
Smart
investment
into EDR-class
protection
and why your
business needs it

A buyer's guide to optimum level of security

Executive summary

For years, SMBs and mid-size enterprises have been able to rely on their endpoint protection platform (EPP) to defend their businesses against an extensive range of commodity threats. But with cybercriminals increasingly turning to new, unknown and evasive threats that can bypass the EPP, it's time to upgrade these defenses with endpoint detection and response (EDR) and/or managed detection and response (MDR) solutions capable of protecting against such threats.

This buyer's guide explains how to identify the optimum EDR-class security for your business in eight easy steps. You'll want to start by reviewing your existing endpoint protection to identify any critical gaps in your endpoint defenses. You'll also need to be clear about what you want to achieve, and identify the protection that best fits your needs by thinking about your use cases. And you should take a serious look at both EDR and MDR, consider these solutions within your broader security landscape, and draw up list of key capabilities required from potential vendors.

By reading this guide, you'll have a clear understanding of why and how to upgrade your defenses, the benefits of the available solutions, and how to create an optimum security solution that not only matches the needs of your business, but also the specialist security skills of your IT team.

Why upgrade your defenses – and why now?



Advanced cybersecurity solutions like endpoint detection and response (EDR) are one of the hottest topics in the market – and with good reason. Especially if yours is a small to medium-sized business (SMB) or mid-size enterprise.

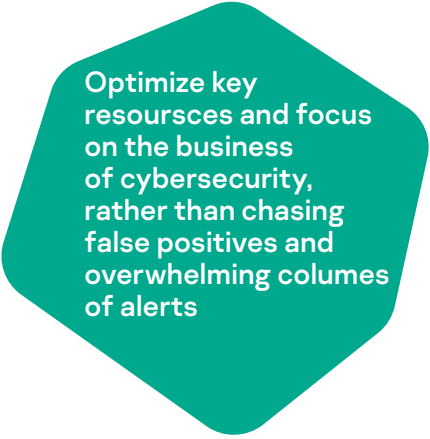
Why these segments in particular? Changes in the cybersecurity landscape mean today's attackers are focusing on organizations of all sizes, spheres of activity and levels of preparedness. More specifically, high-end SMBs and mid-size enterprises are under fire from the more advanced evasive threats previously only directed at much larger organizations.

In response, IT security teams have been supplementing their existing endpoint protection platforms (EPP) with EDR and/or managed detection and response (MDR) solutions enabling them to detect and investigate security incidents, contain the threat at the endpoint, and receive an automated response and/or guidance for remediation.

Unfortunately, adopting these solutions can sometimes cause as many issues as it solves – by alerting security teams to enormous volumes of threats which, although suspicious and requiring investigation, ultimately turn out to be harmless. This can be a particular problem for IT teams with limited in-house security expertise or time with which to deal with these alerts.

The ideal solution is therefore one that supplements endpoint protection with EDR-class security that significantly lightens the EDR workload – as the more threats that are prevented, the less noise is created for security teams to investigate. This in turn means that IT security teams can optimize key resources and focus on the business of cybersecurity, rather than chasing false positives and overwhelming volumes of alerts.

So what changes to the threat landscape are driving the need for more advanced protection? How do these vary for different types of businesses? And (perhaps most crucially of all, given the global shortage of skilled cybersecurity talent) how can you effectively address these threats with a solution that best fits your organization, the size and security skills of your IT team, and the types of cyberattack to which you're potentially exposed?



Optimize key resources and focus on the business of cybersecurity, rather than chasing false positives and overwhelming volumes of alerts

This buyer's guide will help you, by outlining:

- Why existing endpoint security won't ensure protection against the new threat landscape.
- How to assess your evolving security requirements.
- How to identify the protection that best fits your needs – both in terms of the threats to which you're increasingly exposed, and the security skills of your IT team.
- What to do if you have only limited time, headcount and/or in-house security expertise.
- How the latest solutions fit within the broader security landscape.

Why existing endpoint security won't ensure protection against the new threat landscape

When it comes to enhancing your endpoint security, it's easy to think that this is simply a matter of identifying and implementing an EDR solution that seems a good fit for your business. But in the same way that it would be inadvisable to add an extra floor to a building without first checking the foundations, your first step should be to review your existing EPP.

