IDC Technology Spotlight

Sponsor: **Kaspersky**

Authors:

Mark Child
Frank Dickson

July 2020

Security teams must be able to operate efficiently and effectively with the tools they have. Otherwise, their organizations risk damaging cyberattacks that can impact their operations, business strategies, and reputations, as well as potentially leaving them liable to regulatory penalties.

Integrated Cybersecurity Delivers Efficiency and Effectiveness in a Challenging Environment

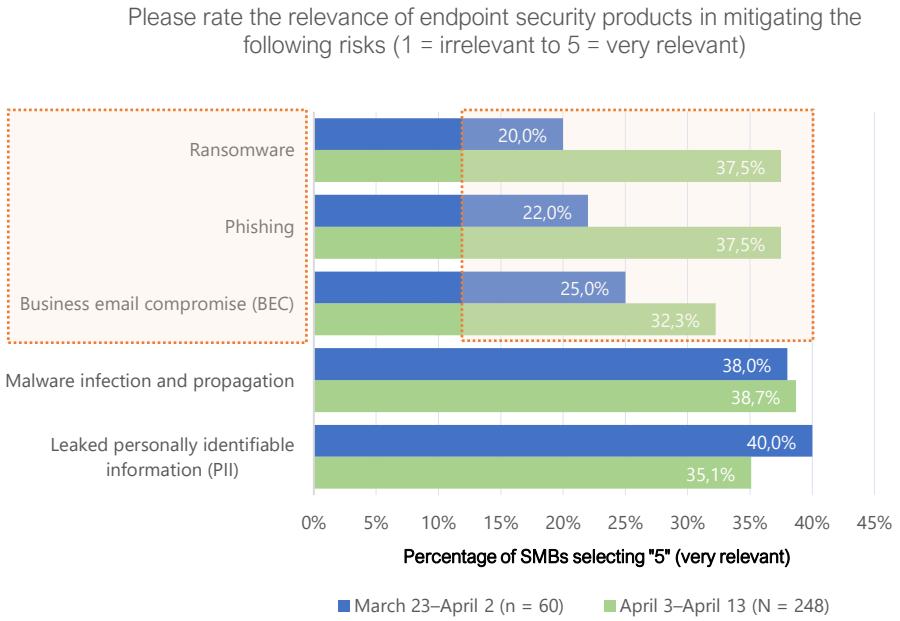
Lack of Integrated Security Puts Organizations at Risk

According to IDC research, the majority (75%) of organizations worldwide recognize that the security team's time is wasted due to a needless lack of integration in its security environment.

Organizations are already struggling with two major security challenges. First, an intense multifaceted cyberthreat landscape. The environment is characterized by a growing number of commercially available threat kits on the Dark Web, creating a lower barrier to entry for unsophisticated attackers. Second, motivated cybercriminal gangs and nation-state attackers can create volumetric attacks (such as DDoS) and very specifically targeted attacks through blended threats.

The recent COVID-19 pandemic makes most cyber-risks *more* relevant. After April 3, IDC saw a dramatic rise in concern over threats such as ransomware, phishing, and business email compromise (Figure 1):

Figure 1
Views on Risk Evolving with the Pandemic — Leaning More on Existing Security Products



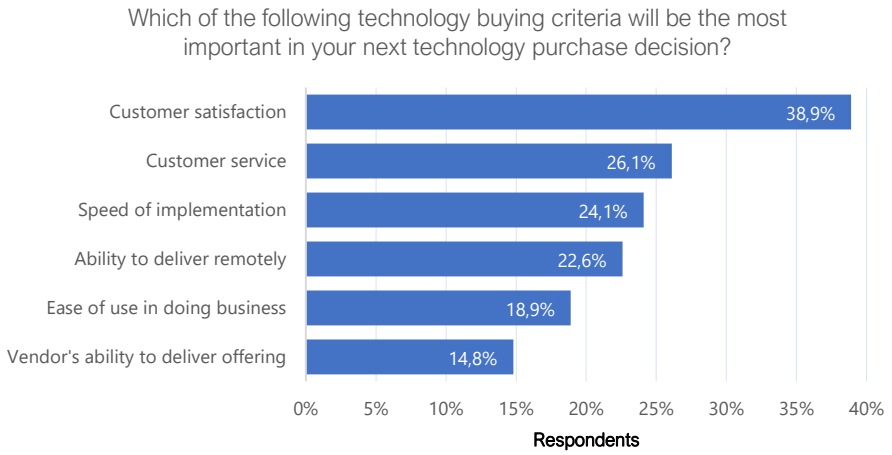
Source: IDC 2020 North America SMB Security Survey, N=308

Additionally, security professionals are in short supply globally. IDC's Worldwide Technology Employment Impact Guide for H2 2018 projected that 10.5 million additional full-time employees would be needed over the 2018–2023 period to provide specialized IT skills, of which 9.6% would be in security. A recent study by (ISC)[2] found more than 4 million unfilled security positions worldwide in 2019. Of these, 561,000 were in North America.

