kaspersky

How can you protect against threats you can’t detect?

The rise of evasive threats – and why it's vital to prevent them

For years now, there's been a well-defined structure to the threat landscape that's been relatively straightforward for organizations to defend themselves against.

Businesses ranging from the smallest SMBs to mid-size enterprises have had to protect themselves against run-of-the mill commodity threats targeting their endpoints – which have always been the #1 target for attack. Arming yourself with a well-equipped endpoint protection platform (EPP) has therefore provided a high degree of confidence that your business is secure.

Of course, there are many other types of threats that are significantly more sophisticated than commodity attacks. But these have traditionally targeted much larger organizations, where the cost of mounting such an attack is justified by the scale of the financial reward and/or damage generated by a successful result.

Unfortunately, this situation is changing rapidly. And the new threat landscape is being driven by four extremely challenging and self-reinforcing trends:

Changes in working practices driven by digital transformation, and the increase in remote working resulting from the pandemic, are dissolving corporate perimeters and making endpoints harder to defend.

Not only are evasive threats harder to defend against, they're also more prevalent. This is because it's now easier – and cheaper – than ever for cybercriminals to find, combine and test ready-made tools, methods and attack scenarios, and attacks of this type promise much higher chances of success than traditional scenarios.

Threats targeting endpoints are becoming increasingly 'evasive'. Specifically designed to bypass existing endpoint protection, these threats are hard to detect thanks to the range of evasion techniques being adopted – particularly the use of legitimate and system-native tools.

And, of course, by staying undetected for longer, evasive threats have the time to explore and entrench themselves into a business's infrastructure and cause the greatest amount of damage – be it a data breach, ransomware attack, directly overriding financial operations and more.

What are evasive threats and why are they so dangerous?

01 Common types include malware, ransomware, financial spyware and more.

02 Tools and techniques for mounting evasive threats are readily available to cybercriminals, including guides and cybercriminal services.

03 Use of legitimate tools (such as PowerShell, PsExec, SoftPerfect) and other techniques for penetration, burrowing and data exfiltration makes them hard to detect and increases persistence.

04 From ransomware to long-lasting data theft, staying hidden makes the threats more dangerous by giving them time to do maximum damage.

Clearly, it’s impossible to defend against threats you can’t detect, so how can you stop them?

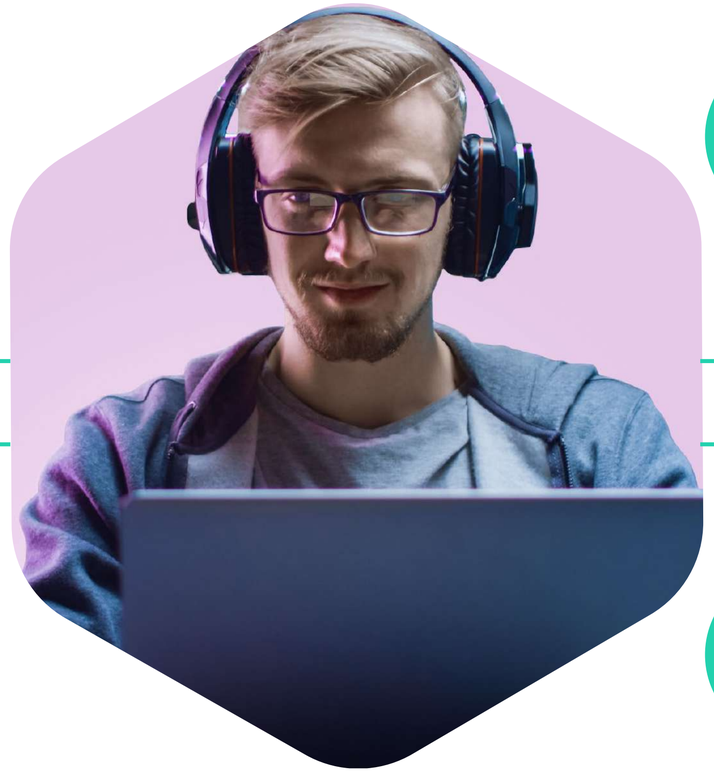
How to identify and defend against threats bypassing your EPP

Has your business been targeted by evasive threats – and would you know if it was under attack right now?

?

Are you confident your IT team have the specialist IT security skills needed to effectively implement and manage these tools?

