Integrated solution for endpoint security

Building robust defenses with limited resources

kaspersky

Learn more on kaspersky.com
#bringonthefuture

Introduction

Most organizations, regardless of size, location or discipline, now understand that when it comes to a cyber-attack, the question's not whether it will happen to them, but when. Nobody should now consider themselves immune.

But having the time, the resources, or (to be frank) the motivation to navigate the current threat and security landscape effectively — well that's another question.

Most information security analysts — and there aren't nearly enough of them to go round — are overworked as it is. Looking after new employees and their devices, figuring out new laws and compliance issues, reading up on the latest threats – all this needs to be dealt with before actually getting down to the main business of corporate protection.

Basically, very few security professionals, if any, can enjoy the luxury of spending all their time hunting down new and exotic threats and responding to them.

Which is where cybersecurity vendors and their products and solutions come in. Our job is help you fully secure your infrastructure and keep your users safe, with the lowest possible expenditure in terms of resources, including time and money as well as expensive and hard-to-get expertise.

The challenges

First, let's take a look at some of the issues today's IT and IT Security Managers face.

Increased threat of an advanced or targeted attack

Targeted attacks and complex threats are a huge problem and are on the rise. Cybercriminal tools are becoming so cheap and accessible that basically anyone with a computer can now launch an advanced attack. Which means that organizations who once assumed they were 'under the radar' in terms of advanced threats are finding out the hard way that things have changed.

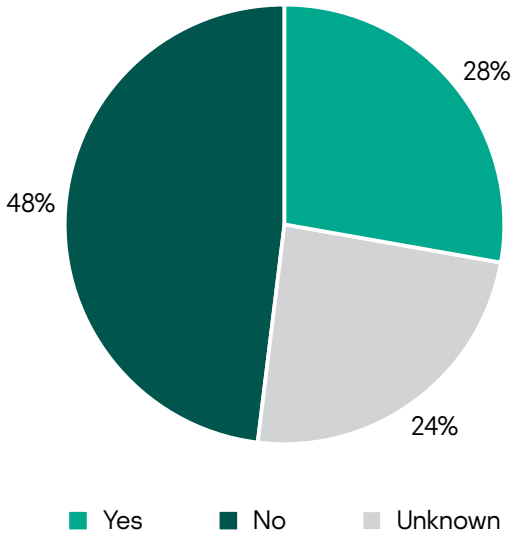
That said, commodity threats also remain an issue: the sheer volume of these is a huge problem in today's world.

The vast majority of cyber-threats either enter through the endpoint, or are designed to trigger there (or both).

So one of the best ways to protect your assets is to protect your endpoints.

According to a SANS institute study[2], 28% of the surveyed organizations have had endpoints accessed by attackers, and 24% don't know whether they'd been breached.

Endpoint compromise rates



91%[1] of organizations have experienced at least one attack in the course of a year.

1 in 10[1] organizations have faced a targeted attack (as far as they are aware) over the same period.

30%[1] of organizations have still not fully implemented anti-malware software

1 The Kaspersky Global IT Risk Report, Kaspersky, 2019

2 2019 SANS Survey on Next-Generation Endpoint Risks and Protections, The SANS Institute, 2019

3 Cybersecurity workforce study, (ISC)[2] 2019,

4 Official Annual Cybersecurity Jobs Report, Cybersecurity Ventures, 2019

Human error

Unfortunately, attached to most of your endpoints is the single most vulnerable component in any organization's infrastructure — the user. Your users may well regularly access your corporate data remotely and on their own devices, and many will have grown up online, picking up bad habits and over-confidence along the way. And they, as well as everything else, must also be kept safe.

So detecting and preventing unsafe behavior in today's complex IT environments becomes yet another job for the hard-pressed security specialist.

And IT professionals can make mistakes too – we're all only human, after all — mistakes that can result in attacks via vulnerabilities on irregularly patched corporate or personal devices, for example.

Resources and the lack of them

2 out of 3[3] organizations are experiencing a lack of information security personnel.

It's projected that by 2021 **3.5 million**[4] cybersecurity jobs are going to be unfilled.

So the IT specialist clearly has a lot to do.

Even for smaller organizations, there's an ever-increasing volume of security events to go through, analyze and respond to daily – hard to keep on doing efficiently and in a timely manner. Cybercriminals know that businesses are struggling here, and are taking full advantage.

And, even for those lucky enough to have deep pockets, there's a global shortage of trained cybersecurity professionals. This problem isn't new, but based on how many specialists are being trained each year, it's not going away anytime soon.

