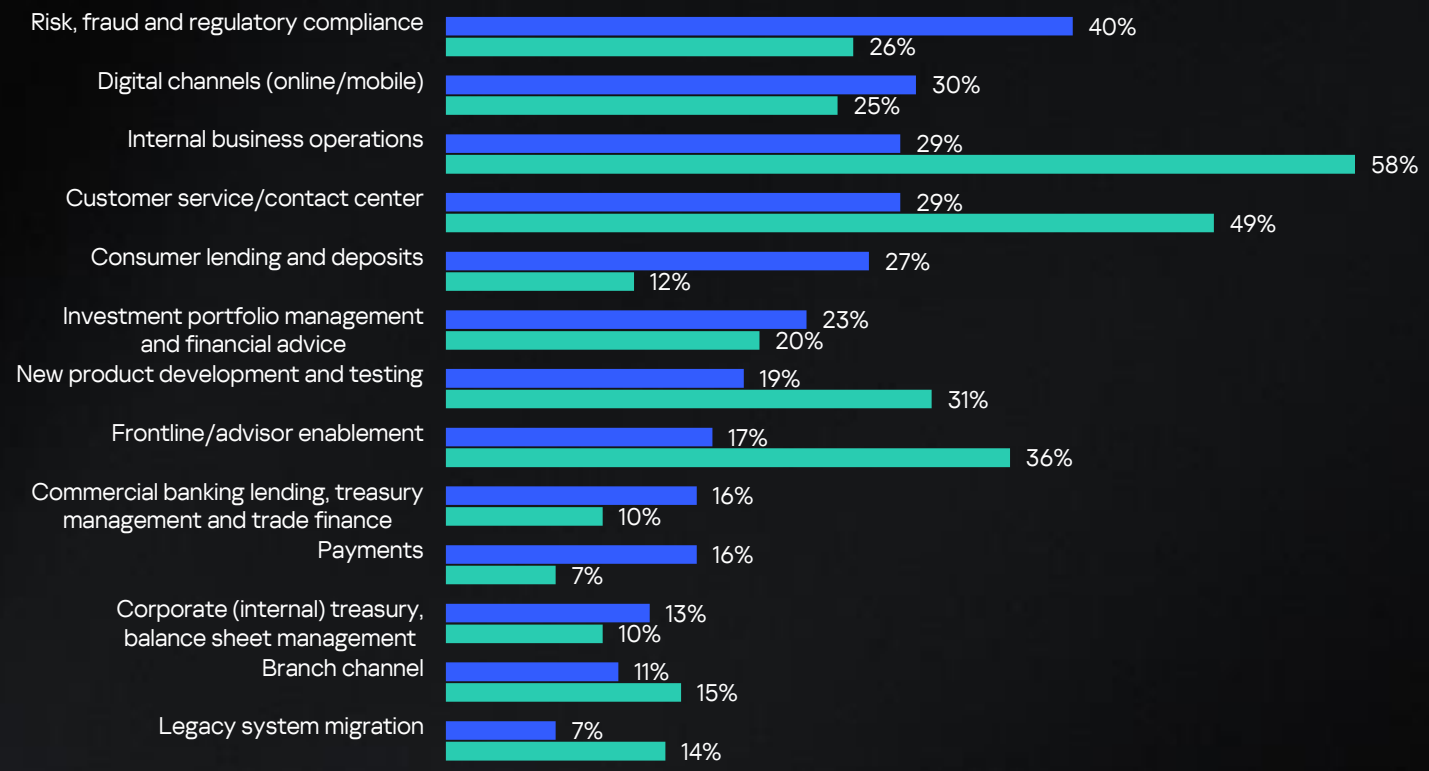
According to Nordea, this resulted in processes being 80% faster and completely eliminated errors.

Source: 2024 Gartner Financial Services Research Panel AI Implementation Trends Survey

Areas using Artificial Intelligence

Q: In which areas of your firm are AI and GenAI initiatives currently underway or already deployed?

Percentage of senior executives at banking / investment organizations where AI initiatives are underway



GenAI deployed or underway

AI deployed or underway

Source: 2024 Gartner Financial Services Research Panel AI Implementation Trends Survey

Common Types of AI Use Cases in Finance

- Customer credit management
- Invoice matching — AP
- T&E optimization
- Cash application

- Duplicate payment identification
- Contract analysis
- Transaction and balance monitoring
- Compliance and risk monitoring

- Scenario and capex planning
- Customer behavior prediction
- Predictive and prescriptive analytical modeling
- Forecasting (demand, revenue, cashflow, expenses)

- Intelligent dashboards
- Chatbots/digital assistants
- Decision support
- Pricing automation
- Natural language query

Source: 2024 Gartner Financial Services Research Panel AI

Key trends

Trends in the financial industry point to a future that is rapidly evolving, borderless and flexible. New technologies are essential to meeting financial institutions' priorities – but they also introduce new risks and serious consequences for failure.

1	Open Banking API	Open Banking enables third parties to use banking data, improving the quality of customer service. The implementation of open API standards requires compliance with enhanced information security measures, including audits by qualified specialists.
2	BaaS	Banking as a Service (BaaS) involves purchasing existing banking products from a bank to support business. BaaS provides infrastructure, products and services to other businesses, so they can make their own offerings.
3	Embedded finance	Embedded finance is a branch of BaaS which involves integrating payment services into the websites/applications of companies that sell products or services. Embedded finance is not focused on business like BaaS is; instead, it's oriented towards end users.
4	Cloud services	Cloud services help businesses to scale and quickly launch new projects without needing additional computing capacity.
5	Digital banking	Banks are continuing to develop remote access, product digitization and online services.
6	Artificial Intelligence (AI)	IDC predicts that by 2026, 85% of organizations will be using artificial intelligence and computer vision, leading to a 25% increase in productivity.

Other finance trends

+

- Digital currencies
- DeFi (decentralized finance)
- Financial marketplaces
- Digital twins
- Investment consulting

Priorities	Relevant trends
Customer engagement	1, 2, 3, 5, 6
Resilient infrastructure	1, 4, 5, 6
Digital trust and stewardship	2, 3, 4, 5

	Trends	Advantages
1	Open Banking API	• Financial inclusion and accessibility • Increased competition and innovation • Enhanced customer experience
2	BaaS	• Reduced app cost and time to market • Diversified product offerings • Increased revenue • Less need for R&D
3	Embedded finance	• Enhanced customer experience • Increased revenue
4	Cloud services	• More scalable and resilient infrastructure • Infrastructure cost reduction • Fast payment processing
5	Digital banking	• Large customer base • Enhanced customer experience • Reduced services time to market
6	Artificial Intelligence (AI)	• Optimization of routine tasks • Competitiveness and development of innovations • Improved customer experience

Today, digitalization helps financial organizations expand their service offerings, automate routine processes, and save resources. However, it also increases cyber risks.

Challenges associated with main trends

- Data privacy and security
- Regulatory compliance

Survey of CISOs

What is currently **the biggest** cybersecurity challenge for financial organizations?

Rapid industry digitalization

Expanding and increasingly complex infrastructure requires stronger protection.

Stringent regulatory requirements

Security systems must be built in compliance with regulatory requirements.

Digital transformation must address cybersecurity threats and risks, and security strategies must comply with regulatory requirements.

Based on in-depth interviews conducted by Kaspersky.

Main digitalization challenges in financial organizations

Fast digitalization → More complex infrastructures need to be protected

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
- Malicious insider activity is widespread and common
- 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)
- Compliance and regulatory challenges must be met in full

Required actions

- Overall Infrastructure defense
- Protect online banking platforms and their customers
- Secure financial transactions across multiple channels including ATMs, points of sale and online
- Protect customer data from breaches and theft
- Deal with risks associated with third-party vendors and providers
- Comply with emerging regulations including GDPR, SOX, PCI-DSS, etc.

Compliance with standards

We understand the importance of meeting the financial industry's regulatory requirements

These standards are the foundation of cybersecurity resilience in the financial sector, helping protect payment systems, customer data and business processes from cyberthreats.

Compliance standards

- SO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls
- PCI DSS (Payment Card Industry Data Security Standard) v4.0

02

Financial Services threat landscape

Widespread threats in the financial industry

42%
of all incidents in 2024 involved ransomware*

Ransomware

1 in 14
infostealer infections result in card data theft*

Infostealers

44%
of phishing attempts targeted users of banking services in 2024**

Fraud

30%
of InfoSec professionals are concerned about increases in DDoS attacks**

DDoS

* According to Kaspersky reports, 2025

** According to Kaspersky reports, 2024

Widespread threats in the financial industry

24%
of all cyber incidents in 2024 involved phishing*

Phishing

26%
of all cyber incidents in the past two years were caused by employees intentionally violating information security policies **

Insiders

Common, widespread threats are often the entry point for more advanced attacks

Advanced threats

* According to Kaspersky MDR Analyst Report, 2025

** According to Kaspersky Human Factor 360^0 Report, 2023

Major advanced threats in the financial industry

Advanced persistent threats (APTs)

US$1 billion

Carbanak is a large-scale financial cybercrime campaign, that has caused total losses of US$1 billion

2023	2024
LoneZerda	Zanubis
BlindEagle	SideWinder
Dark Caracal	

Over the past two years, Kaspersky has detected five major APT campaigns targeting financial organizations

Major advanced threats in the financial industry

Zero-day vulnerability attacks

Google Chrome

In 2024, Kaspersky experts discovered a zero-day vulnerability in the world's most popular browser*

Supply chain attacks

XZ Backdoor

Potentially the most dangerous supply chain attack of 2024 and one of the most significant in the history of Linux systems*

*According to Kaspersky reports, 2024

Major advanced threats in the financial industry

Banking trojans

Grandoreiro

1700

financial institutions and their users were targeted worldwide in 2024

Coyote

A multi-stage banking trojan targeting clients of over 60 financial institutions and using a highly complex infection chain*

*According to Kaspersky reports, 2024

Well-known malware targeting financial organizations

QBot banking Trojan

Also known as QuackBot and Pinkslipbot, QBot was first discovered in 2007 and has been evolving ever since.
Currently, it is delivered to potential victims via existing malware on their systems, as well as through social engineering and spam emails.
Kaspersky's home and business solutions use a multi-layered approach, including behavioral analysis, to detect and block this threat.