This combination of factors makes it paramount that security teams operate efficiently and effectively with the tools they have. Otherwise, their organizations face significant and growing risks of damaging cyberattacks that can impact their operations, business strategies, and reputations, as well as potentially leaving them liable to regulatory penalties.

Achieving effective security operations remains a major challenge. Frankly put, North American security respondents comment that impediments to security include insufficient tool capabilities, existing tools being too hard to use, insufficient staffing, and existing security professionals having insufficient skills. IT purchase criteria reflect this reality. Customer satisfaction and customer service are becoming increasingly important (Figure 2):

Figure 2
Non-feature IT Product Selection Criteria



Source: COVID-19 IMPACT ON IT SPENDING Survey (Survey conducted during 4th June to 15th June period), IDC, June, 2020, N = 162 North American Respondents

Substantial time can be lost on the manual processes of investigation and analysis and on alternating between unintegrated systems during a security incident triage. The rationalization and integration of the security portfolio can therefore deliver considerable benefits to the organization in terms of man-hour efficiency and incident response times.

Improved integration also enables more of the incident response process to be automated, reducing the potential for errors that may occur as analysts correlate data from different systems. According to IDC's 2020 Data Security Survey, complexity is the biggest barrier to adoption/implementation in the organization, ahead of a lack of budget and a lack of staff.

Reducing the burden on security staff to manage disparate tools and solutions within the estate frees them for higher-value tasks (e.g., in-depth incident forensics and analysis and the investigation of higher severity incidents). Increased automation reduces the likelihood of alert fatigue or analyst burnout due to too many mundane tasks. The overall improved efficiency and effectiveness enabled by integration and automation allows security teams to operate more strategically, rather than just managing day-to-day operations.

Organizations also gain from accelerated and more effective responses. The overall cyber-resilience of the organization is boosted by the sharing of insights and threat intelligence from different security tools and functions.

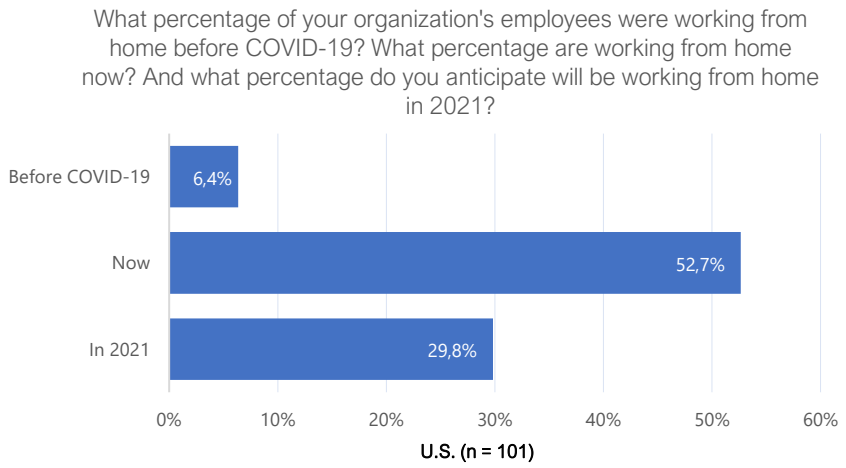
Endpoint Security Key to Improving Security Posture

Endpoint security investments in 2019 constituted the second biggest share of the North American security market (28.1%), closely following the security analytics, intelligence, response, and orchestration category. The endpoint security market is projected to expand at a compound annual growth rate (CAGR) of 4.5% over the next five years. The vast majority of growth is found in the corporate sector.

Endpoint devices are a primary target for cybercriminals seeking to gain access to corporate networks. This vulnerability has intensified in the post-perimeter era due to both digital transformation initiatives and a surge in work-from-home policies triggered by the COVID-19 pandemic. Simply put, IDC regards endpoints as a key control point of protection in the post-perimeter era.

The COVID-19 pandemic has accelerated the importance of the endpoint as a key control point. U.S. IT executives were asked to predict the past, present, and future percentages of remote workers. The results were startling. Simply put, even after the pandemic, workers will not necessarily return to the office.