Keeping your security specialists happy and focused under these circumstances, or just keeping them at all, is a challenge. Burnout is a big issue, particularly if your highly skilled and expensively trained team are spending all day wading through mundane tasks.

Plus, or course, there's the issue of financial resources. And processor power. And everything else it takes to optimize your security without impacting on processing speeds, employee productivity, user satisfaction or budgets.

The solution

So what are the answers?

Effective protection

First and foremost, everything hangs on **effective endpoint protection** and a strong EPP (Endpoint Protection Platform) – it's that simple. Preventing threats at endpoint level, before they can trigger alerts, reduces the stress on resources, mitigates the risk of an attack succeeding, and helps keep the business running smoothly and safely. This applies to both commodity attacks, which take up most of the time, and more complex and even targeted attacks, which are most likely to succeed and to do the most damage.

Our recommended approach is a combination of **multi-layered endpoint defenses** – a strong baseline protection against commodity threats, and layered, multi-faceted defenses against the latest, more complex threats.

Also it's important to remember that some threats are designed specifically to evade EPPs, and for those different detection methods should be used, like **automated sandboxing**.

EDR (Endpoint Detection and Response) provides the next critical security layer. EPP provides initial identification and protection, while EDR provides visibility and deeper analysis options, allowing you to see how the attack has started and what stage it's at right now. Besides detection, EDR also provides multiple response options, so the threat revealed can be quickly and efficiently contained.

EDR can only be effective in combination with a strong bedrock of protection. The more incidents your EPP solution can prevent up front, the fewer your EDR solution has to deal with, and the more resources you can focus on these few.

Tackling human behavior

From a user perspective, one of the best ways to avoid human error is of course to remove opportunity, and temptation, through **application, web and device controls**. Effective controls, far from acting as a constraint on the business, can actually boost productivity – through blocking time-wasting as well as potentially dangerous entertainment websites and social media, for example.

But here, user education really is key. The right **cybersecurity awareness training** can have a profound effect on employee behavior, changing the corporate culture, significantly lowering corporate risk, and dramatically reducing the IT Department workload.

The return on your investment

Finally, any approach has to be able to justify itself financially in terms of ROI, and to operate now, and in future, in environments with finite resources, which may include limited security specialist expertise.

Automation and streamlining

In view of the escalating volumes of threats, and the industry shortage of security specialists available to work on them, **automating security tasks** where possible becomes critical. This leaves your security specialists free to use their valuable time and skills in dealing with those incidents which genuinely require human input and expertise (and keeps them happier and more motivated as a result).

Automating tasks also removes the risk of man error – automatically prioritizing and implementing the patching of systems vulnerabilities, for example, is much more effective than relying on human operators finding the time to undertake this critical but unexciting activity.

Straightforward deployment and a centralized, streamlined **management console** also saves times and resources. Switching consoles between operations, and hunting around for commands, is not just time-consuming and frustrating – it also introduces opportunities for administrative error and omission.

A note on multi-layered protection

We've said that any solution aimed at protecting against all forms of cyberthreats, including advanced and targeted attacks has to be multi-layered.

First of all, the solution has to provide **robust baseline endpoint protection,** including endpoint controls (with web, application and device blocking and restriction capabilities) and a hardened anti-malware engine. It's also preferable to have automated patch management and vulnerability assessment capabilities in place, to save IT personnel time and effort on performing routine tasks.

But advanced malware sets additional challenges which require further security layers. The malware may well be specifically designed to bypass even the most sophisticated endpoint detection mechanisms, lying hidden and dormant until the right opportunity to launch arises. The answer here is to persuade the malware to reveal itself and activate in a safe, controlled environment. This is where a **sandbox** comes in — one, which preferably should be able not only to detect, but to respond to threats in a highly automated manner.

Detecting complex behaviors on endpoints is also the focus of **EDR.** Like EPP, EDR should ideally combine automation with the tools and visibility to support human input where required. The security officer needs to be able to perform root cause analysis of incidents and to respond to threats in a timely manner, manually or by utilizing automated response options.

