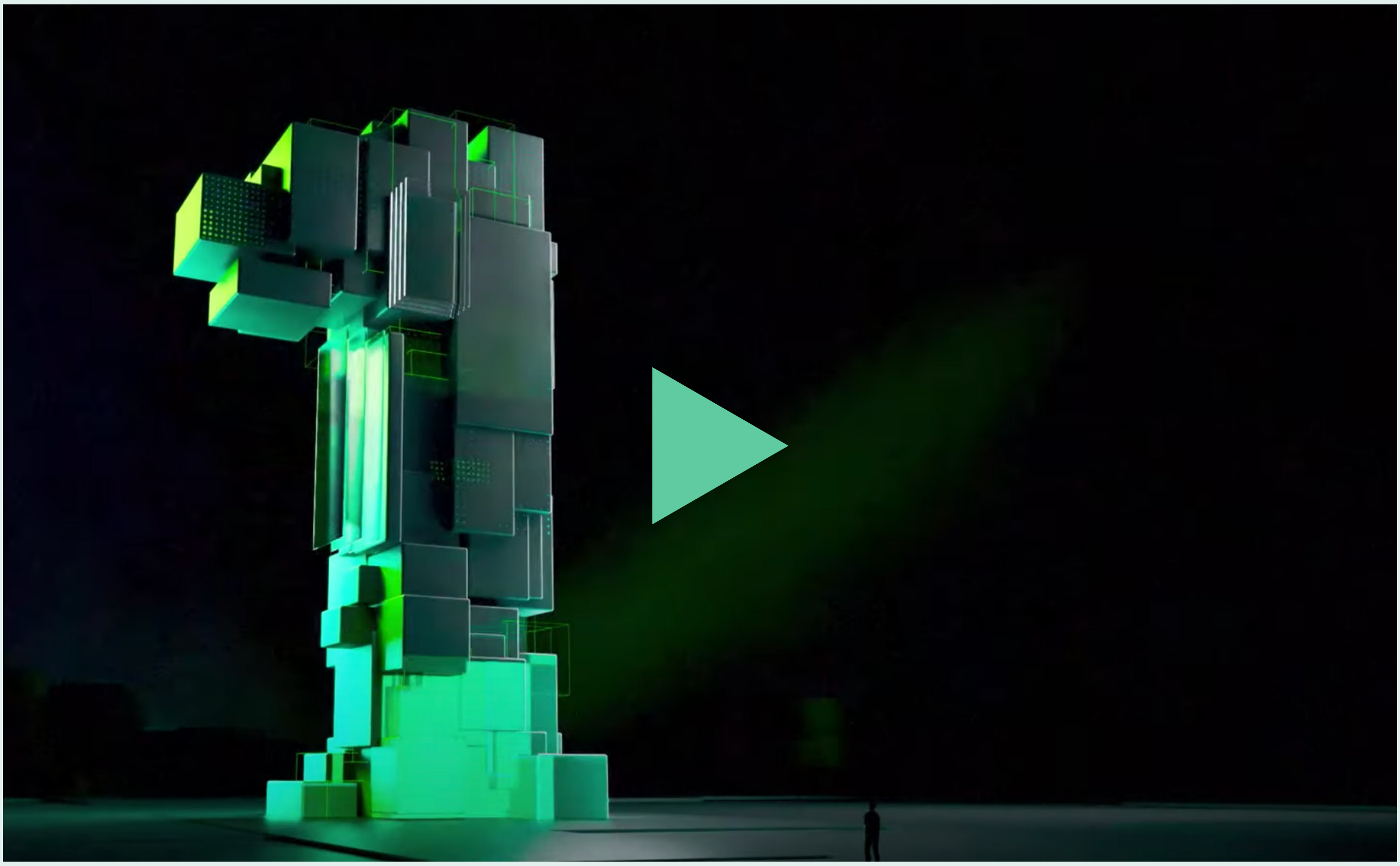
Must-have cybersecurity insights for proactive business decision makers

December 2021

kaspersky BRING ON THE FUTURE

Contents

Kaspersky Enterprise Security: One Cybersecurity Partner Sees the Big Picture



Adding expert understanding to automated cyber-protection

APTs, targeted and supply chain attacks, the increasing number of devices in use, cloud services and the Internet of Things: the cyberthreat landscape and attack points are constantly becoming more complex, and evolving quickly.

Companies say the biggest obstacles to ensuring an adequate cyber protection strategy are a lack of resources and expertise internally, and, externally, the number of regulations they're required to comply with. These issues, coupled with the fact that traditional endpoint protection is rarely enough today to detect threats early and enable us to react accordingly, mean it becomes harder to ensure the protection of critical business assets. So, what is the key to safeguarding your company against the latest threats?

Well, we definitely need to make sure we give all our decision makers the relevant information on prevailing global cyberthreats, the threat landscape generally, and most importantly we should set out the potential financial impact to the business of a breach. The modern business might need support gathering current threat intelligence from around the world to help them maintain immunity from unforeseen cyberattacks; our feeling is such businesses could benefit from a unified, integrated toolkit with multi-level threat discovery, giving the ability to secure multiple entry points from one place.

Every organisation, whether small, medium or large, ought to be addressing cybersecurity proactively and regarding it as a central business need, because overlooking or skimping on cybersecurity today could expose them to greater problems further downstream that are likely to be more challenging and costly to recover from.

The aim of this report is to help senior managers navigate the broad waters of cybersecurity, where our common destination is to protect all of your business-critical assets. It presents the latest market trends, the most pressing pain points and a step-by-step checklist. No deep tech-talk, but a helpful, comprehensive overview with key insights for all decision makers.

With this in mind, let´s get straight to business, and bring you closer to the one cybersecurity partner who sees the full picture!