Figure 3
What will the new normal be? Five times more employees will work from home in 2021.



Source: COVID-19 IMPACT ON IT SPENDING Survey (conducted during 21st May to 28th May period), IDC, May 2020

Traditional signature-based detection methods are open to criticism, but they remain an efficient means to scan large volumes of files and block known threats. Relying on signature-based protection alone, however, would be pure folly. To provide complete protection, a signature defense requires augmentation by signatureless detection within an integrated endpoint protection platform (EPP). The platform enables signature-based detection to protect against commodity malware, while signatureless detection guards against new and unknown complex threats that may otherwise evade detection.

Attention in the market to endpoint detection and response (EDR) is increasing as organizations seek to enhance protection capabilities and detect advanced threats and targeted attacks. EDR has armed security professionals with an arsenal of forensics tools beyond the historic log-based or alert-based security information and event management (SIEM)-centric variety. It also provides a host of endpoint telemetry, enabling security professionals to discover hard-to-find malware.

Adopting an integrated multi-layer approach to endpoint security is fundamental to building a resilient security program. This approach requires the tight bonding of the stack and should include EPP (reactive), EDR (proactive), and threat intelligence (TI), which can be both preventive and proactive. EPP should be expected to protect endpoints as an independent solution. Together, EPP and EDR provide cross-platform visibility and response, stopping maliciousness that cannot possibly be detected with endpoint activity and telemetry alone. Both are important to the complete security program.

TI can significantly improve an organization's security posture. On the preventive side, TI feeds have long been used for blacklisting known threats. Proactively, TI data and reports enable threat hunting, provide greater context during investigations, and can help mitigate risk. From an endpoint security perspective, the additional context that TI provides can guide security controls, increasing the effectiveness of the solution.

The Challenges of EDR

EPP remains critical. EDR has brought many benefits, but it has two major shortcomings:

- **EDR requires a human to operate it.** Security professionals are in short supply, and their time is very valuable. As a result, expectations relating to EDR and its usability have grown exponentially. EDR tools need to be easy to use. They also need to quickly correlate alerts to render a conviction or a benign verdict. They need to provide guided search to enable security professionals to perform at a higher level than they traditionally could. Essentially, EDR tools must evolve to make security professionals more efficient and effective.
- **The "ransomware effect" is an Achilles' heel.** The "ransomware" moniker is an oversimplification, but the reality is that the importance of time in breach detection has risen dramatically: Malware attacks have been measured in milliseconds. Depending on EDR to detect ransomware is a fool's errand. A manual tool cannot respond quickly

enough to stop an attack that happens in minutes, seconds, or milliseconds. Even solutions that use automated cloud-based analytics are not fast enough. A round trip of 200–500ms can be punishing in a ransomware scenario. Thus, EPP must address use cases for which EDR is insufficient.

For EDR to add value to EPP in the ransomware era, EDR tools must do the following:

1. Find malware that cannot be detected using telemetry on the endpoint alone
2. Provide forensic information that will illuminate how malware got past the other layers of security before it was stopped by EPP

These use cases have similar implications: The data that fuels EDR needs to come from more than just the endpoint. Telemetry needs to come from the network, messaging, the web, and other infrastructure components and processes. Vendors are starting to call this expansion "XDR," in which the "X" can stand for "cross-layer," for example.

EDR creates value by extending the view beyond the initial boundaries of the endpoint. The "manifest destiny" of EDR is to be a tool that provides cross-platform visibility and response, stopping maliciousness that evades endpoint detection and telemetry.

PowerShell scripts are not necessarily malicious. However, if a PowerShell script were launched from a macro embedded in a Word file and that Word file was found in a recently delivered email, the chances of the script being malicious are high. This example is simplistic but very real. The response must go beyond sequestering the individual endpoint. The security analyst must be able to sweep all email accounts for similar files, block communications with command-and-control IP addresses, update firewall rules, and force a password reset. In sensitive environments, evaluating other individuals who received the same email may provide forensic insights.

In evaluations of EDR, the conversation is very much about EPP. Expectations for EPP have grown dramatically, and the use of an EDR is not regarded as compensation for the possible shortcomings of EPP. EDR creates value by extending the view beyond the initial boundaries of the endpoint. The "manifest destiny" of EDR is to be a tool that provides cross-platform visibility and response, stopping maliciousness that evades endpoint detection and telemetry.