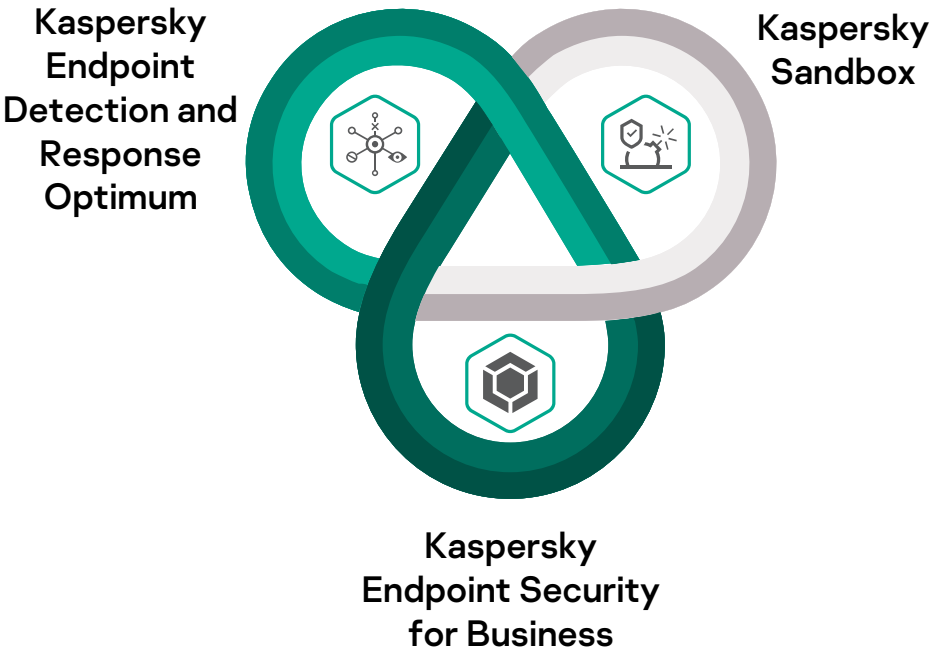
Bringing EPP, Sandbox and EDR technologies together allows commodity malware to be addressed fast and efficiently, limits the opportunities for human error, and reduces the risk of a successful advanced or targeted attack by detecting and responding even to new, unknown and zero-day threats.

And having an integrated solution for all this means no gaps between different tools, which hackers and attackers can exploit.

Kaspersky's solution

All the issues mentioned above are resolved in the optimal manner by Kaspersky's Integrated Endpoint Security solution, a highly automated solution consisting of integrated endpoint protection and controls, an automated sandbox, and EDR. All these three components work together from the basis of a strong EPP. Let's take a more detailed look into each component, as they offer even more than the resolution of the issues described above.

Strong baseline endpoint protection



Kaspersky Endpoint Security for Business is well-established as providing outstandingly robust EPP (including protection against ransomware and fileless attacks) utilizing the most tested and most awarded anti-malware engine on the market.

Endpoint protection layers provided by Kaspersky Endpoint Security for Business include:

- Our award-winning anti-malware engine enhanced with machine learning
- Ransomware detection
- Behavior Detection with Automatic Rollback — identifying and blocking advanced threats including fileless malware and admin account takeover, and reversing any changes already made.
- Exploit prevention
- Mobile threat defenses and EMM integration
- Host-based intrusion prevention (HIPS)
- Firewall and OS firewall management
- Automated threat intelligence (Kaspersky Security Network)
- Encryption — including OS-embedded encryption management
- Security Policy Advisor — monitoring modifications to optimized security settings
- Vulnerability assessment and patch management
- OS & 3rd party software installation
- SIEM systems Integration

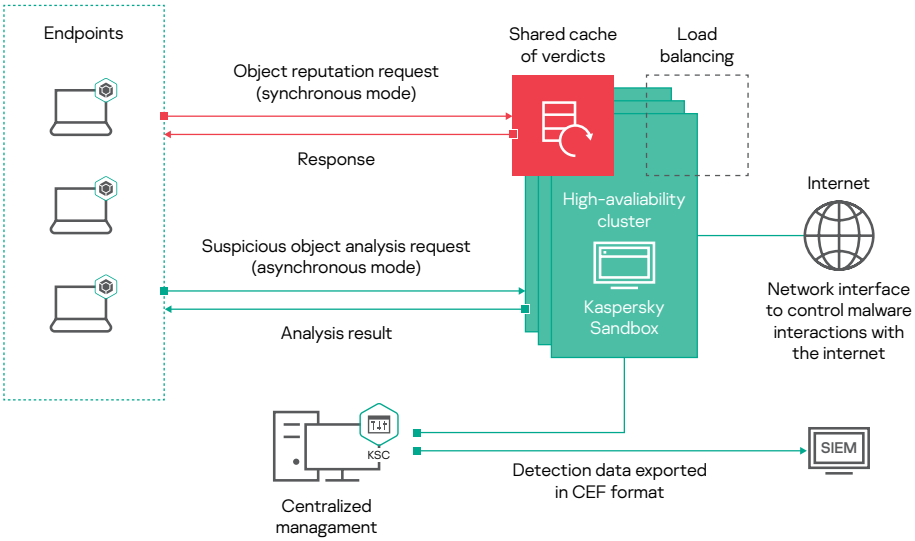
Systems hardening and human error mitigation is provided though controls including:

- Application Control with category-based whitelisting
- Adaptive Anomaly Control which monitors and blocks suspicious actions that are not typical of the computers in a company's network
- Device Control – controlling and blocking the plug-in of external devices
- Web Control – blocking or restricting access of potentially dangerous, time-wasting or inappropriate sites

For more information about Kaspersky Endpoint Security for Business, please visit our website.