Christopher Hurst
General Manager, UK&I, Kaspersky

Survey Report – Why UK business decision makers need to be more proactive about cybersecurity

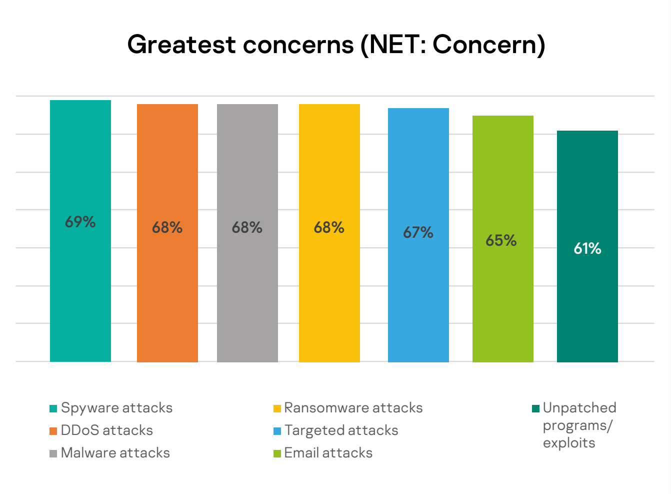
The market research institute Gartner predicts that by 2024 three quarters of all CEOs will be held personally accountable for cybersecurity incidents occurring in their companies, making it all the more important for organisations to reinforce cybersecurity measures in relation to existing and potential threats.

A recent survey by us at Kaspersky shows that most business decision makers are keen to strengthen their security solutions, however it also shows us there is still a lot of catching up to do. According to the findings, **64%** of UK business decision makers would like to be more proactive about their cybersecurity strategies – but lack the specialist knowledge to do so. Senior managers are often held back by a lack of resources or expertise, and budget pressures on them, which all obstruct the investment needed to implement the level of security they really need within their companies.

Methodology: The study was conducted by Arlington Research on behalf of Kaspersky in August 2021. 1500 business decision makers in Europe were surveyed online, 250 each from Germany, United Kingdom, France, Italy, Spain, and the Czech Republic. 62% of the decision makers questioned were employed in small and medium-sized companies with 50-999 employees, 38% work in large corporations with more than 1000 employees.

Two out of three businesses are concerned about cyber threats

Around seven out of ten of UK business decision makers (68%) are concerned about becoming victims of a cyberattack, irrespective of whether they work for a large corporation or a small to medium-sized company (68% NET: Concerned for both).



[1] Respondents were asked to respond on a scale of 1-5 how concerned they were about the threat of a number of cybersecurity attacks for their organisation (where 1 = Not at all concerned and 5 = Extremely concerned) with answers 4&5 labelled as 'Concerned'. Overall concern was a combined score, which was calculated using the average score each respondent gave for each of the attacks asked about in this question.

On average, 82% are already experiencing one or more cyberattacks; just 15% indicate that their company has so far avoided such attacks.

Inadequate protection from the state

When we are victims of theft in real life, the police usually come to our rescue. This is because we are protected by laws and rules that regulate all areas of our lives, protecting both individuals and companies from crime. The state enforces criminal law through agencies such as the police.

With cybercrime, unfortunately the situation is not the same. According to our study, 60% of UK business decision makers believe that organisations affected by cybercrime do not receive the same protection and support from the state as victims of real-life crimes.

The EU Data Protection Regulation (GDPR), and the UK equivalent, protect consumers' personal data, but the legislation places the responsibility for that protection on the company. Organisations of all sizes face a double challenge: on the one hand cyberattacks threaten their own and their customers' data, and on the other the EU data protection guidelines make them responsible for potential security incidents.

- There's little wonder that 56% of the business decision makers surveyed criticised the state support for companies in their country, saying their government provides inadequate backing or assistance to organisations impacted by cybercrime
- 68% believe their government needs to match the level of police protection and punishment for cybercrimes as exist for other types of crime
- 67% aren't at all happy they could be personally liable for any cybersecurity incidents presenting in their own company in future (see Gartner study)

Managers also report a lack of internal support, with 60% of those surveyed being concerned at the lack of support from their organisation to prevent any cybersecurity incidents.

"Business decision makers must proactively strengthen their security precautions against cyberattacks to lead their company into a secure future. An effective way to achieve this is to combine technology that automatically detects and neutralises cyber threats, with external support from experienced cybersecurity experts, leaving the internal IT team free to take care of the company's core tasks"

Christopher Hurst, General Manager, UK&I, Kaspersky

What holds back investment in cybersecurity?

A question, then: given the complex cyberthreat landscape, and potential risk of loss, why do so many businesses behave passively when it comes to implementing proactive cybersecurity measures?

Needless to say, the answer has a great deal to do with cost pressures, regardless of whether the respondents work for large corporations, or small and medium-sized companies.

In the context of the study, more than half (54%) of business decision makers stated that they have most of the resources and knowledge internally, but would need external cybersecurity experts to respond to an incident, and they lack resources to find a trustworthy partner. Most strikingly, 56.8% of respondents say it is very difficult to get budgets for improved cybersecurity within their companies.