One Size Does Not Fit All

On a certain level, all companies' security needs are the same: They need protection from threats and the ability to maintain business operations. But that is where most comparisons end.

- Although the need for protection is the same, the security resources of a small or medium-sized business do not match those of a multinational enterprise.
- Security maturity varies considerably.
- Assets within organizations are not uniform. These differences need to be handled using a risk-based approach.

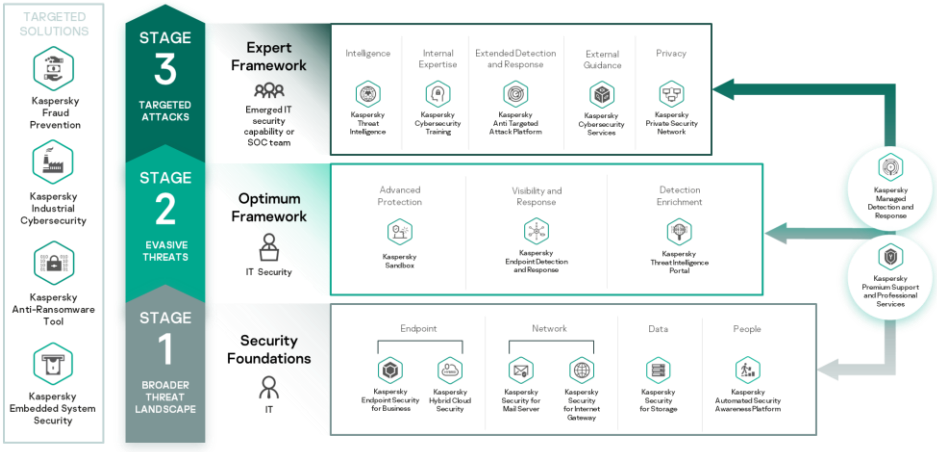
From a security provider's perspective, a comprehensive, structured offering is required, one that provides appropriate levels of protection to end users across the spectrum. Offerings need to:

- Provide granularity of controls to secure heterogeneous infrastructure
- Scale to accommodate the expansion or fluctuation of infrastructure and operations
- Provide protection in hybrid environments
- Address all fundamental components of infrastructure and processes (endpoints, network, messaging, web, mobile, cloud, and operational technology)
- Achieve the above while minimizing the burden on the system and organizational resources
- Be manageable through a unified and integrated solution

A Multi-Level Approach from Kaspersky

Kaspersky's extensive experience in providing cybersecurity solutions and services to a broad spectrum of clients has enabled it to shape an integrated approach that meets the needs of the mainstream market and larger, more security-mature, customers.

Figure 4
Kaspersky's Multi-Stage Cybersecurity Conceptual Framework



Source: Kaspersky

The bedrock of Kaspersky's integrated platform is Security Foundations. This includes the core features that every organization, large or small, must have to protect itself. According to the vendor, Security Foundations can defend against threats (including fileless malware) that comprise 90% of the overall threat landscape.

Kaspersky Security Foundations includes Kaspersky Endpoint Security for Business (KESB), Kaspersky Secure Mail Gateway, Kaspersky Web Traffic Security, and Kaspersky Hybrid Cloud Security. The full set of components is shown in Figure 2.

Kaspersky customers can selectively deploy the components and modules they require to secure their infrastructures and processes. All modules benefit from native integrations, enabling clients to rapidly gain full value from their deployments. The more they deploy, the more cumulative benefits accrue.

The key benefit of Security Foundations is that it offers protection against 90% of threats. The next category of threats, evasive threats, comprises 9.9% of the threat landscape. These complex threats are often able to evade preventive technology and can, in the long term, do considerable damage to an organization.

Addressing these threats requires a more proactive and sophisticated set of tools. This is represented by Kaspersky Optimum Framework, the next level of the pyramid. Kaspersky Optimum Framework includes Kaspersky EDR, Kaspersky Sandbox, and Kaspersky Threat Intelligence Portal. Customers can deploy components individually. However, the vendor also offers bundles, such as KESB with EDR Optimum (i.e., EDR for midmarket clients).

Organizations that have deployed or adopted Security Foundations and Optimum Framework have acquired protection against the vast majority of cyberthreats. They can consider themselves at the higher end of the security maturity spectrum.

That leaves the 0.1% of targeted attacks. It is here that organizations need the elite protection of Kaspersky Expert Framework to support their security operations center (SOC) teams.

A comprehensive evaluation of this most advanced offering is beyond the scope of this report. More detail is available in this companion publication[1].