IDC¹, for example, has suggested:

Do not accept substandard or weak EPP as it corrupts the results of the complete endpoint solution¹. A company should not make up for weak EPP with EDR (and a lot of security analyst time).

- Before discussing considerations for EDR, IDC would first recommend that you look at your existing EPP solution. The expectation for EPP should be that it protects endpoints as an independent solution.
- Do not accept substandard or weak EPP as it corrupts the results of the complete endpoint solution. A company should not make up for weak EPP with EDR (and a lot of security analyst time).

EPP plays a vital role in enabling any business to protect itself against an extensive range of commodity threats, and minimize IT security workloads. But when it comes to evasive threats you need to go further.

To reduce the risks presented by the new threat landscape, you therefore need to start by assessing the effectiveness of your existing endpoint protection and identifying any potential gaps in your defenses.

Why you may not be as well protected as you think

While you might think your business is well protected, it's estimated that in the first half of 2019 alone there were nearly **4,000** data breaches², putting more than four billion users' data at risk.

This alarming figure is quoted in the introduction to IT security economics in 2019, the Kaspersky report summarizing the results of our annual Global Corporate IT Security Risks Survey. The survey involved interviews with almost 5,000 SMBs and enterprises in 23 countries, and revealed some concerning statistics of its own. For example:

55%

of organizations are 'completely confident' that their network hasn't been hacked, despite 38% feeling they lack sufficient insight on the threats facing their business.

12%

of enterprises are concerned about malware infection, despite it being the costliest security incident for them.

51%

of enterprises and 47% of SMBs agreed it's becoming more difficult to tell the difference between a generic or a targeted security attack.

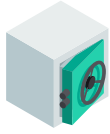
66%

of both enterprises and SMBs were looking to increase their investment in specialist IT staff in 2020, despite critical global shortages – especially in cybersecurity.

¹ IDC Doc # US45794219 - Endpoint Security 2020 The Resurgence of EPP and the Manifest Destiny of EDR - Jan 2020

² <https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report>

What these figures suggest is a dangerous disconnect between organizations' perceptions of the cyberthreat landscape, which types of attack pose the greatest potential risks (including financial), and their preparedness and ability to defend themselves.



For enterprises, malware infection on company-owned devices is actually the form of data breach with the biggest financial impact, costing **US\$2.73 million** in 2019 – despite only 12% of enterprises feeling 'very concerned' about malware infection as a threat.



SMBs too are ignoring their most expensive forms of attack. The costliest type of data breach for smaller businesses were incidents affecting IT infrastructure hosted by a third party, adding up to **US\$162,000**. However, SMBs only ranked this the fifth most important measure, and instead were most concerned about data protection issues, such as the loss of a physical device, or data loss through a targeted attack.



The fact that enterprises and SMBs are finding it more difficult to tell the difference between generic and targeted security attacks is making it harder for them to detect or evaluate the potential harm of the incidents they're experiencing – a possible reason why they're becoming susceptible to growing levels of both moderate and advanced malware threats.

The report concluded by saying 'It's vital that businesses keep investing and rethinking their IT security processes in order to stay one step ahead of the growing rates of cyberattacks, and to limit any financial losses incurred'. But they can only achieve that by effectively addressing the actual threats to which they're increasingly being exposed – i.e. by investing in the EDR-class security needed to protect against evasive threats.

Step 1: Review your existing endpoint protection



With so many advanced cybersecurity solutions available on the market, it's easy to forget the vital role played by your endpoint protection. Why are endpoints so important? Not only are they the most common entry points into a business's infrastructure – and cybercriminals' primary target – they're also key sources of the data needed for effective investigation of complex incidents.

As a result, every organization should choose an EPP delivering automated protection against the large numbers of possible incidents caused by commodity threats – including fileless threats and ransomware.

Because this type of setup requires relatively limited specialist security knowledge or personnel, it meets the endpoint security needs of SMBs or small enterprises without a dedicated security team, or organizations with very low levels of cybersecurity expertise.

It's also a crucial foundation stage for midsize and larger enterprises where, by dealing automatically with large numbers of minor threats, the solution can clear the way for security teams to focus on more advanced defense where needed.

When reviewing your EPP to assess if it's delivering the capabilities you should expect, you need to consider:



How effective is it?

How many false positives are you receiving?