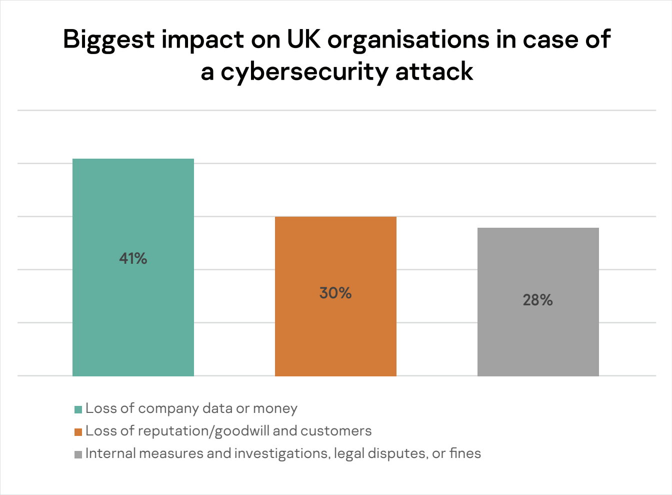
> "In fact, there are often discrepancies between the perceived needs of business decision makers and what IT and security teams actually need – a lack of specialist knowledge influences decision-making here. The solution is obvious: the more businesses proactively invest in protection against cyber threats, the higher the return on the company's future security."
>
> **Christopher Hurst, General Manager, UK&I, Kaspersky**

Cyberattacks can have serious consequences

Cyber threats are constantly evolving, becoming more and more complex, and exposing companies to a broad range of potential risks. One in ten corporate security incidents (whether malware, targeted attacks, or supply chain attacks) is classified as severe.

The business decision makers interviewed as part of the study characterise the potential effects of cybersecurity breaches in distinct ways:

- Just under half the interviewees see the loss of company data or capital (41%) as having the biggest impact on their organisation resulting from a cyberattack; nearly a third of the respondents (30%) rate damage to reputation and loss of customers as the most serious consequences; and almost as many (28%) see internal disruption, investigations, legal disputes, or fines as the most serious consequences of a security incident
- A third (34%) of business decision makers 'strongly agreed' that cybersecurity measures are already embedded into all business operations within their organisation. Interestingly, 57% of the study participants agreed they would like to on-board external security experts, but don't have the resources to find a trusted expert.



Biggest impact on UK organisations in case of a cybersecurity attack

Take the initiative against current cyber threats

This is another reason decision makers should examine whether or not their investment in preventing cyberattacks is enough to deal with all potential threats, and whether they're maybe lagging behind in terms of current tech.

In the study, more than one in five (24% NET: Agree) decision makers admit their company doesn't invest enough in preventive measures for cybersecurity. Whilst we're encouraged to see more than half (52% NET: Agree) respondents are satisfied with the existing investments, around a fifth (24% NET: Agree) think they are spending too much money. We'd summarise that companies need to re-think how they approach investing into cybersecurity - it's really not about saving money while using a solution, but about securing all assets of an organisation.

According to the study, those organisations that rely on the support of professional cybersecurity experts are almost ten percent less affected by attacks than those that work with internal cybersecurity solutions.

Business decision makers from companies of all sizes who want to comprehensively protect their organisation against cyberthreats and stay ahead of emerging risks should consider getting the professional support of an external service provider, preferably one with wide ranging experience in cybersecurity; they really need to invest in the right solutions and services in order to stay cyber-immune.

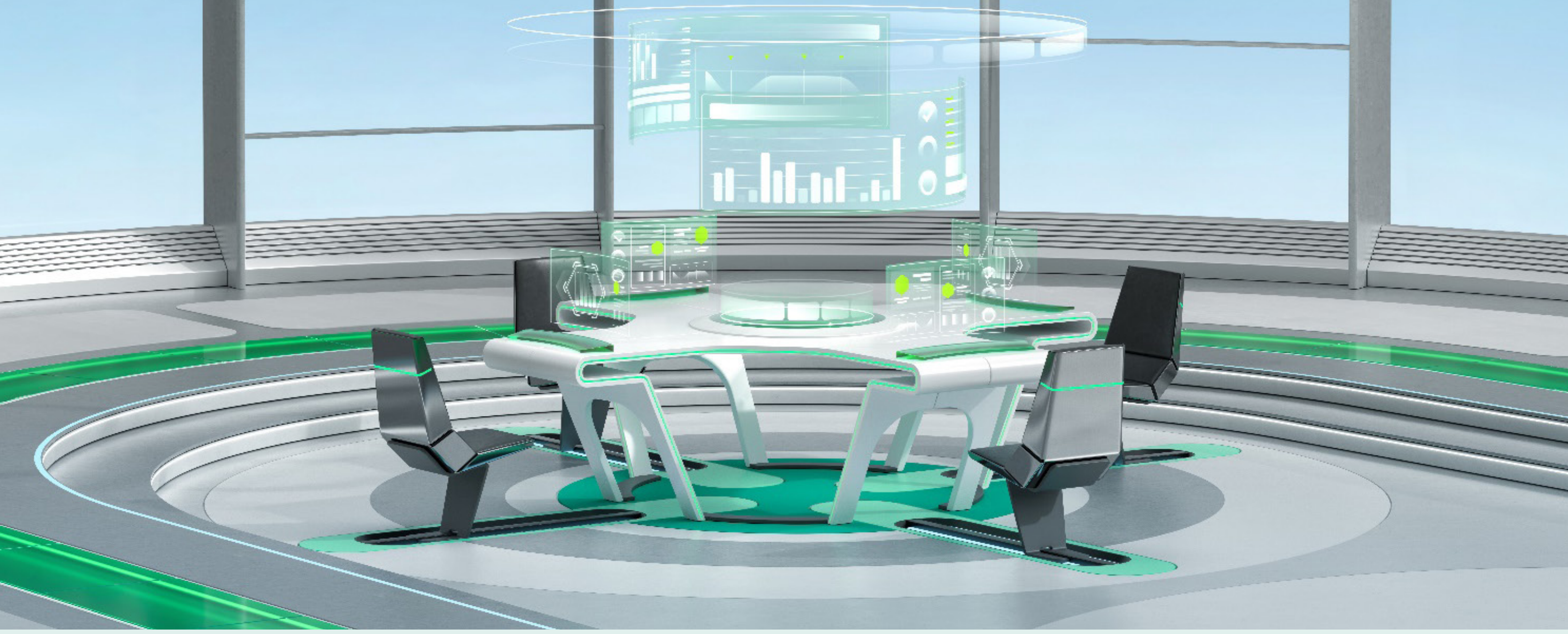
Kaspersky represents the ideal partner to achieve the best, most advanced cyber protection. The company offers a combination of automated security solutions (Endpoint Detection & Response) and MDR systems (Managed Detection and Response), through which our security experts support corporate customers in identifying and neutralising cyberattacks as early as possible. In the case of large corporations, the Security Operation Centre (SOC) and the introduction of Security Information and Event Management (SIEM) further broaden and enhance the level of security. With a proven track record for endpoint detection solutions, as well as unrivalled threat intelligence based on more than 20 years' experience through GReAT (Global Research and Analysis Team), Kaspersky is the right partner to help businesses future-proof their cybersecurity strategies.