Automated sandbox

The Kaspersky Sandbox automatically detects and responds to threats designed to bypass endpoint protection – with no human intervention required.



Kaspersky Sandbox workflow

Objects being scanned are run by the clustered sandbox servers in an isolated virtual machine that simulates a workstation. The component receives a file analysis request from the Kaspersky Endpoint Security for Business agent installed on the end-user machine, after which the object is queued on one of the cluster servers. When the file is sent for processing, Kaspersky Sandbox runs it and logs all actions it performs. The component analyzes the obtained data for malicious and suspicious activity, and returns the verdict to the Kaspersky Endpoint Security for Business agent that requested the scan. The verdict is also sent to the operational cache, allowing other hosts to quickly retrieve information about the scanned object without having to reanalyze it. This reduces the load on the Kaspersky Sandbox servers and improves the response time to threats.

After the file is detected as malicious, its Indicator of Compromise (IoC) can be used to launch an automatic remediation task by the Kaspersky Endpoint Security for Business engine, in order to delete the file from all other machines in the network.

Techniques used by Kaspersky Sandbox include:

- Monitoring interaction with internet resources
- Module loading
- Synchronous and asynchronous scanning modes
- Counter evasion techniques
- Applying different emulation modes
- User action modelling
- Automatic IoC generation and infrastructure scanning
- Automatic prevention

For more information about Kaspersky Sandbox, please visit our website.

Optimized EDR

Kaspersky Endpoint Detection and Response Optimum complements Kaspersky Endpoint Security for Business, delivering full visibility and the ability to apply root cause analysis, for a complete understanding of the status of corporate defenses against advanced threats.

The IT security specialist is provided with the information and insights needed for effective investigation and a fast, accurate response to incidents before any damage can occur.

Working as a part of our Integrated Endpoint Security solution, Kaspersky Endpoint Detection and Response Optimum enables root cause analysis, to be conducted using:

- Attack spread path visualization, showing how the threat developed on the endpoint
- Information on the file, including metadata, file origin, modification data, digital signature, etc.
- Information on the host and the user
- Information on the detect
- Process injection
- File drops
- Registry key modifications
- Connections

After detecting a threat, several automated and 'single-click' response options are available, including:

- Isolate host
- Launch scan of the host
- Remove (quarantine) file
- Kill process
- Prevent process from executing

For further investigation, capabilities like importing IoCs or generating them based on detects, and scanning for those IoCs with preset automated response options are available.

For more information about Kaspersky Endpoint Detection and Response Optimum, please visit our website.

Kaspersky Endpoint Detection and Response Optimum is available both on-premises and in the cloud*.

According to a Forrester study, one of the main requirements for the companies they interviewed is for their security solution to be deployed with little to no disruption to users. This principle is at the heart of Integrated Endpoint Security

Management and administration

All components of our solution are built in-house and administered through the same single console, and utilize the same multi-purpose endpoint agent. So day-to-day management is centralized, straightforward and efficient.

Security awareness

We also offer computer-based training products that combine expertise in cybersecurity with the best-known educational technologies and practices. This approach changes users' behavior and helps to create a cybersafe environment throughout the organization.

The Kaspersky Security Awareness develops a culture of cybersafe behavior:

- educating users about when to alert administrators to signs of a genuine potential threat
- reducing user error resulting from ignorance or naivety
- decreasing the number of security alerts for administrators to triage

You can follow your learners' progress through the user-friendly dashboard, with live data tracking, trends and forecasts, together with recommendations on how to boost your results.

For more information about Kaspersky Security Awareness, please visit our website.