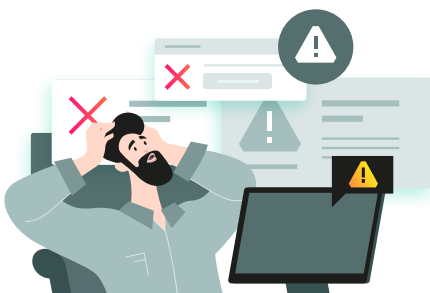
Does it offer effective attack surface reduction capabilities like web, application and device controls?

Does it help to automate routine tasks?

Is it easy to operate, and helping to minimize costs and overheads on your IT team?

Does it help with critical tasks such as vulnerability assessment and patch management?

Step 2: Identify any critical gaps in your endpoint defenses



While your EPP will protect against an extensive range of commodity threats, you also need to consider your defense against new, unknown and evasive threats that are bypassing your EPP.

Preparing an attack is becoming cheaper for cybercriminals, putting more organizations at risk. And as well as occurring more frequently, these kinds of attacks have become much more effective due to criminals combining, testing and using varied techniques in order to effectively bypass endpoint security.

The urgent need to deal with these threats has also become increasingly critical due to changes such as the dissolving of corporate perimeters resulting from the surge in remote working.

Telltale signs that it's time to expand your defenses beyond traditional EPP therefore include:

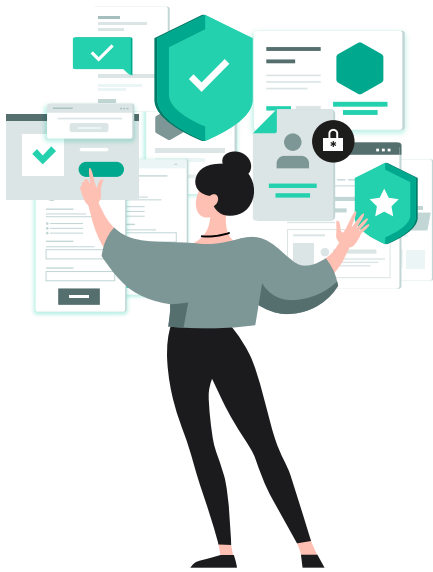
- Your EPP is failing to stop an increasing number of new, unknown and evasive threats.
- You have limited visibility into what's happening on your endpoints. This includes being unable to undertake root cause analysis, investigation and real-time threat response – or having to do this manually, with standard operating system (OS) tools on a case-by-case basis, which is slow, complex and error-prone.
- You don't have the specialist IT security skills or capacity needed to deal with increasingly sophisticated threats.
- You're concerned about potential fines, or the threat to your business's reputation resulting from a major security incident.

The best use of all the functions you actually need, rather than paying for large numbers of functions you don't really want

To implement an effective solution to defend against these threats, you'll need to consider aspects of your organization including its size, corporate profile, security preparedness, existing resources and expertise – and in particular the security skill level (or 'maturity') of your IT or IT security team.

You'll also want a solution that makes the best use of all the functions you actually need, rather than paying for large numbers of functions you don't really want, and then having to try to recruit IT security experts with the skills needed to work with these.

Step 3: Be clear about what you want to achieve



According to Gartner³, EDR tools provide a method for security and risk management technical professionals to answer two key questions about the security of their environment:

- What happened here?
- What is happening right now?

Many organizations have limited expertise (or a small IT security department and no plans to expand it), but need to understand what's happening to their infrastructure and be able to respond to evasive threats before damage can occur.

Adding appropriate EDR capabilities to EPP can provide highly effective defense against more advanced and evasive threats. This should give IT security specialists the information and insights needed for effective investigation, and the tools required for root cause analysis, creating custom Indicators of Compromise (IoCs), importing IoCs, and scanning for them across all endpoints. And it should enable automated and/or fast, accurate 'single-click' responses like quarantining files, host isolation, stopping a process, deleting an object etc.

Step 4. Identify the protection that best fits your needs



Many organizations may not employ anyone dedicated specifically to IT security. Some may just be beginning to build their IT security department. And others may already have fully formed and skilled-up IT security teams. The quality of these organizations' available expertise in relation to threat defenses will therefore vary widely – as can the amount of time they can dedicate to this task.

To deal with these differing circumstances, organizations without dedicated IT security personnel, or those whose IT security staff are overloaded with routine tasks, will need to make strategic use of automation to counter the latest evasive threats.