All Kaspersky customers benefit from being able to select and deploy specific modules that directly address their security requirements or to take advantage of bundled offerings. Native integrations ensure that all components operate together seamlessly, giving the security team the advantage of operating a unified platform. However, Kaspersky has conceived its cybersecurity framework as a maturity spectrum through which organizations can plan strategically, elevating their security postures over time through the deployment of additional integrated components and services. Two key elements are Optimum Framework and Expert Framework.

Kaspersky's Optimum Framework for the Mainstream Market

Optimum Framework is aimed at organizations that have limited IT security capabilities but need to protect themselves against advanced threats. The core components of Optimum Framework are KESB, Kaspersky Sandbox, and EDR Optimum, all run from a single console, providing protection to all endpoints, including servers and virtual machines. The vendor cites two key benefits to deploying KESB and Kaspersky Sandbox together. First, using dynamic threat

[1] IDC Technology Spotlight: Battle for the Modern Security Operations Center

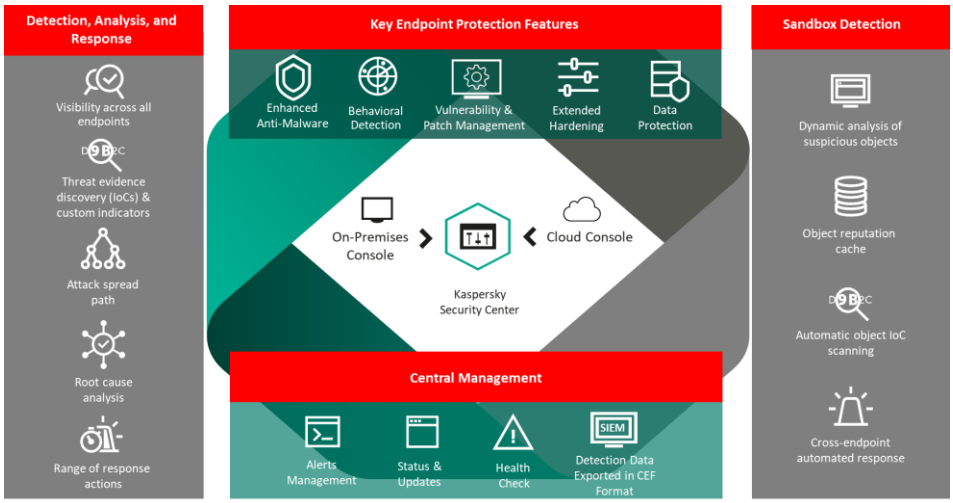
emulation, Kaspersky Sandbox automates "cross-endpoint" incident response scenarios. Second, no action is required from the IT security team. This is particularly important for companies that have limited security resources.

The EDR Optimum offering adds an additional level of protection on top of EPP. It includes indicators-of-compromise (IoC) scanning, the possibility to generate custom threat indicators, tools for root cause analysis (e.g., attack spread path visualization), and some automated response and threat containment capabilities.

For organizations that do not have in-house resources to take full advantage of Kaspersky EDR, the vendor offers a managed detection and response (MDR) service, MDR Optimum. This provides a mature information security function that can be rapidly deployed via a fast turnkey. The service covers both endpoint and network security, with a Kaspersky team managing security data collection and analysis, incident qualification and investigation, and incident alerts and guidance. The company offers a flexible approach to response. The hands-off option leaves the response fully to the customer. At the next level, the Kaspersky team provides response recommendations. The full-service option puts incident response in the hands of the Kaspersky team.

A summary of the key elements of the Kaspersky EPP, Kaspersky Sandbox, and EDR Optimum offerings is shown in Figure 3.

Figure 5
Kaspersky Optimum Framework Tools and Capabilities



Source: Kaspersky

Kaspersky's Expert Framework for IT Security-Mature Clients

Kaspersky's Expert Framework targets organizations with mature IT security postures and established security teams and resources. At the broadest level, it offers a single console to centrally manage all security functions — endpoint, network, mail, and web defense — against targeted attacks and advanced persistent threats. It covers monitoring, visualization, notification, and reporting; advanced threat discovery; deep investigation and threat hunting; and incident

response. As with Optimum Framework, in-house tools and capabilities are complemented by Kaspersky's MDR offering (in this case, MDR Expert). As might be expected, this provides even greater depth of service, adding items such as access to a Kaspersky SOC analyst, extended raw data storage, access to curated features of the Kaspersky Threat Intelligence Portal, and custom response playbooks. A comprehensive overview of Expert Framework is beyond the scope of this document, but more in-depth information can be found here.[2]