Kaspersky Endpoint Detection and Response

- Helps eliminate security gaps and reduce attack dwell-time
- Automates manual tasks during threat detection and response
- Frees up IT and IT security personnel for other crucial tasks
- Simplifies threat analysis and incident response
- Reduces the time taken to identify and respond to threats
- Establishes unified and effective threat hunting, incident management and response processes
- Increases the efficiency of your in-house SOC – doesn't waste their time analysing irrelevant endpoint logs

Kaspersky Managed Detection and Response

- Fast, scalable turnkey deployment enables an instantly matured IT security function, no need to invest in additional expertise
- Superior protection against even the most complex and innovative non-malware threats prevents business disruption and minimises overall incident impact
- Completely managed or guided incident response provides a swift reaction while keeping all response actions within your full control
- Real-time visibility across your assets and their protection status delivers ongoing situational awareness through various communication channels



The economics of EDR and MDR Why investments in detection and response solutions pay off

By Oliver Schonschek, security analyst and IDG influencer

How effective are investments in cybersecurity? Security managers regularly have to answer this question when justifying their budget use or gathering 'evidence' for their next budget request.

But measuring cybersecurity effectiveness is far from easy because it is not a profit-generating investment but one that helps to prevent losses.

To make matters worse, implementing safeguards are no guarantee of success. Cyberattacks can occur even when robust security measures are in place. A recent survey, by cybersecurity company Kaspersky, shows that 38% of large companies suffered at least one targeted cyberattack in 2020.

And this is despite over half (52%) of them having a dedicated IT Security department, and 20% having an internal Security Operations Centre (SOC) responsible for continuous monitoring and response to security incidents.

For some enterprises, this not only raises the question of how much budget they should invest in cybersecurity, but also leaves them wondering whether security investments are paying off.

“Many customers invest millions in basic IT protection, but then fail to fully leverage their investment,” explains Uwe Kissmann, Managing Director, Cyber Defence Services Accenture EMEA. “Basically, this is a purely economic discussion: How do I ensure that the cybersecurity investments we’ve already made can develop their full potential, and how can we ensure future investments perform optimally?”

To this end, security expert and former CISO, Kissmann recommends:

“It is crucial to not only invest in static protection, but to provide resources, processes, and technology that enable seamless detection of conceivable gateways. This also means developing a clear response strategy in the event of an attack. Establishing static and dynamic protection in equal measure serves to maximize the benefits of cybersecurity investments.”

Detection and response: Protection must become more proactive

A successful cyberattack against a business does not mean that cybersecurity investments are pointless. This is a false view of security.

It is important to remember that any company can and probably will be successfully attacked at some point. Cybersecurity should therefore not be limited to protecting against attacks but also include detecting and defending against them.

The goal of cybersecurity is to detect successful cyberattacks as quickly as possible, and minimize their potential consequences.

According to the international Kaspersky study, "IT Security Economics 2021: Managing the trend of growing IT complexity" , the average cost of a data breach is currently $106,577 for small and medium-sized enterprises.

Large companies should expect even higher losses. For example, the companies surveyed within the study reported that an IT security incident cost them an average of $1,06 million at enterprise level

"Our study shows a welcome trend reversal: Companies have become better and faster at detecting cybersecurity incidents. Even though the follow-up costs in the event of damage are still enormous, they can be minimised through better and earlier detection. This can be achieved by involving external IT security experts and using appropriate solutions."

Christopher Hurst, General Manager, UK&I, Kaspersky.

However, there is good news too. In the previous year, the impact was significant even when security incidents were discovered promptly. For example, when an IT security incident went undetected for a week, the costs greatly increased.

To detect and defend against an incident early on and thereby keep costs down – companies need to ensure they have robust detection and response capabilities. Especially around endpoints, as these are the focus of most cyberattacks.