?



Are you clear about how best to find, analyze and repel these threats, and the kinds of tools and approaches you need to use?

?

And do you have a clearly defined basic incident response processes?

?

When thinking about how best to answer these questions and extend your defenses beyond EPP, you'll almost certainly have a wish list of capabilities you'd like your enhanced solution to offer.

From discussions with many similar businesses and within the community, these are likely to include:

- Automatically protecting against traditional threats without compromising your current endpoint protection levels.
- Getting help from cybersecurity experts – possibly including managed protection.
- Adding an extra layer of detection to increase confidence that you're detecting evasive threats.
- Gaining visibility into detects, understanding where the threats came from and how they developed.
- Increasing control over users and endpoints – especially as users can't always be trusted to follow good IT hygiene and cybersecurity practices.
- Minimizing mean time to respond (MTTR) by not requiring IT to raise tickets for threat responses such as host isolation or scanning for Indicators of Compromise (IoCs), or having to do this manually with standard OS tools.
- The ability to scan your whole network for threats notified by regulatory authorities, imported from other trusted sources, or IoCs generated from other incidents.
- Not having to integrate multiple tools, or use and operate multiple consoles on a daily basis.

Kaspersky Optimum Security gives you precisely these capabilities

More visibility.
More power.
More control.

Kaspersky Optimum Security is a unified, cloud-enabled solution which complements your cybersecurity skills in a resource-conscious way - through effective endpoint detection and response (EDR) with managed threat hunting, and guided and remote response scenarios, but without prohibitive costs or complexity.

The solution delivers the protection you need against new, unknown and evasive threats – without the need to hire or retrain IT security specialists, or allocate additional resources – through:

Powerful advanced detection of evasive threats, based on a combination of machine learning, sandboxing, behavior analysis and automated threat hunting with Indicators of Attack (IoA).

Enhanced threat visibility to enrich detected threats with context and details, and simple root cause analysis and visualization tools that let you quickly and efficiently investigate and understand each threat and how it has developed.

Fast, ‘single-click’ or automated cross-endpoint response, helping you rapidly respond to fast-moving threats across your infrastructure.

How Kaspersky Optimum Security helps

You'll find Kaspersky Optimum Security particularly beneficial if you've been experiencing common pain points such as:

Being unable to recruit the IT security specialists you need, or lacking appropriate security skills.

Struggling to defend your corporate perimeter due to remote working and lack of visibility.

Becoming overwhelmed with routine tasks, too slow to respond to incidents due to too many manual tools, or being unable to deal with evasive threats.

Technologies

Prevent, detect, analyze, respond and train

To enable you to supplement your defenses with tools which, as well as providing the visibility needed to identify attacks bypassing your EPP, are easy to use and incorporate lots of automation, Kaspersky Optimum Security includes advanced technologies across the entire cycle of preventing, detecting, analyzing and responding to evasive threats – along with training programs with the proven ability to transform employee behaviors and prevent threats occurring in the first place.

The solution builds on and integrates with Kaspersky Security Foundations, which automatically blocks the maximum number of commodity threats with multi-vector prevention, and itself includes a variety of advanced technologies such as web, device and application controls, behavior detection, exploit prevention, system hardening, file and memory protection, vulnerability assessment, patch management and ransomware protection.

Prevent

Adaptive anomaly control

Automatic system hardening uses ML techniques to study user behavior and learn to block unusual scenarios related to specific users or groups – minimizing the attack surface and preventing any unusual actions. This also ensures users don't suffer from unnecessary restrictions, and administrators don't need to spend time identifying and implementing appropriate rules.

Automatic exploit prevention and attack surface reduction

Building on technologies included in Kaspersky Security Foundations, automatic exploit prevention technology specifically targets malware that utilizes software vulnerabilities, and system hardening capabilities include application, web and device controls.

Application control manages application startup rights, and controls actions and access to protected resources like files, folders and registry keys. Web control provides centralized control over access to non-work-related or suspicious web resources. And device control restricts user access to various devices to protect data from being stored, transferred or converted illegally.

Vulnerability assessment and Patch Management

Enables OS and application vulnerability detection and prioritization.

Enables automated distribution of patches and updates.