Prilex malware

Prilex is a cybercriminal group that has been stealing bank card data since 2014. More recently, they have focused on attacking POS (point-of-sale) terminals.
The malware continues to evolve, with recent developments including the ability to block NFC-based transactions.
Attackers typically install the malware on POS terminals using social engineering tactics.
Prilex activity is most frequently observed in Latin America, though it has also been detected in Germany.

*APK (Android Package) is a file format used by the Android operating system for installing and distributing applications.

Securelist | Kaspersky threat research and reports

Well-known malware targeting financial organizations

PixPirate Android banking Trojan

PixPirate is part of the latest generation of Android banking Trojans.
It can perform Automated Transfer System (ATS) functions, allowing attackers to automate malicious money transfers through the Pix instant payment platform, widely used by several Brazilian banks.
The dropper apps used to deliver PixPirate are disguised as authenticator apps and are typically distributed through .apk files on phishing websites.

Emotet Trojan

With Emotet, cybercriminals can gain access to confidential data on victims' devices.
Emotet is notorious for bypassing basic antivirus programs, making it harder to detect. Once downloaded, the malware can spread across networks by infiltrating other devices.
Emotet is mainly spread through phishing emails containing malicious links or infected documents.
First detected in 2014 after targeting German and Austrian bank customers, Emotet has since spread globally and can attack organizations in any industry, including government agencies.

*APK (Android Package) is a file format used by the Android operating system for installing and distributing applications.

Crimeware and financial cyberthreats in 2024

1. Increase in AI-powered cyberattacks
2. Fraudulent schemes targeting direct payment systems
3. Ransomware target selection
4. Resurgence of Brazilian banking trojans
5. Open-source backdoored packages
6. Exploitation of misconfigured devices and services
7. Fluid composition of affiliate groups
8. Adoption of less popular / cross-platform languages
9. Emergence of hacktivist groups

Crimeware and financial cyberthreats predictions for 2025

How is the financial cyberthreat landscape expected to evolve in 2025? Here are the key attack trends we anticipate while protecting businesses and individuals in the year ahead.

1. Upsurge in stealer activity
2. Attacks against central banks and open banking initiatives
3. Increase in supply chain attacks on open-source projects
4. New blockchain-based threats
5. Expansion of Chinese-speaking crimeware worldwide
6. Synthetic data poisoning through ransomware
7. Quantum-resistant ransomware
8. Weaponization of regulatory compliance by ransomware attackers
9. Ransomware-as-a-service proliferation
10. More AI and machine learning on the defense side
11. Upsurge in financial cyberattacks targeting smartphones

https://securelist.com/ksb-financial-and-crimeware-predictions-2025/114565/

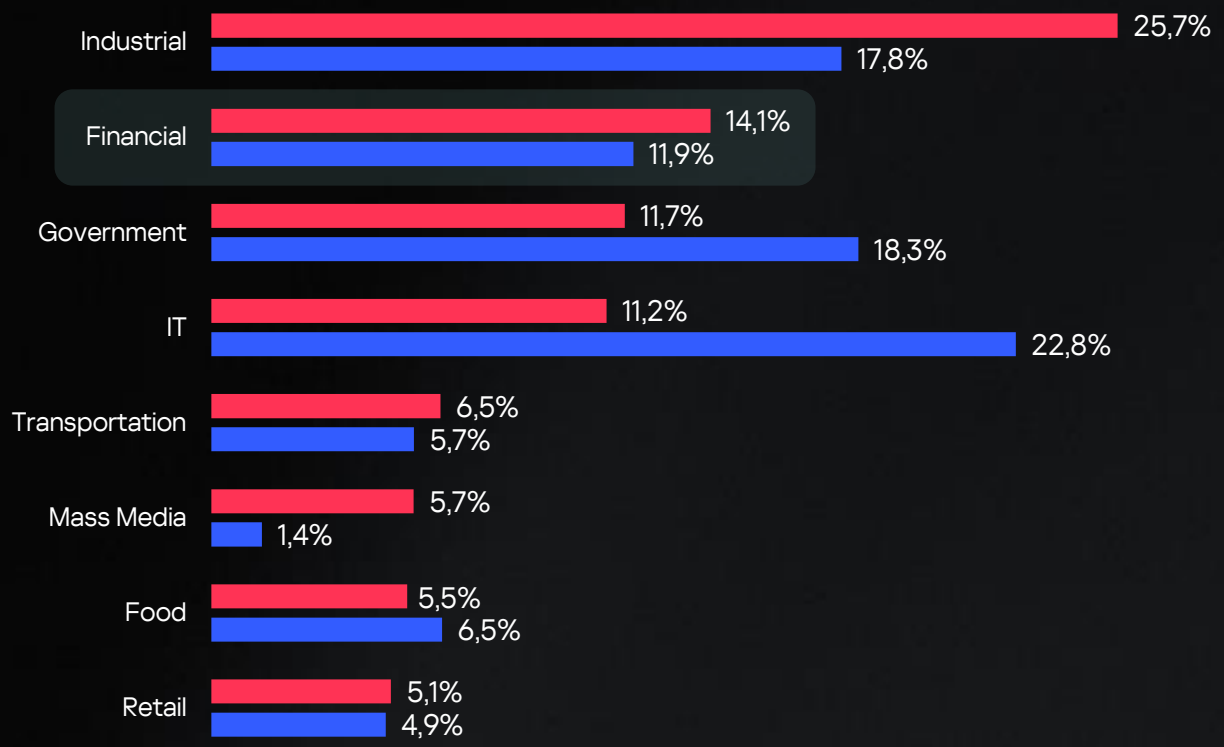
Cyber incidents in the financial industry

~ 270,000
security alerts were observed in the financial industry in 2024*

18.3%
- share of reported incidents in the financial industry in 2024*

US$ 3.2 million
- average losses of BFSI companies in 2024**

14.9%
of reported high-severity incidents in 2024 involved the financial industry*



2 highest
by regular incidents

4 highest
by severe incidents

Regular

The share of reported incidents in a specific industry from the total number of incidents across all industries

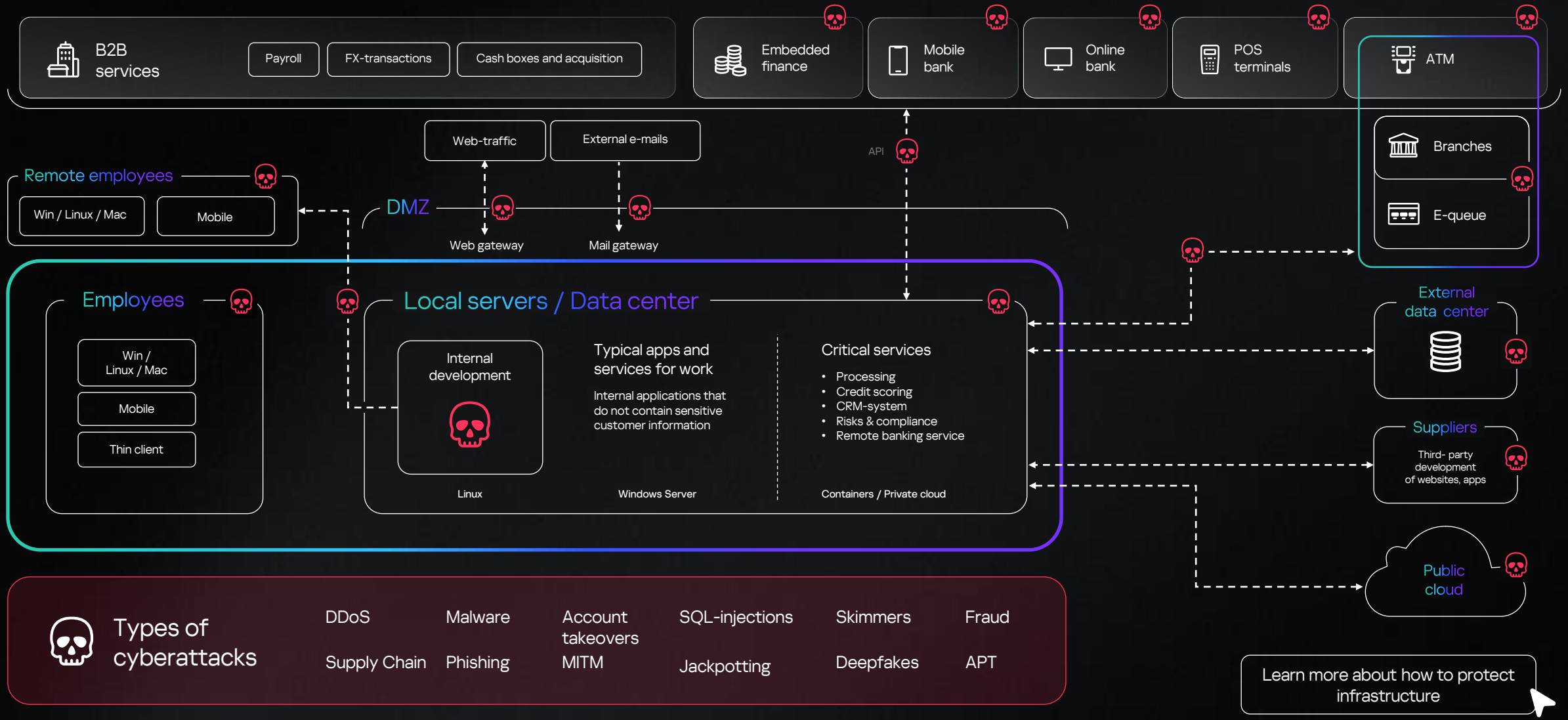
Severe

The share of reported high-severity incidents in a specific industry from the total number of high severity incidents across all industries

* According to the Kaspersky MDR Analyst report, 2024

** According to the Kaspersky IT Security Economics report, 2024

Example of an infrastructure with potential attack entry points and threats



Consequences of cyberattacks for financial organizations

- Ransomware
- Infostealers
- Fraud
- Phishing
- Insiders
- DDoS
- Advanced persistent threats (APTs)
- Zero-day vulnerability attacks
- Supply chain attacks
- Banking trojans

Data leaks

Disruption of business processes

Money theft

Reputational damage

03

A comprehensive approach to protection

How can the financial industry protect itself against cyberattacks?