- **52%** of companies regard employeesas the biggest threat to corporate cybersecurity[6]
- **60%** of employees have confidential data on their corporate device (financial data, email database, etc.)
- **30%** of employees admit that they share their work PC's login and password details with colleagues[8]

6 The cost of a data breach, Kaspersky, 2018

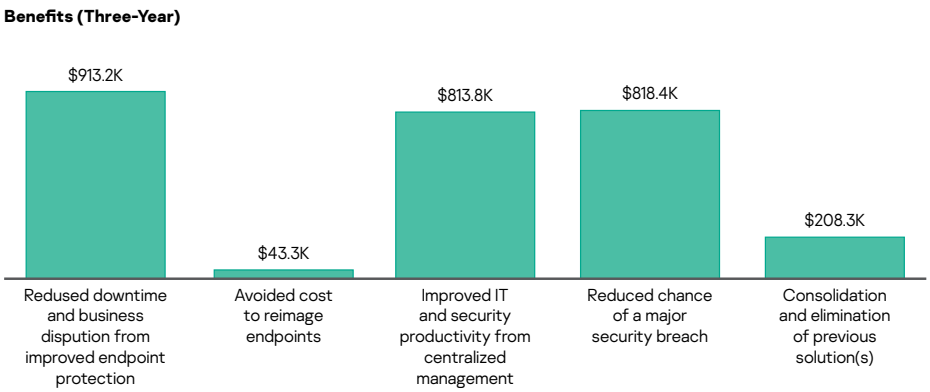
* There are some restrictions to the range of features and functionality that can be managed via the cloud console. For full information, see the online help.

Your ROI

As with any solution, the costs are as important as the benefits we provide. Below is an example of what Return on Investment for Kaspersky solutions looks like, based on a Forrester study[7] of a Kaspersky security solution built upon Kaspersky Endpoint Security for Business and Kaspersky Endpoint Detection and Response.

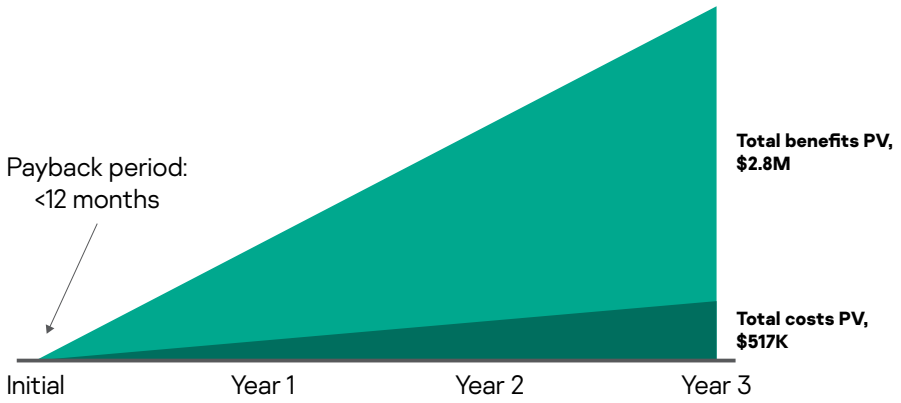
Risk-adjusted present value (PV) quantified benefits experienced by companies interviewed for the Forrester study:

- **Nearly $1.0 million:** the revenue impact of improved uptime at the endpoint from fewer instances of disruption.
- **Over $40,000:** fewer security related incidents saved IT productivity by reducing the need to reimage endpoints.
- **Over $800,000:** facilitated management of multiple security solutions through the centralized management console drove productivity savings.
- **Over $800,000:** a major uplift to overall security posture reduced the chance of a "major" security breach.
- **Over $200,000:** the cost savings associated with moving to Kaspersky.



Forrester's interviews with existing customers and subsequent financial analysis found that an organization based on these interviewed organizations would experience benefits of $2.8 million over three years versus costs of over $500,000, adding up to a net present value (NPV) of $2.3 million and an ROI of 441%.

Financial Summary



7 The Total Economic Impact™ Of Kaspersky Security Solutions, a commissioned study conducted by Forrester Consulting, January 2020

8 Sorting out a Digital Clutter, Kaspersky, 2019

In summary

Endpoint protection is vital in keeping your organization safe in today's threat landscape. And the best way to protect your endpoints is a multi-layered solution, using different techniques to detect and respond to threats in a highly automated way, while enabling human input for more complicated tasks and important decisions.

Kaspersky's Integrated Endpoint Security solution has been designed specifically to address the needs of organizations for protection against commodity threats, advanced and complex threats and human error by:

- implementing **a multi-layered, integrated protection, detection and response** strategy
- **automating** your defenses, reducing the time and effort required to respond even to targeted and advanced attacks
- achieving the **highest detection rates**
- fostering a **cybersafe culture through controls and security awareness**
- ensuring a **substantial return on your investment**

All this means that you can enjoy the highest levels of security against even the most complex cyberthreats without tying up valuable resources.

For more information about how Integrated Endpoint Security can help secure your organization against complex attacks without putting pressure on your resources, please **visit our website**.

www.kaspersky.com