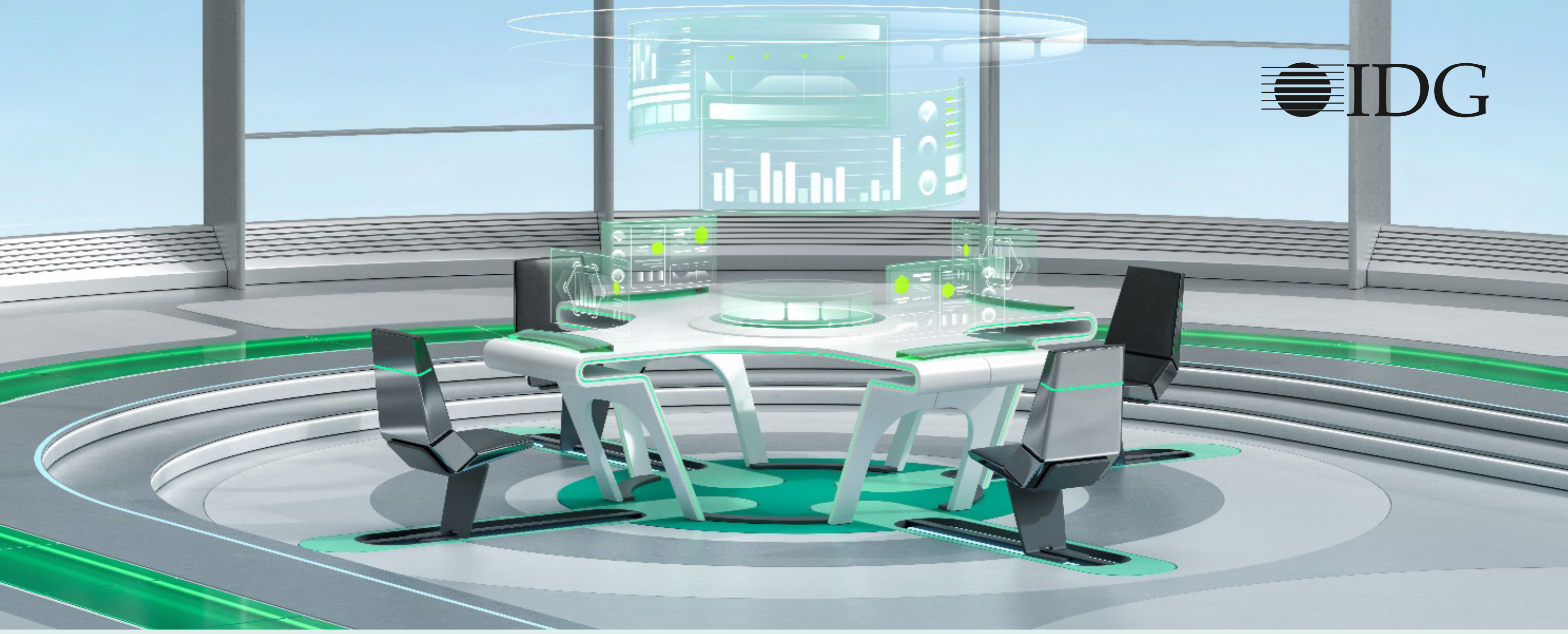
Endpoint Detection and Response (EDR) refers to endpoint security solutions that collect, aggregate, store and analyse system and usage data from monitored endpoints. The endpoint analysis provides indications of suspicious events and warns of possible IT security incidents, such as a hacking attempt on an endpoint.

EDR detects potential attacks not based on signatures, as classic anti-malware does, but by determining expected behaviour of individual endpoints and monitoring whether they show any anomalies. This also makes it easier to detect previously unknown attack techniques, since these change the behaviour of endpoint processes, functions, and applications. Managed services for EDR are called Managed Detection and Response (MDR).

"The risk environment for businesses has grown increasingly complex in the wake of digital transformation efforts as well as workplace changes brought on by the pandemic," says Bob Bragdon, SVP/Managing Director of CSO, looking at the need for new security approaches. "Organisations that continue to be reactive to their security risks will see direct hits to their bottom lines which will always outweigh the cost of investing in good security up-front."

Bob Bragdon advises companies to, "Focus on the basics: Keep your technology current, keep it properly configured, and adopt a risk-based model to prioritize technology investments. With most attacks targeting the endpoint, a great place to begin is to use EDR, MDR and external expertise."

[2] The Kaspersky Corporate IT Security Risks Survey (ITSRS) is a global survey of IT decision makers. This was conducted between May and June 2021 among a total of 4,303 interviews of companies with more than 50 employees. Kaspersky conducts the survey annually.



Compliance: Identifying incidents earlier also helps meet reporting requirements

IDC's Cyber Security 2020+ study reports increasing budgets for cybersecurity during the Coronavirus pandemic.

Compliance issues are also driving companies to increase their security budgets. "At least that is our observation with our clients – with respect to IT security, but also with regard to data protection, supply chain law, KYC checks, and so on," explains attorney Mareike Gehrmann, who specialises in IT law.

EDR and MDR make it possible to detect and ward off attacks, and subsequent data protection violations in particular, at an earlier stage. This also reduces or avoids any sanctions and fines stipulated in the GDPR (General Data Protection Regulation) if a data protection breach is reported too late or not at all.

In the event of a data protection breach, the GDPR sanctions and fines are high enough to threaten the viability of SMBs. For example, supervisory authorities can impose fines of up to 20 million euros, or up to 4% of the total annual global revenue generated in the previous fiscal year, whichever is higher.

External support to combat skill shortages and keep workloads manageable

The need for new approaches to security is also evident elsewhere. Cyberattacks are becoming increasingly complex and sophisticated, while companies are experiencing a shortage of security professionals and noticeably limited knowledge of the dynamic threat landscape. This is as true for mid-sized businesses as it is for larger enterprises.

To address the lack of security professionals and expertise, companies are increasingly turning to cybersecurity service providers.

"For both detection and response, experts with a very high degree of specialisation and, above all, permanently up-to-date information are in high demand," security expert Uwe Kissmann explains. "A professional hacker often flies below the radar. Before hackers risk getting caught, they'll make a defensive move to stay undetected. And then, at some point, companies are amazed to discover that unknown people have been roaming their systems for years without ever being noticed."

But attacks can certainly be detected, as Kissmann knows: "Often, however, the indicators are overlooked or misinterpreted. Experts who monitor systems 24/7/365, and have an up-to-date and very specialised level of knowledge, can help here."

External support pays off: Optimising Detection and Response

External support in security makes sense especially where detection and defence against cyberattacks can be optimised and accelerated.

For mid-sized companies, Managed Detection and Response (MDR) provides access to 'external cybersecurity experts' who make it possible to implement additional security measures without the need to hire new employees.