Detect

Advanced detection

Machine learning (ML) algorithms detect previously unknown malicious patterns of application behavior at the earliest stages of execution. Selected features of analyzed files are run through a carefully tuned decision tree to detect malicious properties, and depersonalized malware data shared by voluntary participants is analyzed by AI and human experts to identify new threats.

Automatic sandbox technologies

Dynamic threat emulation identifies evasive threats by detonating suspicious objects in an isolated environment and analyzing their behavior. Anti-evasion techniques prevent malware from detecting it's running inside a sandbox and hiding its presence. And automation features allow the sandbox to be easily used by organizations without dedicated IT security staff.

Threat intelligence

Kaspersky Threat Intelligence is available via a simple web portal, and integrates with Kaspersky Optimum Security using a combination of threat lookup, file and web address analysis. File analysis detects advanced threats present in files by running them through the full stack of Kaspersky technologies. Threat lookup enriches and prioritizes alerts by analyzing suspicious IPs, file hashes, domains and web addresses. And web address analysis executes suspicious web addresses in a URL sandbox to create a comprehensive threat report.

Analyze

Enhanced threat visibility

Data from multiple sources is automatically gathered into a single alert card for quick and efficient analysis without the need for multiple tools. Basic detect information is supplemented by the most relevant file, host, user and other data. Relevant contextual data is also collected for analysis, including correlating events, parent processes and response action history.

Root cause analysis

Enriched data on each detect enables a full understanding of exactly what has occurred, on which host and under which user. Data and visualization tools including automatically generated drill-down attack spread-path visualizations enable rapid analysis of how the threat developed on the host, to determine its root cause and whether any additional response actions are needed.

Expert help

Managed detection and response (MDR) can drive cost efficiencies by focusing in-house resources on critical tasks demanding IT security involvement, and maximize capacity by leveraging advanced ML models to significantly increase analyst throughput and minimize mean time to respond. MDR delivers 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.

Analyze

Automated threat hunting with IoAs

Proprietary Indicators of Attack (IoA) created by Kaspersky experts take threat detection to the next level by essentially providing threat hunting supported by our cybersecurity specialists.

Cross-endpoint scan

Indicators of Compromise (IoC) are imported from a trusted source or generated from past incidents, and a scan is run across hosts to reveal any current evasive threats hiding on endpoints. An IoC for an analyzed alert can be generated with just a few clicks, and scans for similar threats run on other hosts to determine the true scope of the discovered threat. Scans can then be scheduled or run on-demand to find current threats.

Respond

Automated response

Automated response enables single-click threat response from the alert card, and instant action to be taken on analyzed threats. An automated response can be set up with a simple checkbox, and will be applied upon threat discovery by an IoC scan, with options including isolating the host, quarantining the file, scanning critical areas and preventing file execution.

Guided and remote response scenarios

With MDR, Kaspersky experts can provide response recommendations for detected threats or run specific remote response scenarios. MDR offers advanced, round-the-clock protection from threats that can otherwise bypass automated security barriers, and supplies all the major benefits of a 24/7 Security Operations Center (SOC) without the prohibitive costs.

Train

IT online training

Cybersecurity for IT Online provides interactive training for IT generalists (IT support, service desks, etc.) where standard awareness programs are insufficient but in-depth security expertise is not required. The training develops practical skills essential to recognizing a possible attack in an ostensibly benign PC incident, and collecting incident data for handover to IT security.

Simulations

Interactive games are based on custom-built simulations of the impact cyberattacks and associated management decisions can have on business performance and revenue. Gameplay develops an understanding of cybersecurity measures, establishes a better security understanding among senior managers and decision makers, and increases awareness of the risks and security challenges of running modern computerized systems.

Automated tools

Combining the latest learning technologies with Kaspersky's 20+ years of cybersecurity expertise

Maximization of employee awareness and new cyber-safety behavior patterns with a competency model consisting of 350 key cybersecurity skills.

Adaptive training

Training addresses all levels of the organization, ensuring all employees are trained to the optimal level. Gamification, learning-by-doing and repeated reinforcement ensure strong skills retention, as each engaging exercise highlights the direct relevance of cybersecurity to the individual. The employee's workplace environment and behavior are emulated, relating directly to users' practical interests, increasing their motivation to learn and guaranteeing that skills learned will be applied.

Why invest in Kaspersky Optimum Security?

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.