This means supplementing their EPP with additional EDR tools which, while protecting against these threats, also incorporate appropriate levels of automation (full or partial).

³ Gartner – Solution Comparison for Endpoint Detection and Response Technologies and Solutions – Jan 2020

Tools that are as straightforward and simple as possible – saving time and reducing frustration

Alternatively, rather than investing in an overly complex EDR solution for which they may not have the necessary time or skills, managed detection and response (MDR) lets them access capabilities such as 24/7 security monitoring by industry experts, automated and managed threat hunting, and guided and remote response scenarios – either from a vendor, managed service provider (MSP) or managed security service provider (MSSP).

A third option is to combine EDR and MDR. Many organizations do not have the expertise required for threat hunting, so outsourcing this while implementing detection and response capabilities in-house is often an ideal solution. And this can be particularly beneficial for businesses that want to develop their own cybersecurity team, but lack the resources, personpower and/or skills to support specialist detection and response.

Whichever best fits your particular situation, you'll want tools that are as straightforward and simple as possible – saving time and reducing frustration. To minimize alert fatigue, you'll also want a solution that deals with large numbers of potential threats automatically.

Step 5: Think about your use cases

To identify the protection that best fits your needs, you need to set clear requirements for it. This means considering critical aspects of the solution's performance and regular use, such as the use cases you need it to fulfil and the results you expect it to deliver.

For example, when you receive a security alert, EDR and/or MDR should enable you to answer key questions such as:



It should also help you understand the full scope of the threat. For example:

If you're at risk of a global threat, your management team will likely want to be reassured you're not currently under attack, for which you'll need the ability to find an IoC online, run a scan and answer their concerns correctly.

If a regulatory authority asks you to run a scan for a specific IoC, you should be able to import IoCs from trusted sources and run periodic scans for signs of an attack.

If you've thoroughly investigated an alert, and generated an IoC based on the discovered threat, rather than running scans throughout the entire network to find if other hosts have been affected, this should be done for you automatically.

Similarly, you should be able to quickly respond to prolific, fast-moving threats by:

- Containing the threat by isolating the host, quarantining the file or preventing files being executed during the investigation.
- Automated cross-endpoint response based on IoC scans – enabling you to respond to evasive threats as soon as they're discovered.
- And, importantly, guided and remote response scenarios if you're using MDR.

Among the key results you should therefore expect from your solution include:

- Protecting against more frequent and more disruptive evasive threats.
- Saving time and resources with a simple, automated tool.
- Seeing the full scope of evasive threats over the whole of your network.
- Understanding the root cause of each threat and how it actually occurred.
- Avoiding further damage with rapid automated response.



What if you have only limited in-house security expertise?

Let's assume you have limited internal IT security expertise, or a small team of one or two security specialists. Let's also assume you're trying to decide whether to supplement your EPP with EDR and/or MDR. What kinds of benefits can you expect and what would be right for you?

Step 6: Take a serious look at both EDR and MDR

If you prefer a more hands-on approach (and your IT team has sufficiently mature IT security skills), EDR can help prevent business disruption and damage by eliminating the risks posed by new, unknown and evasive threats, and giving your security personnel the visibility needed for threat investigation, root cause analysis and response.

This can drive cost efficiencies by enabling your security team to work more effectively without having to juggle multiple tools and consoles, and maximize capacity by automating an extensive array of processes. It also gives you peace of mind by making it easy to monitor and detect threats, and respond to and prevent attacks.

If you're looking to expand your internal IT security capacity by offloading key detection and response tasks, MDR can offer advanced, round-the-clock protection from threats that can otherwise bypass automated security barriers. This can help to empower your business by solving the cybersecurity talent crisis, and supplying all the major benefits of a 24/7 Security Operations Center (SOC) without the prohibitive costs.