Outsourcing detection and response can help both mid-sized and large organisations improve detection and defence: MDR protects against even advanced threats through proactive round-the-clock monitoring and expert knowledge, as well as external threat intelligence.

Kaspersky Managed Detection and Response offers all the key benefits of an outsourced Security Operations Centre (SOC). It does not require specialised skills of internal teams for threat detection and incident analysis, so this is particularly relevant for mid-sized companies.

The service is complemented by detection technologies, extensive expertise in threat hunting and incident response from security experts. In addition, the service is equipped with the AI Analyst solution, which automatically evaluates attacks, enabling SOC analysts to focus on the most important warning signals.

"Organisations without a dedicated security team should consider investing in EDR solutions and MDR", Christopher Hurst, General Manager, UK&I, Kaspersky, recommends. "External SOC professionals with deep expertise in detecting and investigating targeted attacks will notice suspicious activity on the corporate network, analyse it, and report an incident. This means that an attack is detected at an early stage and the customer is saved from the disaster of a potential ransomware attack, for example."

Companies with an in-house SOC can also benefit from managed detection and response: "An MDR service can provide a second opinion even if the organisation already has its own SOC team," said Christopher Hurst, General Manager, UK&I, Kaspersky.

For large organisations, detection and response outsourcing is often considered an 'extended arm' of the internal Security Operations Centre (SOC) or internal security department. By its very nature, the internal SOC has a limited view because its security intelligence is based on its own monitored infrastructure and security sensors.

ROSI Analysis Challenge: How do you measure the cost of cybersecurity?

One possible answer is provided by **ROSI**, according to ENISA, the EU's cybersecurity agency.

ROSI stands for "return on security investment".

Therefore, a security investment is judged to be profitable if the risk mitigation effect is greater than the expected costs.

Risk-mitigation effects reveal the benefits of security investment. Put simply, it's a 'reduction of at-risk values' that comes from mitigating the risk associated with financial value losses, according to ENISA.

The ROSI formula was developed by a University of Idaho team led by researcher Huaqiang Wei. The team used existing metrics from the field of information security investment, combined them with some proprietary theories, and assigned values to all factors – from tangible to intangible assets.

ROSI = R - (R-E) + T
or
ROSI = R – ALE

R: Costs incurred per year to address any number of safety-related incidents.

E: Annual financial savings resulting from reducing the number of safety-related incidents by implementing the safety solution.

T: Annual cost of the security investment.

ARO: Probability that a risk will occur in a given year (Annual Rate of Occurrence)

SLE: The expected amount of money that will be lost if a risk occurs (Single Loss Expectancy)

ALE: Annual Loss Expectancy

ALE = SLE*ARO

A sample calculation:

The company Muster GmbH is considering investing in a security solution. Every year, Muster GmbH suffers five cyberattacks (ARO=5). The security manager estimates that each attack causes approximately 15,000 euros in losses (SLE=15,000).

For example, the security solution fends off at least 80% of the attacks (mitigation ratio=80%) and costs 25,000 euros per year (license fees 15,000 euros + 10,000 euros for training, installation, maintenance, etc.). The return on security investment for this solution is then calculated as follows:

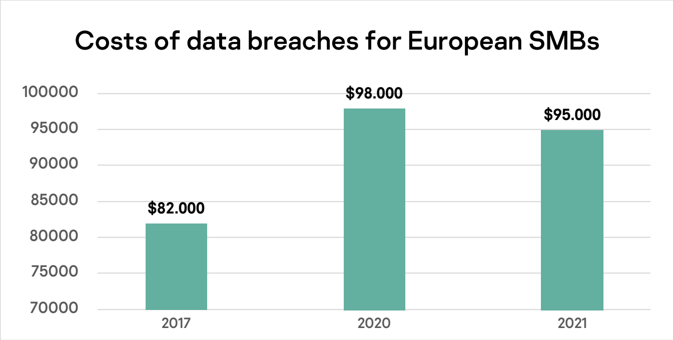
ROSI = ((5 * 15,000) * 0.8 – 25,000) / 25,000 = 140%

According to the ROSI calculation, this security solution is a cost-effective solution and thus economically feasible.

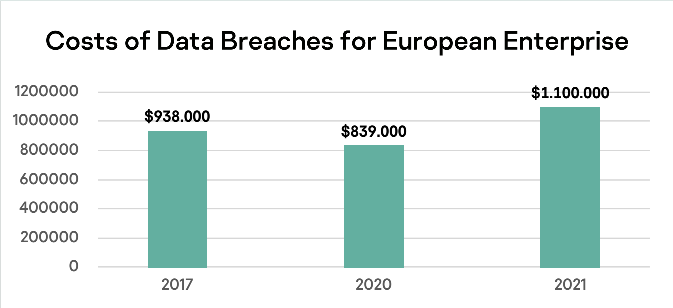
How high are costs caused by IT security incidents compared to the expenses set against them?

According to the international Kaspersky study, “IT Security Economics 2021: Managing the trend of growing IT complexity” , the average cost of IT security incidents for medium-sized businesses and large enterprises is highlighted below.