Detection and Response for All: EDR and MDR

Over the last couple of years, the North American market has seen a rapid rise in the use of EDR tools and MDR services. EDR tools enable threat hunting, forensic analysis, anomaly detection, and incident response. The analytical capabilities of the EDR toolset help security analysts detect stealthy or evasive threats, extending the detection horizon beyond that which an EPP suite can deliver. Some North American organizations have invested in EDR to complement and enhance their endpoint protection suites. But benefiting from these tools requires dedicated analysts. This raises the questions of security headcount and skills shortages — issues that impact all but the most affluent organizations or those whose assets, activities, and/or regulatory obligations demand the most stringent security.

However, endpoint security affects all organizations. In April 2020, IDC surveyed 308 North American companies with up to 2,500 employees about cybersecurity. On average, each company (based on estimates given in the survey) runs 337 endpoint agents to analyze its endpoint equipment (workstations, laptops, detachable tablets, and other mobile devices).

The situation has created a ripe market for MDR services, one in which EDR tools are run on behalf of clients by managed security services providers (MSSPs). This segment has grown rapidly, with players coming from the security solutions side (e.g., Kaspersky) and the services side. Most MDR providers offer tiered services with multiple levels of dedicated support, reporting, threat hunting, and incident response to meet the needs of all customer groups. Because not all organizations have the resources to run EDR themselves, these services fulfill a market need. IDC expects demand to continue to rise in 2020 and beyond.

Challenges

Kaspersky has developed a comprehensive and complex portfolio and mapped out detailed frameworks to guide organizations in addressing endpoint security and security integration. Nevertheless, the vendor faces challenges in executing its vision.

The MDR market is growing rapidly in the U.S. and Canada and is home to a large pool of players. These comprise both strong EDR solution providers and vendor-agnostic MSSPs, which have teams of highly skilled and experienced analysts. It will be a challenge for any vendor to differentiate themselves in this space. Doing so will require an appropriate investment of resources to ensure clients feel they are

[2] IDC Technology Spotlight: Battle for the Modern Security Operations Center

getting the service they have paid for. Of course, the ultimate measure of success is whether a company is protected from breaches. CISOs, however, may also need to justify to the board that their investments are delivering returns. It is important that Kaspersky is ready to support its MDR clients with the metrics they need.

Kaspersky's graduated approach and its Optimum Framework show that the vendor is well positioned to help midmarket companies that have a strategic outlook on improving their security postures. However, at the high end of the market, the vendor faces entrenched enterprise security players with established clients. A major benefit of Kaspersky's platform is the native integrations of its modules and components — from the security foundation level to the integrated cybersecurity level — and the cumulative benefits that accrue from deploying more modules. The more extensive a deployment is, however, the more legacy products must be displaced.

The breadth of Kaspersky's cybersecurity solutions and services and the wide spectrum of clients it serves have enabled the vendor to shape an integrated cybersecurity approach to meet the needs of both the mainstream market and larger, more security-mature, customers.

Kaspersky's offering is an extensive stage-by-stage approach (see Figure 2) that features both numerous standalone components and services within the Security Foundations, Optimum Framework, and Expert Framework layers and the dual tier of EDR and MDR, as well as providing further options around regular EDR and automated EDR and MDR. The vendor must ensure that customers and prospects receive a clear message that Kaspersky can help them find the most effective combination of solutions and services to meet their needs.

Finally, germane to the global economic consequences of COVID-19, the economic drag is heavier than the technical benefit lift for companies purchasing cybersecurity solutions. In February 2020, the National Bureau of Economic Research said the U.S. fell into recession, ending a 128-month economic expansion. The practical effect is that all industries are hurt, but cybersecurity investments may be more resistant to cuts in some sectors.

Future Outlook

Facing an extensive and intense threat landscape and struggling to manage security operations with limited teams and fragmented security infrastructure, companies need integrated and unified cybersecurity solutions. The breadth of Kaspersky's solutions and services and the wide spectrum of clients it serves have enabled the vendor to shape an integrated cybersecurity approach to meet the needs of both the mainstream market and larger, more security-mature, customers.

Kaspersky regularly scores highly in independent tests of its products against known, unknown, and advanced threats. The vendor is also well-regarded for its security research, which it publishes regularly. Kaspersky has the vision, the approach, and the frameworks. Its task is to communicate these strengths to the market and lead its clients on the journey to improved cybersecurity.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC #EUR246697420