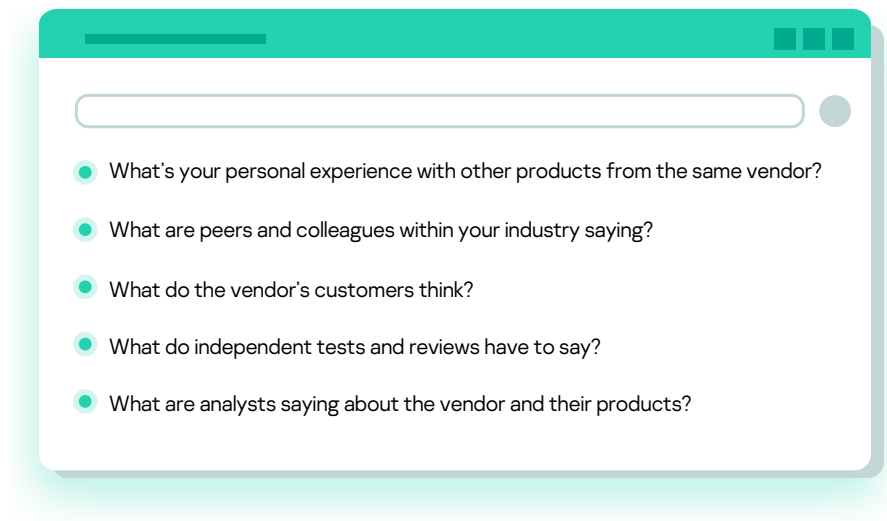
MDR can also drive cost efficiencies by focusing in-house resources on those critical tasks that really demand your IT security team's involvement, and maximize capacity by leveraging advanced machine learning models to significantly increase analyst throughput and minimize mean-time-to-respond. And it can deliver continuous security monitoring by industry experts, along with automated and managed threat hunting. This includes analysis of complex non-malware threats, and dangerous, hard to detect threats using legitimate OS tools in attacks.

Combining EDR and MDR, meanwhile, lets you tailor their respective EDR-class capabilities to your particular needs, for example by outsourcing threat hunting (for which you may not have the required expertise) while implementing endpoint detection and response capabilities in-house.

What about the bigger picture?



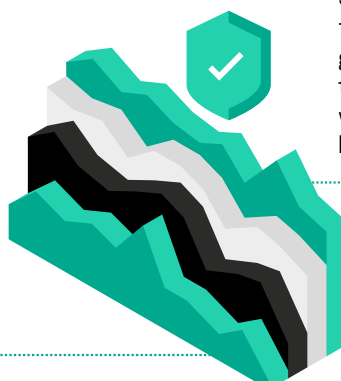
Having established your preferences for EDR and/or MDR, you'll also want to assess how the various available solutions are viewed by the market. When you're looking for a product as vital as cybersecurity, the opinions of independent experts and existing users should far outweigh any potential vendor's marketing claims. So, for example:



Step 7: Consider your broader security landscape

In many organizations, EPP, EDR and/or MDR solutions will need to integrate with and operate as part of a much broader security framework.

Alongside these solutions, you could, for example, benefit from:



Security awareness training

for your employees, which helps address gaps in cybersecurity awareness and transform employee behaviors – especially with the vast majority of cyber incidents being caused by human error.

Threat intelligence – enabling you to better deal with issues such as cyberthreats in suspicious files, URLs, IPs and domains, and investigate threats more quickly and thoroughly.

You'll also want to consider how your solution will be managed – for example by giving you a unified, single pane of glass cloud-enabled console for all the various components, and including web, on-premises and air-gapped management options.

Step 8: Ask your vendor if they offer all this:

Different vendors offer EDR and MDR solutions with (sometimes widely) differing capabilities. As a simple rule of thumb, a comprehensive solution should ideally incorporate the following.



- Quick and hassle-free deployment
- Easy and intuitive tools that do not require lengthy familiarization or retraining
- A unified management console to configure your cybersecurity tools and react to incidents from one place
- Ability to meet your specific needs and requirements with every possible deployment option: cloud, on-premises, hybrid, air-gapped
- Threat visibility
- Root cause analysis including visualization and drill-down capabilities for quicker and more convenient analysis
- IoC import, generation and scanning
- Fast and preferably automated response capabilities
- Guided response scenarios
- Automated threat hunting, supported by vendor/MS(S) P specialists
- Tightly integrated endpoint protection and endpoint detection and response functionality
- Capacity
- Integrated fileless protection
- Anti-exploit technology
- Ransomware protection
- Vulnerability and patch management functionality
- Application, web and device control, and other system hardening methods
- High performance to prevent user and network slowdowns
- Effective technical support in your local language

How Kaspersky Optimum Security can help

In independent tests, Kaspersky consistently demonstrates a higher quality of protection compared to any other vendor.