For example, since 2017, the cost per data breach for SMBs has leveled:

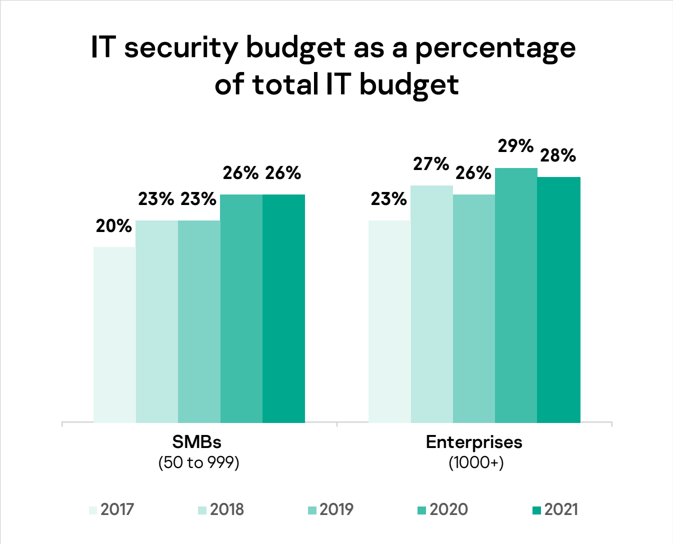

Costs of data breaches for European SMBs

For large enterprises, the costs are as follows:


Costs of Data Breaches for European Enterprise

> "Our study shows that state-of-the-art approaches to security such as EDR and MDR are working. For the companies we surveyed, follow-up costs of IT security incidents have decreased compared to previous years. The increasing willingness to invest in recent years is demonstrating a positive effect with financial damage from a cybersecurity incident being successfully reduced."
>
> **Christopher Hurst, General Manager, UK&I, Kaspersky.**

Since 2017, IT security budgets have increased in the SMB and enterprise sectors worldwide. They now account for more than a quarter of the total IT budget.


IT security budget as a percentage of total IT budget

> “It is vital that SMBs and large enterprises make strategic investments to survive in an increasingly complex landscape of threats. They should invest in external expertise and services, such as MDR and Incident Response, cutting edge solutions such as EDR or MDR, and security layers such as cloud protection, which suit their specific case.”
>
> **Christopher Hurst, General Manager, UK&I, Kaspersky.**

[3] The Kaspersky Corporate IT Security Risks Survey (ITSRS) is a global survey of IT decision makers. This was conducted between May and June 2021 among a total of 4,303 interviews of companies with more than 50 employees. Kaspersky conducts the survey annually..

Some CISOs use the ROSI method, and others choose not to. In the end, it's an individual decision.

"When it comes to strategic consulting at the C-level, ROSI – among other approaches – is at the core of the discussion," reports Accenture manager Uwe Kissmann. "In many cases, the participants want to see the effectiveness and efficiency of their cybersecurity strategy in numbers, on an Excel spreadsheet. This makes it easy to determine how effectively cybersecurity budgets are allocated in the long term."

Kissmann explains the importance of the economic perspective: "In the case of cybersecurity, the best approach is to add a financial viewpoint to the predominantly technological mindset. Here, ROSI is a great help and creates the economic foundation for sustainably efficient protection. However, we must keep in mind that quantifying methods are often insufficient in the cyber-area, so the approach must be supplemented in a meaningful way."

Stefan Wittjen, CISO at Vivantes Netzwerk für Gesundheit GmbH, takes a different view: "For me, the ROSI debate is too academic, and I'm glad I don't usually need to play such number games. If our hospitals are forced to close their doors due to incidents caused by inadequate security measures, no one will care which investments would have made financial sense."

"Investments in cybersecurity, detection and response in particular, really do pay off. They can also be outsourced cost-effectively to external security experts like us," said Christopher Hurst, General Manager, UK&I, Kaspersky. "This puts less strain on security budgets while detecting cyberthreats more reliably and quickly –significantly reducing consequential damage."

Key steps to safeguarding your corporate assets

Taking the right approach at the right time is crucial to enhancing business cybersecurity and protecting corporate assets. To ensure business decision makers can navigate the cyber threat landscape and put the appropriate protection and processes in place by finding the one cybersecurity partner, Kaspersky suggests the following six key steps for success:

Assess and understand the risks

In order to protect your business assets, you need to know every possible risk which might affect them. To fully understand your company's cyber threat landscape, you need enterprise-wide visibility into everything that's going on within the network. This calls for an integrated approach of technology and expert understanding.

Cyber threats today are diverse and sophisticated, ranging from ransomware, APTs, supply chain attacks and data breaches. But when it comes to safeguarding the integrity of data and corporate assets, it's not just cyber threats that could have huge financial and reputational consequences. Disgruntled employees, ex-employees and even clients could pose a risk if the right processes and safeguards are not put in place to protect data and assets.

To show the extent of the issue if not taken seriously, a recent study from Kaspersky found that a data breach discovered over one week after a cyberattack costs enterprises in Europe half a million US dollars (less for SMBs at US$122,963). Meanwhile, companies who detect an attack instantly would pay US$213,737 (SMBs would be US$97,817 out of pocket).

Ask the right questions

With that in mind, asking the right questions when it comes to cybersecurity is a crucial next step, to ensure no stone is unturned and the right type of plan is implemented. This starts with understanding the most important business processes and their key technology dependencies, that's before talking about budgets and solutions.

How is the network infrastructure currently managed and secured? What are the mission critical business processes, and where would downtime lead to lost revenue and damaged relationships? What existing security expertise is there at employee level? How have previous security incidents been handled and responded to? Where are the gaps in knowledge and skill?

Taking an outcome-driven approach will help determine the right priorities and investments based on what levels of protection are needed across the business.

Create awareness and a sense of ownership

A security-first culture is vital to enhancing cybersecurity levels across the business. But this can only be achieved if everyone within the organisation understands their role and responsibilities. With more than half of all security breaches caused by insider threats, this is often down to a lack of awareness or human error.

Awareness training and regular follow-up exercises, to test if advice is being put into action, are therefore vital at all levels – from the most junior employees to senior executives. This can be done online and should include best practices such as password management, email security and secure web browsing. As well as understanding the risks, people also need to know who to turn to if they have a problem and be equipped with clear guidelines and recommendations to support a sense of ownership.