This helps you:

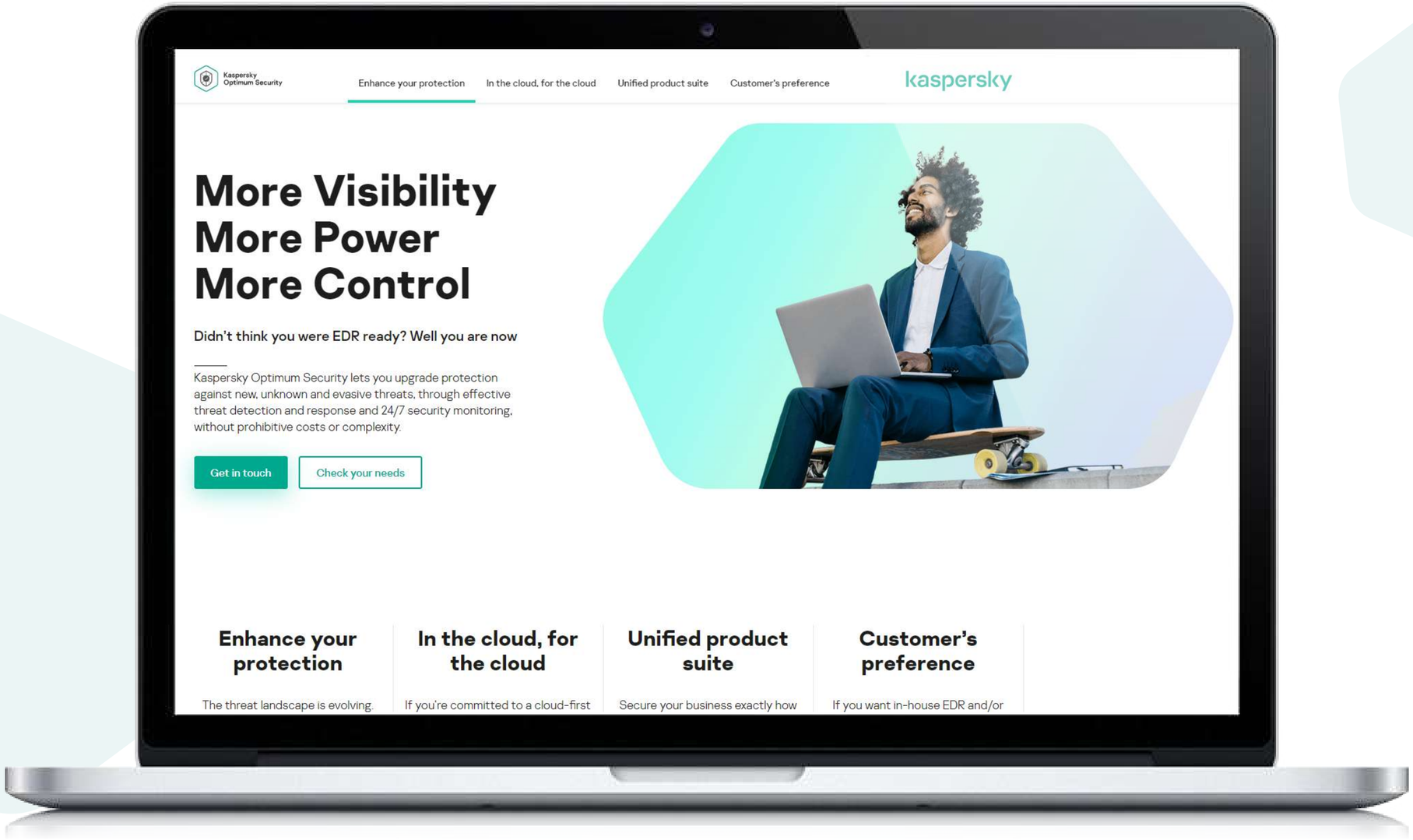
- Stay on top of new, unknown and evasive threats, and offload the most taxing cybersecurity tasks with 24/7 managed protection supported by Kaspersky experts.
- Build or improve detection and response capabilities in a simple yet effective way – giving your cybersecurity specialists the necessary tools, simple processes and automation features to develop their incident response capabilities.
- Educate users into forming safe behaviors, shielding you from various threats before they ever get a chance to infect your hosts, and lowering your workload from analyzing avoidable alerts and incidents.

Why invest in Kaspersky Optimum Security?

With 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**

kaspersky