In 2019, we were Gartner Peer Insights Customers' Choice for Endpoint Protection Platforms⁴ for the third year running, and the most tested, most awarded security vendor for the seventh year in a row.

In 2020 we were also one of only six vendors worldwide to receive Gartner Peer Insights Customers' Choice recognition for Endpoint Detection and Response solutions⁵, with the highest rating of any vendor for service and support.

Other recent awards include:

- AA product rating in the [2020 NSS Labs Advanced Endpoint Protection \(AEP\) group test](#)
- The highest possible score for protection against advanced cyberthreats in [AV-Comparatives Enhanced Real-World Test](#)
- [2020 SE Labs Best Enterprise Endpoint annual award](#)

Kaspersky Optimum Security protects your business against new, unknown and evasive threats in a resource-conscious way. With it, you can quickly and easily adopt an effective threat prevention, detection and response solution, backed by support from Kaspersky experts for 24/7 security monitoring, automated threat hunting, and guided and remote response scenarios.

And, if you're looking for EPP, EDR and MDR, managed from a cloud console, a threat intelligence portal and security awareness training, Kaspersky Optimum Security enables complete protection for all your endpoints in a unified solution delivering automatic prevention, detection and response, managed protection and cyber-safety training.

Advanced threat protection

- Advanced prevention and detection mechanisms (machine learning, behavior analysis, automated threat hunting with Indicators of Attack (IoA)) maximize protection against dangerous evasive threats – building on strong EPP protection against commodity threats with Kaspersky Endpoint Security for Business
- Enhanced threat visibility provides context and details on detected threats, while simple root cause analysis and visualization tools allow you to quickly and efficiently investigate and understand the threat and how it has developed.
- Automated threat hunting helps establish and improve early, effective threat detection and response, through 24/7 continuous monitoring by industry-leading experts.
- Quick 'single-click' and cross-endpoint automated response options and IoC scans across the whole infrastructure help you quickly respond to fast-moving threats.
- Guided and remote response scenarios provide your security teams with expert analysis and responses to new, unknown and evasive threats.
- Raising employee awareness of cyberthreats, the methods used by cybercriminals, and how employees can help prevent attacks from ever happening, reduces risks of human error and social engineering.

Fast, scalable turnkey protection

- Works across workstations, laptops and servers, physical and virtual machines, public clouds and containers.
- Consolidated, multi-layered endpoint security prioritizes incidents and expedites threat discovery and investigation with threat intelligence via a convenient web portal.
- Stops known and emerging threats using industry-leading technologies that are proven to prevent ransomware, exploits, fileless and other malware attacks.

⁴ Gartner Peer Insights 'Voice of the Customer': Endpoint Protection Platforms, 10 December 2019

⁵ Gartner Peer Insights 'Voice of the Customer': Endpoint Detection and Response Solutions, 1 May 2020

Minimizes needs for additional staff or expertise

- Straightforward analysis and response processes within a single cloud-enabled console help security personnel optimize time and effort spent on investigation and remediation.
- Unified console enables single pane of glass management for major Kaspersky security applications. Cybersecurity tools can be configured and react to incidents from one place, and meet specific needs with every possible deployment option including cloud, on-premises, hybrid and air-gapped.
- 24/7 security monitoring provides round-the-clock protection, even for organizations with a lack of IT security staff.

Why invest in Kaspersky Optimum Security

Through **Kaspersky Optimum Security** we can take you from a situation where you're under significant risk of an evasive attack, to one where you have renewed confidence in your endpoint security. Rather than being unsure about what's happening in your environment, you'll have visibility and control over all of your endpoints, wherever they are. And, rather than being reluctant to upgrade security because of the complexity involved, you'll have a simplified and consolidated solution that helps optimize your resources.

You can learn more about how to get the advanced protection your business needs – while minimizing needs for additional resources – by visiting go.kaspersky.com/optimum.

Cyber Threats News: www.securelist.com
IT Security News: www.kaspersky.com/blog
Threat Intelligence Portal: opentip.kaspersky.com
Technologies at glance: www.kaspersky.com/TechnoWiki
Awards and recognitions: media.kaspersky.com/en/awards
Interactive Portfolio Tool: kaspersky.com/int_portfolio

www.kaspersky.com

kaspersky BRING ON
THE FUTURE