Implement a comprehensive strategy to equip, inform, and prepare your in-house experts to handle all 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

Click the product icons to learn more

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 various 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

- 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 Who Calls SDK / REST API
- Kaspersky DDoS Protection
- Kaspersky Scan Engine

Beyond traditional cybersecurity

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

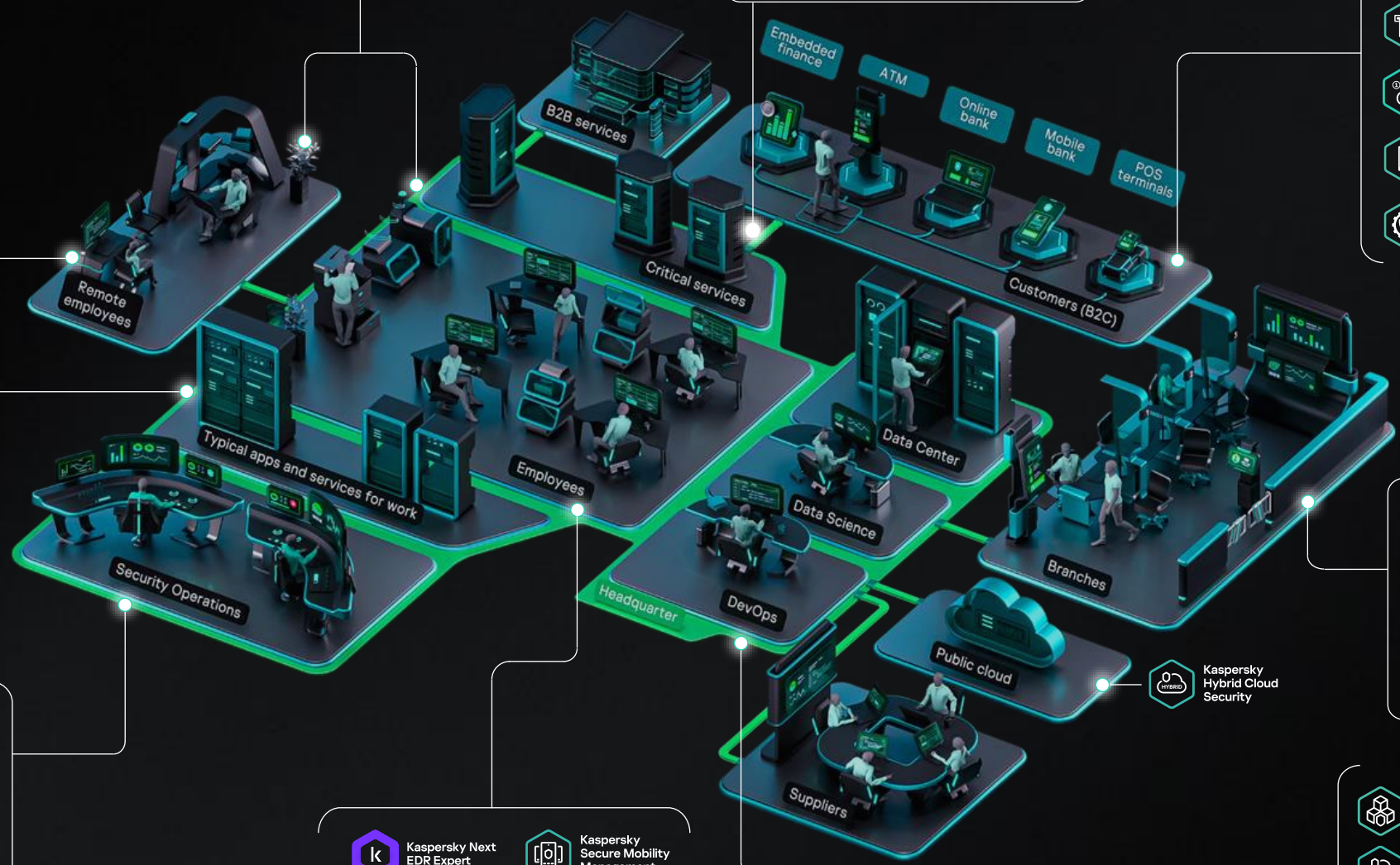
2 Knowledge

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

3 Expertise

- **Assessment** — Kaspersky Security Assessment; Kaspersky ATM Security Assessment
- **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

How Kaspersky protects financial organizations



Kaspersky Thin Client

Kaspersky DDoS Protection

Kaspersky Fraud Prevention

Kaspersky Next EDR Foundations

Kaspersky Next EDR Optimum

Kaspersky Scan Engine

Kaspersky Embedded Systems Security

Kaspersky ATM Security Assessment

Kaspersky Mobile Security SDK

Kaspersky Who Calls SDK

Kaspersky Security for Mail Server

Kaspersky Next EDR Optimum

Kaspersky Embedded Systems Security

Kaspersky Secure Mobility Management

Kaspersky SD-WAN

Kaspersky Hybrid Cloud Security

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Next XDR Expert

Kaspersky Anti Targeted Attack

Kaspersky Threat Intelligence

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Kaspersky SOC Consulting

Kaspersky Security Services

Kaspersky Next EDR Expert

Kaspersky Secure Mobility Management

Kaspersky Next EDR Optimum

Kaspersky Automated Security Awareness Platform

Kaspersky Container Security

Kaspersky Hybrid Cloud Security

Kaspersky Open Source Software Threats Data Feed

What you gain from a strong cybersecurity strategy

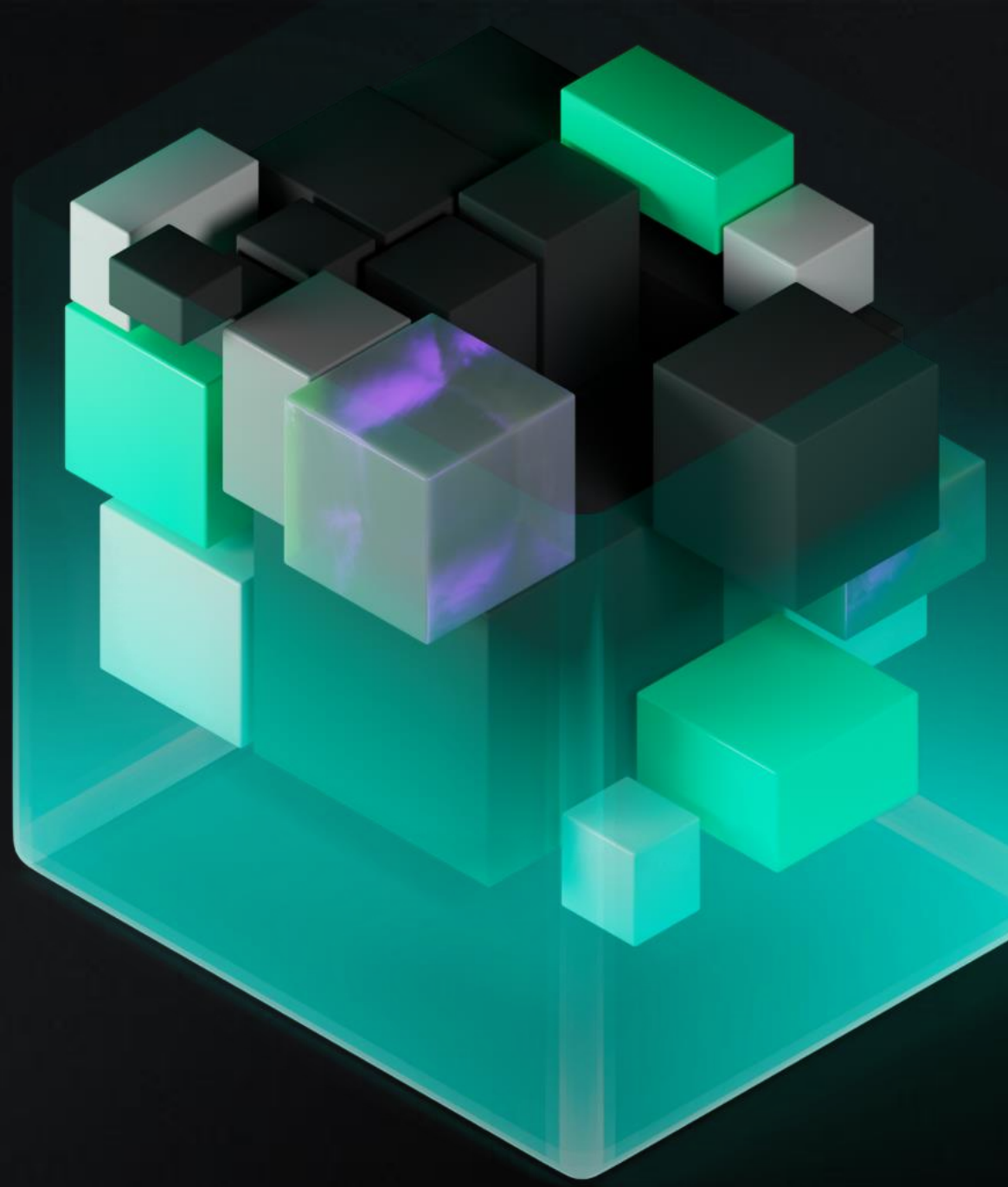
- Resilient, fault-tolerant infrastructure
- Sensitive data is protected
- Minimized financial risk
- Regulatory compliance

- Business continuity and always-on service availability
- Trust from customers and partners
- Freedom to focus on what matters most

04

Product and service cards

The Kaspersky portfolio — protecting and supporting your priorities



Effective cybersecurity strategies to protect the integrity of Financial Services: Tools

Comprehensive protection against all threats

Cyber control across all potential attack vectors, asset protection, and full coverage of security scenarios.

