

Cybersecurity for
small and mid-sized
businesses

What makes your growing business stronger

43%* of attacks target SMBs

1 week to 6 months

Potential downtime



= \$70 000*

The average cost of an incident (data loss, phishing, ransomware, fraud, reputational damage)

What's happening — and why it matters to your business

Cloud platforms, remote work, mobile devices, online tools and services and AI-driven automation make many aspects of day-to-day operations easier, but they also add complexity and make it harder to keep systems secure.



More tools, more entry points

Every new service adds another potential door into your business



Limited time and staff

Small IT teams can't monitor everything, all the time



Work outside company control

Using personal accounts and devices for work puts data outside protection and exposes the business to potential fines



More attacks powered by AI

AI enables low-cost, automated phishing and password attacks at scale

All of these factors threaten business continuity and growth, leading to:

- potential financial losses,
- data breaches,
- and reputational damage.

What puts your business at risk — inside and out

Most cyber incidents don't start with something dramatic. They start with everyday situations and current challenges.

External and internal risks



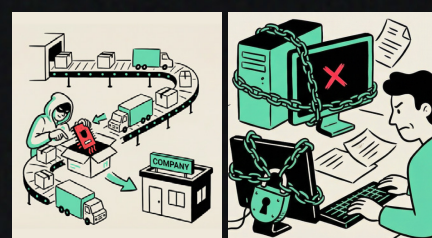
Ransomware → Operations grind to a halt



Social engineering → Stolen credentials, business disruption



Malware and fileless attacks → Data theft, unstable systems



Supply chain attacks → Disruption to customers and a resulting loss of trust

Challenges



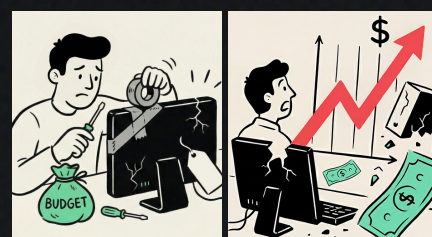
Fast IT growth → Security can't keep up



Skill shortage in incident handling → Wrong decisions make situations worse

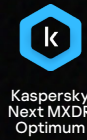
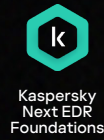


Overloaded IT → Missed threats and delayed response



Limited budget → Higher recovery costs later

How Kaspersky addresses threats and challenges



	Malware + <i>Common threats</i>	•	•	•	•
	Ransomware	•	•	•	•
	Fileless attacks	•	•	•	•
	Phishing	•	•	•	•
	Unknown malware <i>New & targeted</i>		•	•	•
	Human error		•	•	•
	Uncontrolled third parties		•	•	•
	Social engineering			•	•
	Lateral movement			•	•
	Lack of resources				•
	Business continuity				•

Managed service from Kaspersky experts

What reliable security means for you

Automatic threat protection

Built-in protection against mass threats reducing the need for manual response

Lower workload for IT

Fewer manual tasks, fewer mistakes, more time for what matters – with streamlined cloud-based deployment

Early threat detection

Stop evasive threats before they become incidents

Fast recovery if something goes wrong

Less downtime – more business stability and less lost revenue

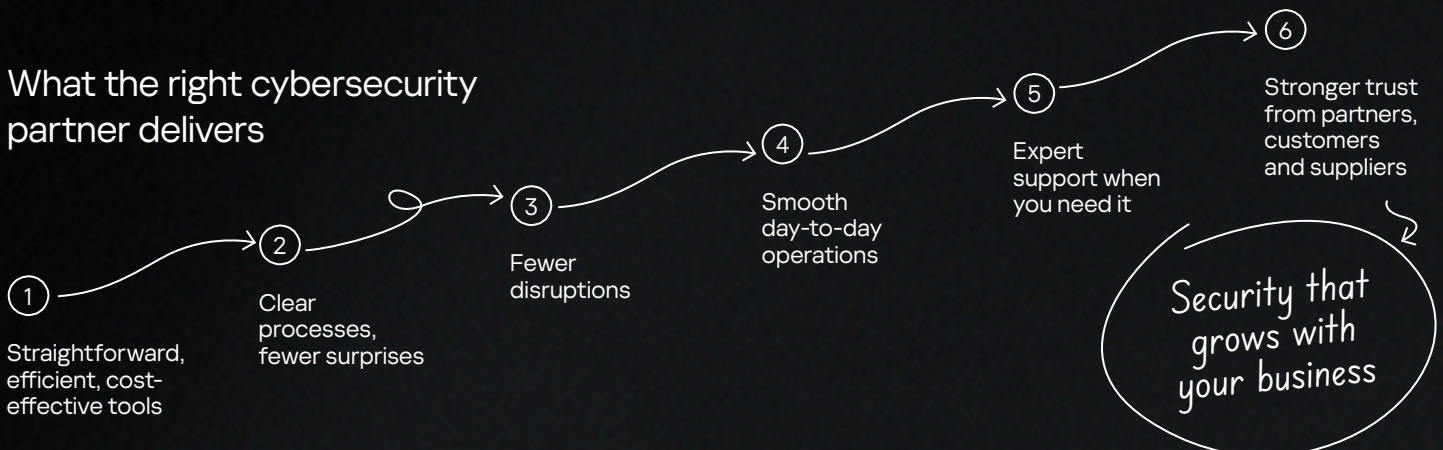
Protection against social engineering

Cybersecurity training that helps employees spot scams, phishing and manipulation

Expert security without building a team

Strong protection without the cost and hassle of hiring specialists

What the right cybersecurity partner delivers



Ready for cloud-native security built for you?

Get protection that works from day one

Contact us

www.kaspersky.com

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.