Invest in intelligence

As well as giving people the skills to spot and prevent an attack, future-proofing the business with state-of-the-art, robust cybersecurity protection is essential. This holistic approach can only be achieved through having the right level of threat intelligence and being able to apply big data analytics capabilities to security. Actionable insight on threats affecting the business will ensure that plans and processes can evolve based on meaningful data to prevent businesses falling foul of future threats or security incidents. To gain this essential layer of automated intelligence, business decision makers need to find the right partner with a proven track record that can also automate threat intelligence for even faster reaction capabilities.

Kaspersky supports businesses with access to the latest threat intelligence through our Threat Intelligence Portal. This provides extensive data on cyberattacks and intelligence, which our experts have accumulated over more than 20 years.

Prepare to react quickly

Today's attackers are skilled and use sophisticated tactics. They will use any means possible to get past defences. Prevention alone is not enough. Organisations need to be able to respond quickly and decisively. Planning, practicing and making sure the right security tools are in place are vital.

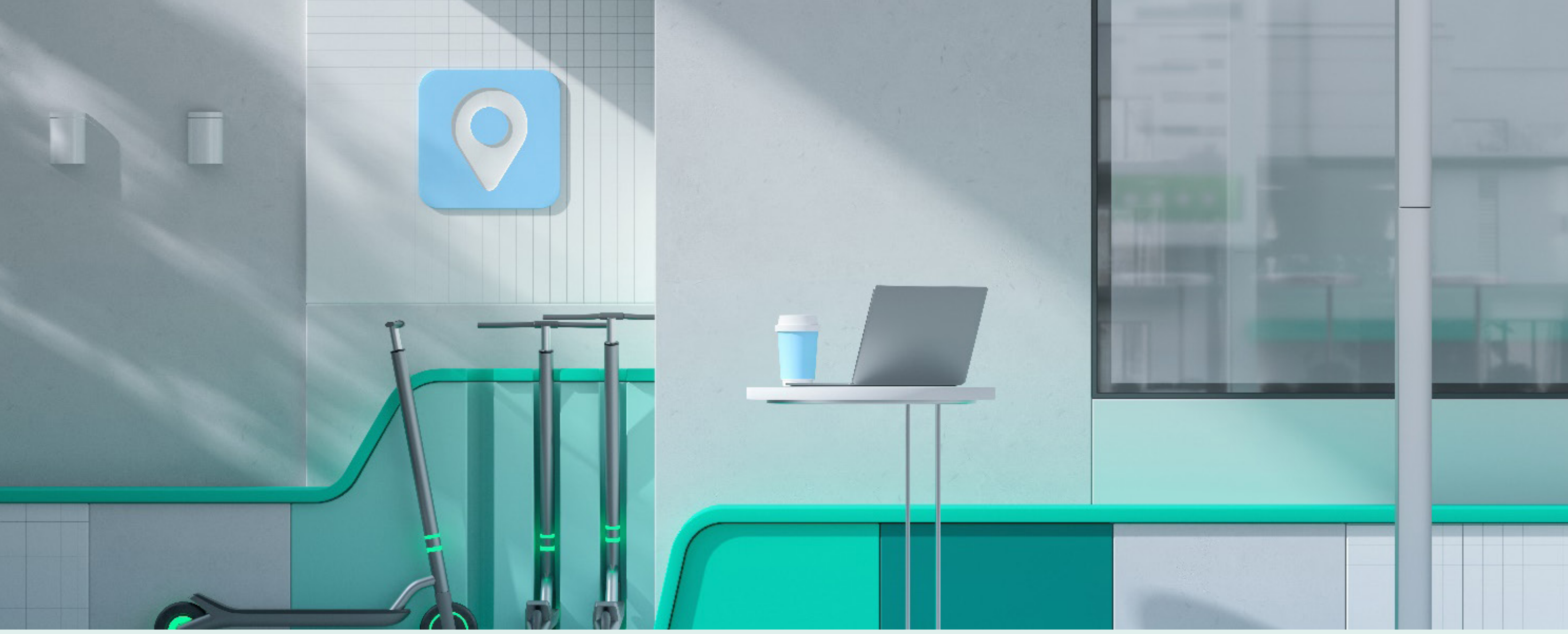
Solutions such as Kaspersky Endpoint Detection and Response and Kaspersky Managed Detection and Response can help identify, investigate, and quickly resolve incidents on all employee endpoints. This is especially valuable as BYOD becomes mainstream, particularly following the pandemic and prolonged periods of working from home.

Review and revise plans

Security threats – both externally and internally – are ever evolving, which means your plans and processes need to do the same in order to keep up. Security plans need to be reviewed and upgraded regularly to help ward off and recover from security threats.

Working with external third-party experts can help to keep plans current and future-proofed as businesses grow and the threat landscape continues to change.

One cybersecurity partner, who can see the full picture through expert understanding, can support you with the latest threat intelligence and provides a unified framework that does it all, means you can be confident in your approach to cybersecurity and focused on innovating.



Which protection suits your company the best?

	Automated EDR	EDR Optimum	MDR	XDR/EDR Expert
Your IT resources landscape	You only have limited IT resources	You have employees within your IT department who, in addition to operating the infrastructure, also deal with security and analysis if necessary	You only have limited IT resources	In addition to the classic IT department, you have a dedicated IT security team
Your security expertise level	You do not have a dedicated employee for IT security and there are no plans to build up security expertise	You already have a little experience in analysing incidents or are in the process of building up your own security expertise within your company	You do not want to build up your own IT security expertise now or long-term. Still, to get the best possible level of protection, you would like to outsource this function to a 24/7 service	Your employees have good to very good security expertise. You have established a dedicated team of experts, or you have already organised defence and detection capabilities

kaspersky

BRING ON
THE FUTURE

kaspersky.com
www.securelist.com