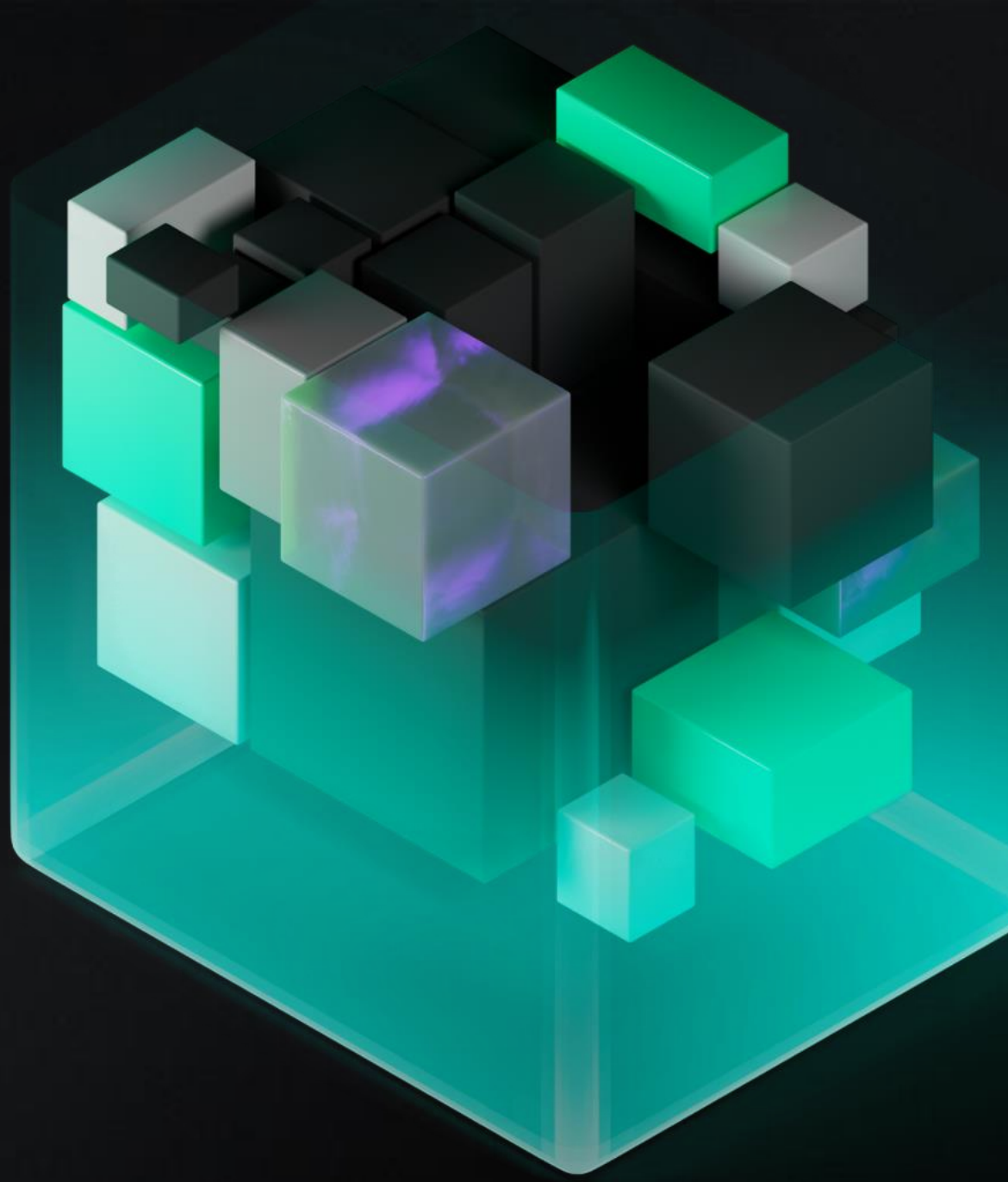
Tailored solutions for the financial industry

Designed to meet industry-specific needs, including regulatory requirements and unique threat landscapes.

Beyond traditional cybersecurity

We don’t only protect IT systems and processes – we also create a unified, secure network, delivering cyber-immune solutions built for the future.

Comprehensive threat coverage



Kaspersky Next

1 Technologies

Combines strong endpoint protection and controls with the transparency and speed of EDR and the visibility and powerful tools of XDR, in straightforward product tiers

Strong, proven endpoint defense

Kaspersky Next EDR Foundations

EDR for small cybersecurity teams

Kaspersky Next EDR Optimum

Ultimate tool for large cybersecurity or SOC teams

Kaspersky Next XDR Expert

Kaspersky Next EDR Expert

Comparison of Kaspersky Next tiers

1 Technologies

Kaspersky Next EDR Foundations → Kaspersky Next EDR Optimum → Kaspersky Next XDR Expert

Each tier includes the features and capabilities of the previous tier

Kaspersky Next EDR Foundations provides straightforward, affordable protection to keep your business running smoothly while Kaspersky blocks ransomware, fileless malware, zero-day attacks and other emerging threats.

Kaspersky Next EDR Optimum provides strong endpoint protection, improved controls, training, patch management and more, enhanced by essential EDR functionality.

Threat visibility, investigation and response are simple, quick and guided to help deflect attacks rapidly and with minimal resources.

Kaspersky Next EDR Expert provides a comprehensive view of endpoints across the corporate infrastructure and visualization of every stage of the investigation process. Equipped with advanced detection engines and root cause analysis tools, it ensures effective threat detection and streamlined investigations.

Kaspersky Next XDR Expert combines best-in-class endpoint protection, security for email and hybrid environments with the advanced detection capabilities of Kaspersky Next EDR Expert. It includes a powerful correlation engine, automated responses, and supports third-party connectors to centralize data.

Return to the scheme

1 Technologies

Kaspersky Next EDR Foundations

Product page

Kaspersky Next EDR Foundations' powerful ML-based endpoint protection, flexible security controls and EDR root cause analysis tools equip you with the most straightforward way to build a strong core for your cybersecurity. A simple console, flexible deployment options (cloud or on-prem), and features designed to improve day-to-day workflows all help reduce complexity and increase efficiency.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Knowledge gaps
- Shortage of specialists
- Stringent regulations
- Budgetary constraints

How we help

Secure every endpoint in your financial infrastructure

Provide a single console for centralized endpoint management

Protect against exploits and encryptors, assessing and remediating vulnerabilities at endpoint level

Help monitor programs, devices and applications running on servers

Support all major operating systems and virtualization tools

Kaspersky Next EDR Optimum

Product page

Return to the scheme

1 Technologies

Kaspersky Next EDR Optimum provides strong endpoint protection, improved controls, training, patch management and more – all enhanced by essential EDR functionality. Threat visibility, investigation and response are simple, quick and guided to help you deflect attacks rapidly and with minimal resources.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Knowledge gaps
- Shortage of specialists
- Stringent regulations
- Budgetary constraints

How we help

- Secure every endpoint of your financial infrastructure
- Provide a single console for centralized endpoint management
- Protect against exploits and encryptors, assessing and remediating vulnerabilities at endpoint level
- Monitor programs, devices and applications running on servers
- Support all major operating systems and virtualization tools
- Block file, email and web threats, and prevent intrusions

Kaspersky Next EDR Expert

Product page

Return to the scheme

1 Technologies

Kaspersky Next EDR Expert is a powerful Endpoint Detection and Response (EDR) solution that works together with an Endpoint Protection Platform (EPP) to block mass attacks, detect more complex cyberthreats – helping you to proactively investigate incidents, and equipping your IT specialists with comprehensive response tools.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Shortage of specialists
- Stringent regulations

How we help

- Block mass threats and detect and help investigate complex threats across your endpoint infrastructure
- Enhance the detection of complex threats and targeted attacks by combining EPP and EDR technologies into a single solution
- Provide comprehensive visibility across all roles in your financial organization's infrastructure
- Optimize incident handling costs at endpoint level
- Provide the tools for proactive threat hunting and retrospective analysis
- Support a variety of response measures

Kaspersky Next XDR Expert

Product page

Return to the scheme

1 Technologies

The most advanced tier of the Next product line, Kaspersky Next XDR Expert is a powerful cybersecurity tool for your SOC team that delivers total control over your protected infrastructure through full visibility, real-time correlation, and automation - leveraging a wide range of response tools and data sources, including endpoint, network and cloud data.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

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

How we help

Provide a comprehensive overview of your entire protected corporate infrastructure to identify complex and persistent threats, and improve MTTD

Ensure that mass threats are stopped automatically, without disturbing your information security experts , through superior endpoint, hybrid cloud and email security

Help establish response processes to improve MTTR and minimize errors in common scenarios through playbooks and advanced case management

Protect the confidentiality of customer data processing by offering data sovereignty without compromise via our on-premises installation

Enable the rapid detection of suspicious activity in the infrastructure and help minimize potential harm caused by cyber-incidents with AI components

Use powerful built-in and custom connectors to hundreds of sources from Kaspersky and third-party vendors to reduce the number of configuration-related tasks your security teams have to perform

Return to the scheme

1 Technologies

Kaspersky Secure Mobility Management

Product page

Kaspersky Secure Mobility Management provides a unified solution for managing your mobile fleet, combining leading security technologies with mobile lifecycle management best practices. It supports all major platforms and ensures compliance by aligning with regulatory recommendations. Effortless integration into the Kaspersky security ecosystem transforms corporate mobility into a secure, organic component of your IT infrastructure, streamlining workflows and enhancing overall effectiveness and efficiency.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Legacy systems
- Budgetary constraints
- Stringent regulations
- Attack surface expansion

How we help

Provide strong security and management for different types of mobile device through a single integrated solution

Enable more effective incident containment and accountability through unified management and XDR ecosystem integration

Reduce your operational costs and employee workload by automating repetitive lifecycle management tasks

Minimize the risk of human error — a critical requirement in the tightly regulated Banking & Finance sector

Help ensure compliance with institutional and regulatory requirements through a comprehensive suite of management, protection, and security policy enforcement tools

Kaspersky Hybrid Cloud Security

Product page

The solution mitigates security risks inherent in cloud environments, including malware, phishing and network threats, and reduces virtualization resource consumption. Kaspersky Hybrid Cloud Security increases business resilience and provides effective protection for hybrid environments, regardless of the cloud used.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Attack surface expansion
- New vulnerabilities and threats
- Shortage of specialists
- Stringent regulations

How we help

- Protect hybrid environments regardless of the type of workload and cloud you use
- Support a wide range of cloud platforms and virtualization environments
- Increase visibility of your hybrid infrastructures and reduce IT incidents
- Provide a single management console for your entire cloud infrastructure
- Maximize the return on your hybrid infrastructure investment through optimized lightweight agents
- Support ongoing compliance with regulatory requirements

Kaspersky Security for Mail Server

Product page

Kaspersky Security for Mail Server protects your primary communication channel – email – by blocking spam, email-borne infections, and all forms of phishing. It also helps control information transfer, reducing the risk of business disruption, financial losses due to scams, and data leaks.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Attack surface expansion
- New vulnerabilities and threats
- Budgetary constraints
- Legacy systems

Return to the scheme

1 Technologies

How we help

Provide trusted, secure corporate email exchange without sacrificing communications speed

Reduce the risk of infection and data leaks through advanced content filtering rules

Deliver comprehensive protection by detecting and blocking malware, ransomware, spam, phishing, BEC, APTs, etc. using ML-based technologies

Leverage trusted external sources of threat intelligence as well as our own leading research and Threat Intelligence data

Enable the analysis of objects in isolated environments and detection of even carefully disguised malware through integration with KATA

Enable easy integration with existing infrastructure, complementing email security solutions already in place

Kaspersky Anti Targeted Attack

Product page

Return to the scheme

1 Technologies

A comprehensive anti-APT solution that protects against sophisticated cyberthreats with network sandboxing, advanced NDR and EDR capabilities. By securing key attack entry points across both network and endpoint levels, Kaspersky Anti Targeted Attack delivers full visibility across your entire IT infrastructure and total protection against targeted attacks.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Attack surface expansion
- New vulnerabilities and threats
- Budgetary constraints
- Stringent regulations
- Shortage of specialists

How we help

Provide advanced protection against targeted attacks at network, mail and endpoints levels

Minimize the risks of leaks and financial losses through proactive risk detection and hunting for threats and anomalies

Reveal attacks targeting your infrastructure with advanced detection technologies and proactive threat hunting

Analyze network traffic and identify both external and internal network threats

Provide a comprehensive overview of all devices in the network, associated threats, and assets that require priority attention

Use global analytical data on current APTs and threats targeting financial organizations

Return to the scheme

1 Technologies

Kaspersky Unified Monitoring and Analysis Platform

Product page

The Kaspersky Unified Monitoring and Analysis Platform is high-performance next-generation SIEM solution for centralized collection, analysis and correlation of information security events from multiple sources – enabling fast detection and response to cyber incidents. It's a critical technology for any financial organization building its own SOC.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Attack surface expansion
- Knowledge gaps
- Budgetary constraints
- Shortage of specialists
- Stringent regulations

How we help

Detect attacks on your banking infrastructure by collecting, normalizing, storing and correlating events from an array of different sources

Minimize losses from fraudulent transactions by detecting them early and suspending processing, together with any other cybercriminal activity

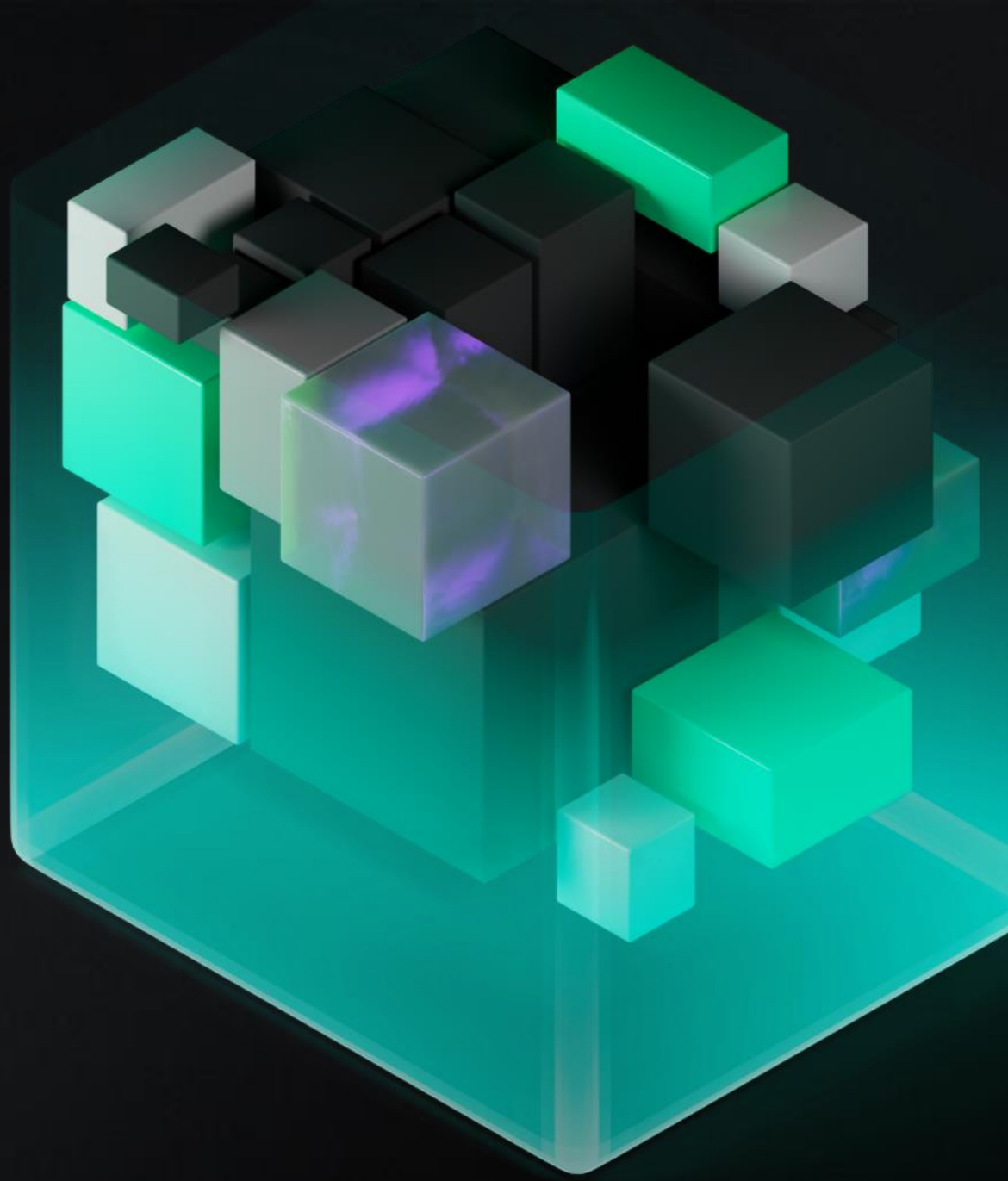
Optimize routine monitoring, alert prioritization and proactive search processes by leveraging AI

Provide a solution for reliable and cost-effective log storage with easy search of stored data

Improve the speed of detecting sophisticated attacks on your organization's infrastructure

Help you meet regulatory requirements cost-effectively, with secure local log storage

Solutions designed to meet your sector's unique challenges



Kaspersky Embedded Systems Security

Product page

Kaspersky Embedded System Security delivers robust protection tailored to the unique challenges of embedded devices like ATMs and payment terminals. It secures Windows-based devices (including those running obsolete versions such as Windows XP) as well as Linux-based devices. The multi-layered technology stack provides the best security possible for devices with different power levels, while also supporting compliance.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Legacy systems
- Stringent regulations
- Attack surface expansion

How we help

Optimize costs by providing effective protection for your mixed fleets, including low-power ATMs and POS with limited system resources

Enable more effective incident containment and accountability through unified security with centralized event logging

Provide high resilience against external interference and insider threats

Support different embedded platforms (Windows, Linux) and different types of devices

Help ensure compliance with regulatory requirements

Reduce your operational costs through high stability and minimal reliance on direct maintenance

Kaspersky Scan Engine

Product page

Kaspersky Scan Engine is a powerful threat detection and mitigation solution that easily integrates with a wide range of applications. It operates over HTTP and ICAP protocols to scan network traffic and transmitted objects., and integrates seamlessly with information systems, web apps, proxy servers, network data storage, and email gateways.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Attack surface expansion
- Management and protection of complex infrastructure
- Stringent regulations

Return to the scheme

1 Technologies

How we help

Protect your financial systems from file-based threats uploaded by customers

Filter malicious, phishing and advertising URLs

Neutralize infected files, archives and encrypted objects

Protect your files and backup storage

Provide extensive integrations with a wide range of platforms and enterprise systems

Kaspersky Mobile Security SDK

Product page

A set of libraries that lets you quickly build secure applications by integrating security features during development. Kaspersky Mobile Security SDK creates a secure environment for mobile banking apps and ensures safe access to your financial organization's servers, detecting and blocking a wide range of common cyberthreats.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Attack surface expansion
- Stringent regulations

Return to the scheme

1 Technologies

How we help

- Ensure that your customers' mobile devices are reliably protected
- Ensure secure transmission of financial information to designated recipients only
- Block access to malicious and phishing websites and SMS messages
- Support compliance with security rules and policies
- Reduce the number of successful fraud attempts against your customers
- Help maintain customer loyalty by keeping fraudulent activity to a minimum

Kaspersky Who Calls SDK

Product page

Kaspersky Who Calls SDK is a set of libraries that can be integrated into your organization's mobile apps to protect customers from spam and fraudulent calls. The application, with built-in Kaspersky Who Calls SDK libraries and AI algorithms , can identify, flag and block suspicious calls in real time. These features are also available through the Kaspersky Who Calls REST API web service, which can be integrated into your PBX system.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Stringent regulations
- Attack surface expansion
- Knowledge gaps

How we help

Identify calls from phone numbers and messaging apps

Identify and block fraudulent and advertising/spam calls

Provide detailed information about the phone number, including its reputation

Enrich your internal anti-fraud systems with valuable data

Reduce the number of successful fraud attempts against your customers

Help support and maintain customer loyalty

Return to the scheme

1 Technologies

Kaspersky Fraud Prevention

Product page

Our session-based anti-fraud technology detects complex fraud schemes early and in real time across digital channels, including websites and mobile apps.
By combining a wide range of technologies, Kaspersky Fraud Prevention boosts the security of your financial institution's customers and enhances the customer experience you provide.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Attack surface expansion
- Knowledge gaps
- Budgetary constraints
- Stringent regulations

How we help

- Detect account takeovers, unauthorized access and fake accounts
- Identify social engineering fraud
- Reduce costs related to claims and two-factor authentication (SMS, push notifications, etc.)
- Reveal abuse of marketing campaigns and bonus programs
- Help detect money laundering or terrorist financing
- Reduce fraud while improving the customer experience
- Enhance fraud monitoring with enriched data
- Support compliance with national and international regulations

Return to the scheme

1 Technologies

Kaspersky DDoS Protection

Product page

Kaspersky DDoS Protection minimizes the impact of DDoS attacks, ensuring continuous availability of the entire infrastructure and of critical online resources - such as customer services. The solution includes everything necessary to protect against all types of DDoS attack and mitigate their consequences – continuous traffic analysis, potential attack alerts, traffic redirection to scrubbing centers and the return of 'clean' traffic to the network.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

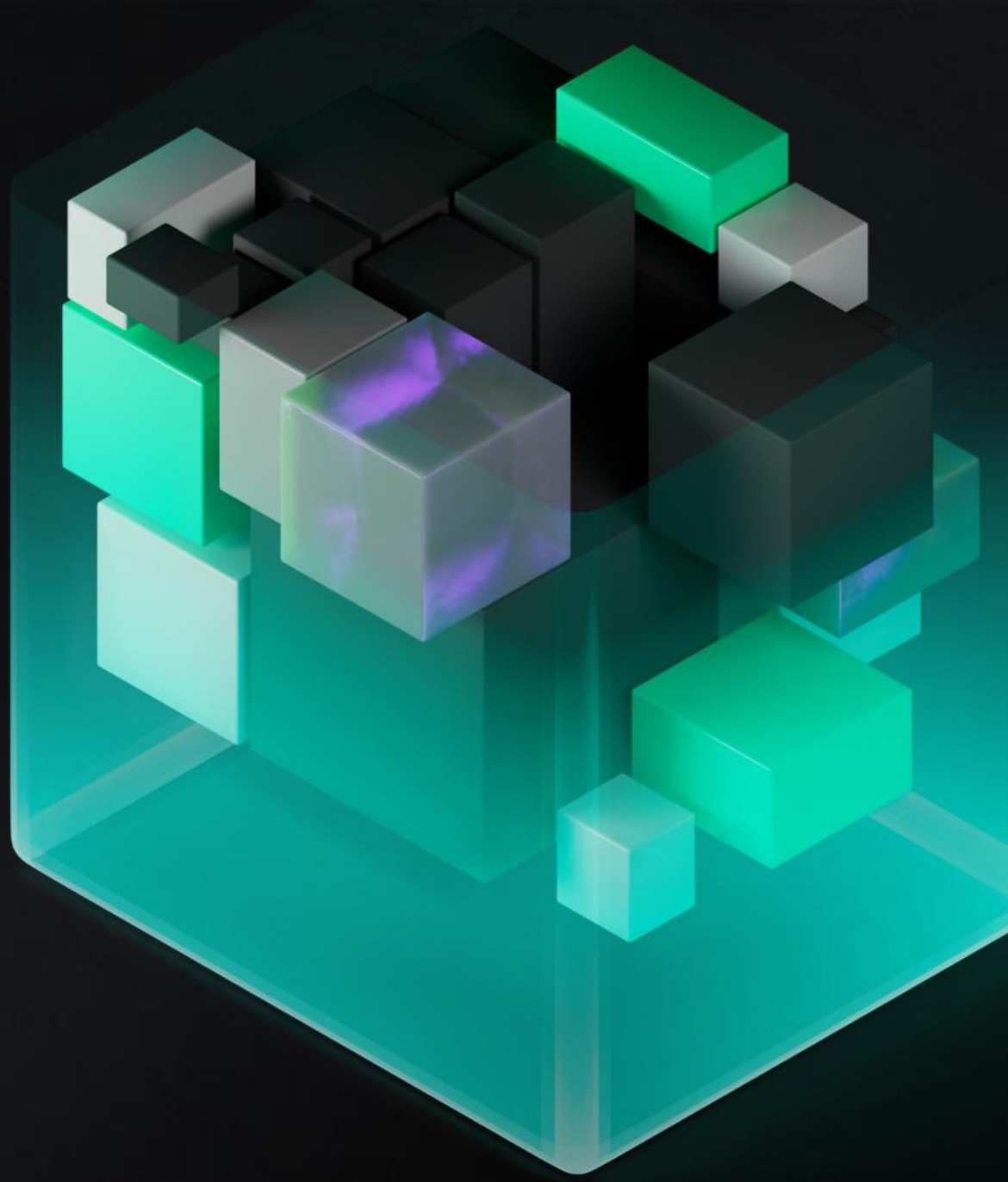
Challenges addressed

- New vulnerabilities and threats
- Attack surface expansion
- Budgetary constraints
- Shortage of specialists
- Stringent regulations

How we help

- Detect and filter DDoS attacks right from the first packet
- Ensure exceptionally high – 99.95% – availability of your infrastructure and services
- Ensure the security of your financial organization's web resources, including simulating bot attacks
- Protect encrypted traffic without exposing your TLS certificates
- Provide integration capabilities with WAF solutions to protect against threats
- Support regulatory compliance

Beyond traditional cybersecurity



Kaspersky Container Security

Product page

Return to the scheme

1 Technologies

The solution secures containerized applications at all stages of their lifecycle. Kaspersky Container Security seamlessly integrates into the software development process, takes into account the specifics of your containerized environment and protects every component — from container image registry to orchestrator. User-friendly widgets help you monitor product health and detect security incidents.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Attack surface expansion
- Knowledge gaps
- Stringent regulations

How we help

Provide security for containerized applications, whether internal or client-oriented

Protect applications at every step of development and operation

Audit your infrastructure and applications for compliance with regulations

Increase the transparency of your development environment and processes

Support major orchestrators, CI/CD platforms and image registries

Accelerate the release of client-oriented applications and services

Return to the scheme

1 Technologies

Kaspersky SD-WAN

Product page

Kaspersky SD-WAN builds fault-tolerant, scalable and secure networks with unified management, addressing the challenges associated with traditional WANs. The solution allows you to use diverse communication channels, rapidly connect new locations with a zero-touch experience, optimize costs and cloud connections, enhance the security and improve the performance of applications, and speed up the implementation of new services.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Management and protection of complex infrastructure
- Budgetary constraints
- Legacy systems
- Stringent regulations
- Shortage of specialists

How we help

- Enable easy, rapid connections between new offices, ATMs and data centers
- Manage the entire network through a single console, modifying CPE settings and security policies
- Ensure data transfer and financial apps performance
- Easily integrate security tools as well as cloud services
- Optimize the cost of communication channels and infrastructure maintenance
- Reduce the number of IT incidents as well as Mean Time to Restore
- Optimize routine tasks and network monitoring
- Remove the need for in-branch specialists

Kaspersky Thin Client

Product page

Kaspersky Thin Client is a cyber immune thin client infrastructure based on KasperskyOS. The thin clients are designed to provide users with access to remote desktops and serve as a replacement for local workstations. Thanks to our cyber immune approach, thin clients based on KasperskyOS are secure by default. The solution quickly integrates into your infrastructure and receives settings automatically.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Management and protection of complex infrastructure
- Attack surface expansion
- Stringent regulations

Return to the scheme

1 Technologies

How we help

Provide secure cyber-immune workstations for employees

Monitor user network connections to remote desktops

Ensure the security of data transmitted between your employees and financial infrastructure

Provide a centralized management system for your cybersecurity and IT specialists

Enable flexible management and control of your entire thin client infrastructure, which can contain up to 100,000 nodes

Effective cybersecurity strategies to protect the integrity of financial services: Knowledge

2 Knowledge

Threat intelligence

We provide reliable, relevant threat data in various formats. Advanced, unique analytics strengthen security systems and support informed decision-making.

Cyber awareness

Training programs build employees' cybersecurity skills and encourage their practical use in everyday operations.

Incident response training

Hands-on training equips experts to analyze digital evidence, detect and investigate malware, and respond effectively to incidents.

Kaspersky Security Awareness

Product page

Return to the scheme

2 Knowledge

A portfolio of solutions designed to boost corporate engagement with security and reduce human-related incidents, using a flexible approach tailored to different staff levels. Our finance-specific, game-based training helps executives and managers implement effective cybersecurity strategies, while our automated platform empowers employees to adopt safe behaviors – strengthening overall corporate resilience by proactively defending against threats.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerability & threats
- Knowledge gaps
- Stringent regulations
- Attack surface expansion

How we help

- Reduce and prevent human-related security incidents
- Add another layer of protection to your overall security by upskilling your workforce
- Identify and address gaps in employee knowledge
- Boost employee engagement in protecting confidential data
- Adjust security settings based on employee training outcomes
- Equip staff to recognize signs of an attack and respond appropriately

Kaspersky Threat Intelligence Portal

Product page

The portal provides access to all human-readable threat intelligence data through a unified web interface, where services work together to enhance each other. By combining expert knowledge and experience with data processing and analysis technologies, the portal helps financial organizations effectively deal with the cyberthreat landscape.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Attack surface expansion
- Knowledge gaps
- Shortage of specialists

How we help

- Provide a single access point to up-to-date and reliable threat intelligence for early attack prevention
- Enhance internal specialists' knowledge about threats and improve incident response efficiency
- Offer a flexible threat search service and correlation tools to accelerate incident investigation
- Help protect brand reputation by tracking digital assets and threats across darknet resources
- Strengthen file analysis using sandboxing, attack attribution, and file similarity detection
- Deliver a relevant threat landscape overview based on industry and regional specifics
- Provide reports on threats related to APT groups and financially motivated cybercriminals
- Help analysts track cybercriminal infrastructures

Kaspersky Threat Data Feeds

Product page

Return to the scheme

2 Knowledge

More than 30 ready-to-use threat intelligence data feeds are available to address various cybersecurity challenges faced by financial organizations. These data feeds provide information on known malware, phishing websites, the latest vulnerabilities, exploits, and more, enhancing security solutions. Kaspersky Threat Data help security teams detect threats and prioritize incidents that require immediate remediation, enriched with valuable context from Kaspersky's diverse sources.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Attack surface expansion
- Knowledge gaps
- Shortage of specialists

How we help

Enhance security solutions, including SIEM, XDR, firewalls, IPS/IDS, and security proxies, with continuously updated indicators of compromise and actionable context

Enrich SIEM systems with high-quality threat intelligence and relevant context, improving detection quality and reducing false positives

Integration with TI platforms, including Kaspersky Cyber Trace, for effective threat intelligence management and proactive cyber threat protection

Enable integration of high-confidence indicators into perimeter security solutions, including third-party NGFWs, for real-time threat blocking

Help security teams quickly identify critical alerts and prioritize them for incident response teams

Protect the software development process from threats related to open-source components

Kaspersky Digital Footprint Intelligence

Product page

A comprehensive digital threat protection service that helps organizations monitor their digital assets and detect threats across both the visible web and the darknet. With real-time alerts, Kaspersky Digital Footprint Intelligence enables quick and effective responses to potential threats.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- New vulnerabilities and threats
- Attack surface expansion
- Knowledge gaps
- Shortage of specialists

Return to the scheme

2 Knowledge

How we help

Provide comprehensive monitoring of all digital assets s that could be targeted or compromised

Identify network resources and services that may be potential attack vectors

Monitor fraudulent activities that may damage the company's reputation or mislead customers

Detect compromised employee, partner, and customer data, including bank card details

Deliver continuous darknet monitoring for any mentions of the client's organization online

Prevent negative impacts on business operations

Kaspersky Cybersecurity Training

Product page

Return to the scheme

2 Knowledge

Our comprehensive set of training programs is designed to strengthen your IT security team's skills in malware analysis, reverse engineering, threat hunting and incident response, enabling them to mitigate your organization's risk and respond effectively to incidents. By enhancing the knowledge and skills of your in-house specialists, we help you retain your cybersecurity professionals and avoid having to recruit additional specialists.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Attack surface expansion
- Stringent regulations
- Knowledge gaps
- Shortage of specialists

How we help

Develop your IT security team's specialized skillsets and capabilities

Reduce and mitigate your recruitment needs in the face of the global skills shortage

Increase the effectiveness of your threat detection and accelerates incident response

Empower your staff to fully manage the protection of your infrastructure, without the need for external expertise

Promote risk mitigation and team effectiveness

Show your commitment to valuable staff by helping them gain recognized cybersecurity qualifications that benefit them – and your organization

Effective cybersecurity strategies to protect the integrity of financial services: Support

Managed protection

24/7 managed security provided by Kaspersky experts to detect and stop growing cyberthreats.

Consulting and security assessment

Comprehensive assessment of systems and security measures to ensure resilience.

Professional services

Deployment, maintenance, and optimization of Kaspersky products to maximize their benefits.

Kaspersky Application Security Assessment

Product page

Kaspersky Application Security Assessment service helps identify vulnerabilities across web and mobile apps, online banking and other systems. Leveraging expert analysis with advanced tools, the service focuses on uncovering weaknesses in application architecture and business logic, providing actionable insights to strengthen security.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Knowledge gaps
- New vulnerabilities and threats
- Shortage of specialists
- Attack surface expansion

How we help

- Provide comprehensive expert-led assessment for critical applications
- Identify software vulnerabilities and logic flaws in applications
- Deliver expert recommendations to enhance application security
- Minimize financial losses through early detection of vulnerabilities in apps
- Reduce the risk of data breaches and fraud by uncovering weaknesses in business-critical systems
- Safeguard business operations and protect your reputation by uncovering and fixing critical flaws in apps

Kaspersky Penetration Testing

Product page

Kaspersky Penetration Testing involves the proactive identification and exploration of attack vectors targeting your critical assets. By simulating real-world attacker behavior and applying relevant tactics, techniques, and procedures (TTPs), our team demonstrates the potential impact on key business processes — regardless of the complexity of your infrastructure — within a controlled, secure environment.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Legacy systems
- New vulnerabilities and threats
- Shortage of specialists
- Attack surface expansion

How we help

- Uncover exploitable vulnerabilities across the infrastructure
- Minimize financial losses though early detection of critical vulnerabilities
- Assess your organization's resilience to real-world cyberthreats targeting your infrastructure
- Prioritize security measures for maximum impact
- Protect data and prevent fraud by uncovering weaknesses in your infrastructure
- Provide expert recommendations to enhance infrastructure resilience

Kaspersky Red Teaming

Product page

Return to the scheme

3 Expertise

Kaspersky Red Teaming simulates a real hacker attack, assessing your detection and response capabilities in order to help you protect critical business functions. The service is delivered by security experts who ensure confidentiality, integrity, and availability while following international standards and best practices.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Knowledge gaps
- New vulnerabilities and threats
- Shortage of specialists
- Attack surface expansion

How we help

- Assess Blue Team detection and response capabilities
- Evaluate resilience against attacks on critical business functions
- Share actionable insights to strengthen your security posture
- Enhance resilience to targeted attacks with realistic, industry-relevant simulations
- Reduce the risk of breaches and operational disruption by uncovering weaknesses in critical systems
- Minimize financial losses through early detection of key risks

Kaspersky ATM Security Assessment

Product page

Return to the scheme

3 Expertise

Kaspersky ATM Security Assessment is an expert-led service that uncovers vulnerabilities in your ATM/POS systems. Combining real-world attack simulations with in-depth expert analysis, it identifies potential exploits and provides actionable recommendations to strengthen the security of your payment infrastructure.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Legacy systems
- New vulnerabilities and threats
- Shortage of specialists
- Attack surface expansion

How we help

- Assess the security posture of your ATM / POS infrastructure
- Identify exploitable vulnerabilities in your payment systems
- Provide tailored recommendations to strengthen ATM / POS systems
- Analyze potential breach scenarios and the consequences of a cyberattack
- Prevent fraud and service disruptions by identifying vulnerabilities in ATM / POS devices
- Prioritize security measures to enhance payment systems resilience

Kaspersky Managed Detection and Response

Product page

Kaspersky Managed Detection and Response (MDR) offers round-the-clock managed protection against cyberthreats and sophisticated attacks that traditional automated security measures miss.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Attack surface expansion
- New vulnerabilities and threats
- Shortage of specialists
- Budgetary constraints
- Stringent regulations

How we help

- Provide 24/7 monitoring and proactive threat hunting for your expert teams
- Detect and respond to threats proactively, using AI-driven insights
- Refocus your in-house IT security resources to deal with business-critical issues
- Deliver actionable reporting to help guide informed decision-making
- Reduce security costs overall — no need to keep hiring and training more expensive IT security professionals
- Minimize potential downtime and financial losses through the early detection of advanced threats and cyberattacks

Kaspersky Incident Response

Product page

Kaspersky Incident Response provides a complete, detailed picture of an incident. The service covers the full incident investigation and response cycle, from initial response and evidence collection to identifying the primary attack vector and preparing an attack mitigation plan.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Shortage of specialists
- New vulnerabilities and threats
- Stringent regulations
- Budgetary constraints
- Knowledge gaps

How we help

- Rapid containment of threats to prevent further damage
- Provide detailed forensic analysis to uncover attack vectors and root causes
- Rebuild an incident timeline and determine the root cause
- Provide tailored remediation plans to restore operations
- Minimize the risk of data breaches and financial penalties by accelerating incident recovery
- Offer expert guidance to enhance your long-term security posture

Kaspersky Compromise Assessment

Product page

Return to the scheme

3 Expertise

Kaspersky Compromise Assessment focuses on uncovering active cyberattacks as well as previous unknown attacks that may have flown under the radar of your IT security tools and processes.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Shortage of specialists
- New vulnerabilities and threats
- Stringent regulations
- Knowledge gaps
- Budgetary constraints
- Attack surface expansion

How we help

- Conduct a thorough investigation to uncover hidden threats
- Provide information about the behavior and functionality of specific malware files
- Deliver a comprehensive report with actionable recommendations
- Provide expert guidance on addressing the identified risks, strengthening your defenses
- Conduct an impartial evaluation of the risk of infrastructure compromise
- Reduce the risk of data breaches and financial losses by detecting hidden threats

Kaspersky SOC Consulting

Product page

Return to the scheme

3 Expertise

Kaspersky SOC Consulting empowers your organization to build and optimize your own Security Operations Center. From architecture design to process improvement, the service helps ensure efficient detection and response to evolving cyberthreats.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Shortage of specialists
- New vulnerabilities and threats
- Stringent regulations
- Budgetary constraints
- Knowledge gaps

How we help

- Design or optimize your SOC architecture for enhanced efficiency
- Implement best practices to streamline your processes and workflows
- Assess your SOC's maturity and identify areas for improvement
- Deliver training to upskill your in-house SOC team
- Reduce operational costs through streamlined SOC processes
- Improve the efficiency of threat detection and response

Kaspersky Professional Services

Product page

Kaspersky Professional Services provides expert support to optimize and secure your IT environment. Leveraging Kaspersky's advanced solutions, our experts deliver tailored support to enhance infrastructure protection and build resilience against sophisticated cyberthreats.

Priorities supported

- Customer engagement
- Resilient infrastructure
- Digital trust and stewardship

Challenges addressed

- Knowledge gaps
- Legacy systems
- Shortage of specialists

How we help

Provide security solutions specifically designed to meet the needs of financial organizations

Offer continuous support to ensure your security systems always perform optimally

Handle routine security tasks, allowing your team to focus on higher-priority issues

Improve the performance and effectiveness of your security infrastructure

Strengthen your infrastructure against advanced and evolving cyber risks

Optimize your cybersecurity spend to deliver better value and protection

05

Our experience, clients, and success stories

Kaspersky's track record in the finance sector

We help financial organizations minimize risk through proven technologies and deep expertise.
Our solutions follow global best practices in cybersecurity.

> 15 years

> 100 countries

>3,400
BFSI around the world

~1900
in CIS

~430
in APAC

~530
in Europe

~360
in Americas

~230
in META

Success stories

See the full case study

Bank in Italy

Banca Popolare di Sondrio

Challenges

- Dissatisfied with previous IT security solutions
- No clear roadmap provided by the previous vendor
- Concern that the previous vendor couldn't keep up with evolving security needs
- The bank needed a fast, effective, and easy-to-manage solution to defend against cyberattacks

The bank was introduced to Kaspersky through Kaspersky Endpoint Security. Its successful implementation exceeded expectations, leading to the subsequent purchase of Kaspersky Private Network Security and Kaspersky Anti Targeted Attack.

Kaspersky solutions

- Kaspersky Anti Targeted Attack
- Kaspersky EDR Expert
- Kaspersky Endpoint Security for Business

> 2600
Employees

330
Branches

2
Data centers

Success stories

See the full case study

Bank in the Dominican Republic

Challenges

- Rising number of cyberattacks targeting the national financial sector
- Business growth and new services required stronger cybersecurity
- Outdated security solutions made it difficult to protect the entire infrastructure

> The Bank's CTO: «The company's business and strategy areas are technology-oriented, with security at their core. The impact of where we are going involves many financial instruments that require greater security. We need to be at the forefront»

Kaspersky delivered a complete solution that includes not just products, but expert services.

Kaspersky solutions

- Kaspersky Anti Targeted Attack
- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Security for Business
- Kaspersky Professional Services

\+ Enhanced Support with Technical Account Manager

500 Employees

31 Branches

Success stories

See the full case study

Islamic Bank in Bangladesh

aibl
আল-আরাফাহ ইসলামী ব্যাংক পিএলসি
Al-Arafah Islami Bank PLC.

Challenges

- Weak national infrastructure and lack of clear regulation
- No centralized control over day-to-day operations
- No built-in protection for ICT networks and systems
- Frequent large-scale malware outbreaks and infections
- Risk of complete branch shutdowns, blocking efforts to offer online banking services

Consequences

- Multiple virus, worm and Trojan attacks on local systems and across the bank's network
- Uncontrolled access to malicious websites and use of unauthorized USB devices

Outcome

- Systems now run smoothly and securely
- Infected USB devices are blocked, and access to harmful websites is restricted

To address ongoing and future potential threats, the bank has deployed Kaspersky Endpoint Security for Business.

Kaspersky solutions

Kaspersky
Endpoint Security
for Business

2600+
Employees

119
Branches

1000+
Users

06

Why Kaspersky

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

>220,000

corporate clients worldwide choose our protection

>900

active groups and operations associated with APT are monitored by us

5

unique Centers of Expertise

Technology leadership build 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

5 Centers of Expertise

Our unique team of experts work together across five centers of expertise, combining specialized knowledge and skills to tackle the most sophisticated, dangerous cyberthreats.

This collaborative approach strengthens our state-of-the-art protection technologies and ensures our products and solutions set the industry standard for security and reliability.

Driving innovation, ready for tomorrow's challenges

1,500+

successfully registered patents

500+

inventions between 2005–2024

20+ years

For over 20 years we've used ML and AI to stay ahead of evolving cyberthreats.

Our dedicated AI Technology Research Center drives innovation while ensuring AI and ML are used securely and ethically.

KasperskyOS

Be Immune

Our groundbreaking KasperskyOS enables the shift from cybersecurity to Cyber Immunity.

kaspersky cyber immunity

Cyber Immunity is our approach and methodology for developing secure-by-design solutions

5 key ways AI enables us to protect our customers better than anyone else

AI at the core of our portfolio

1. AI- and ML-powered threat discovery
2. Enhancing SOC efficiency through AI
3. GenAI for Threat Intelligence and Security Operations
4. Secure AI approaches and methodologies
5. AI-based behavior analysis and anomaly detection in IT and OT environments

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

Learn more

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.

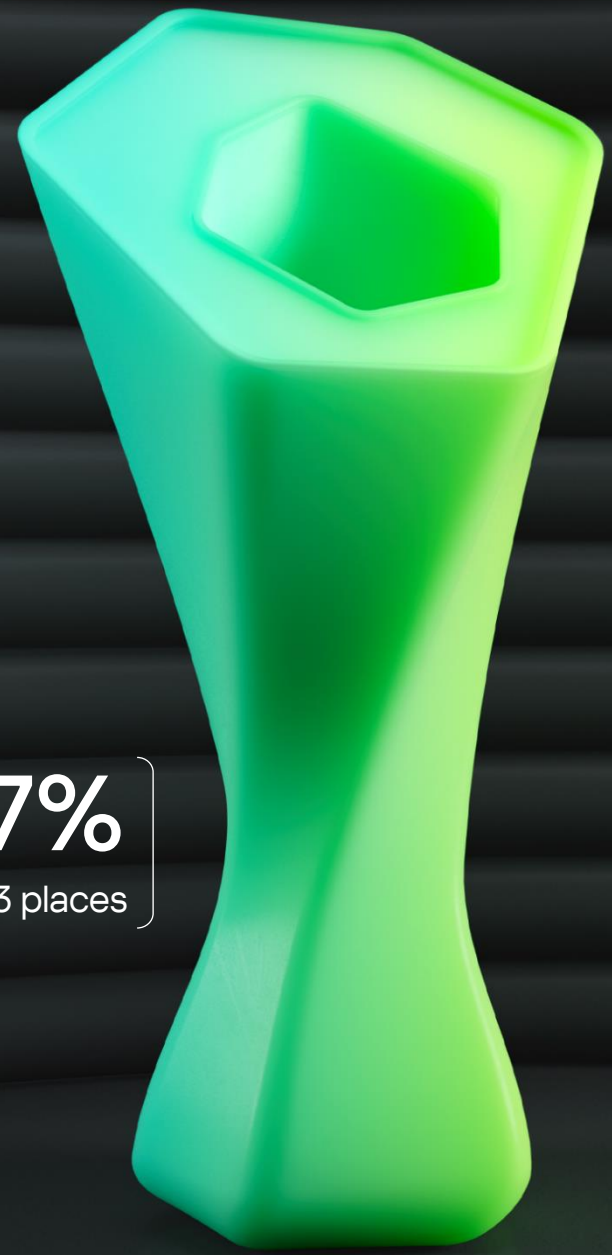
Most tested. Most awarded.

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.

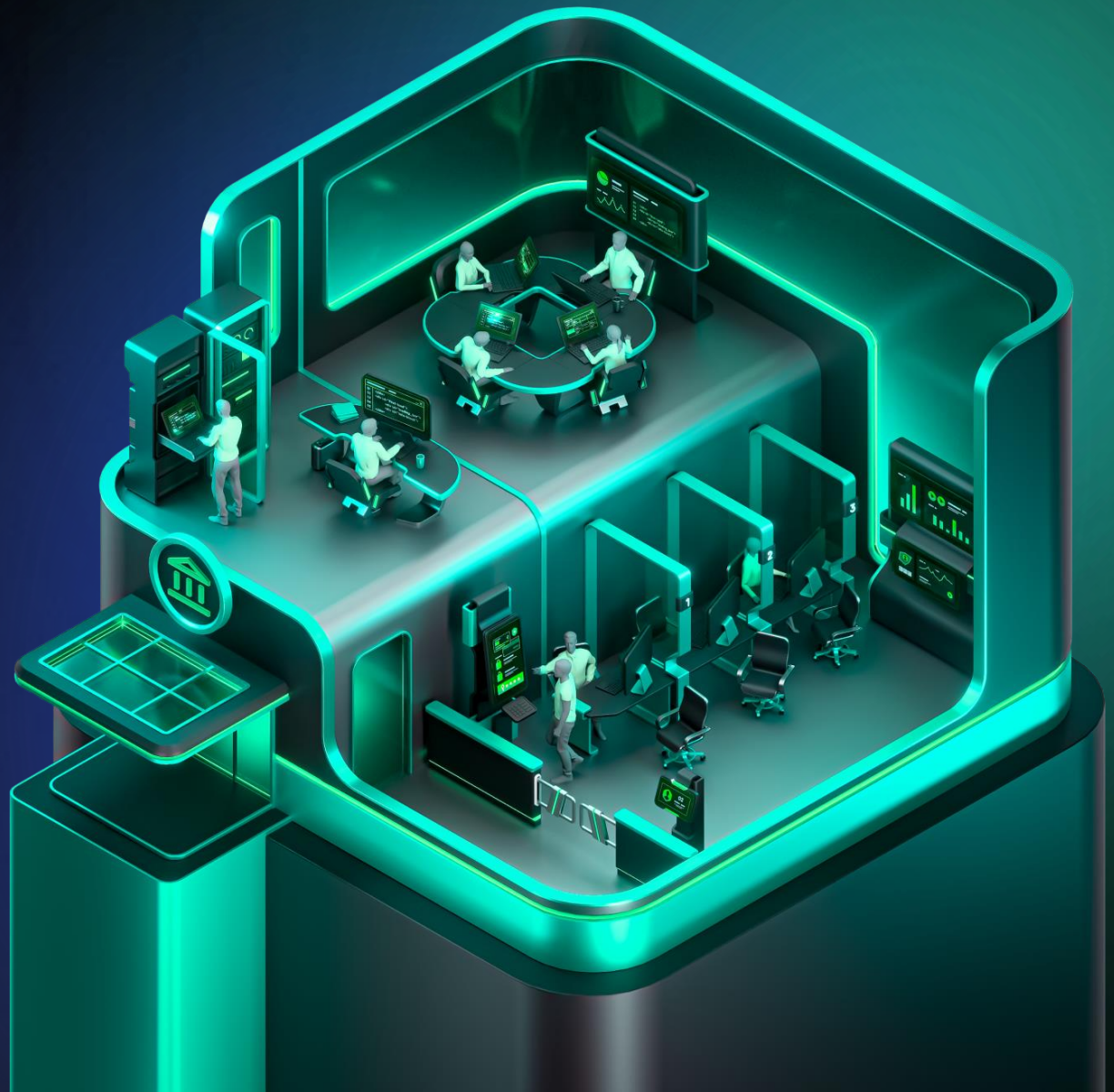
MITRE | ATT&CK®

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 leading companies such as Adobe, Microsoft, Google, Apple, etc.

kaspersky



Thank you for your attention!

Contact us to learn more about cybersecurity for financial services

Learn more