Integrated solutions 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.

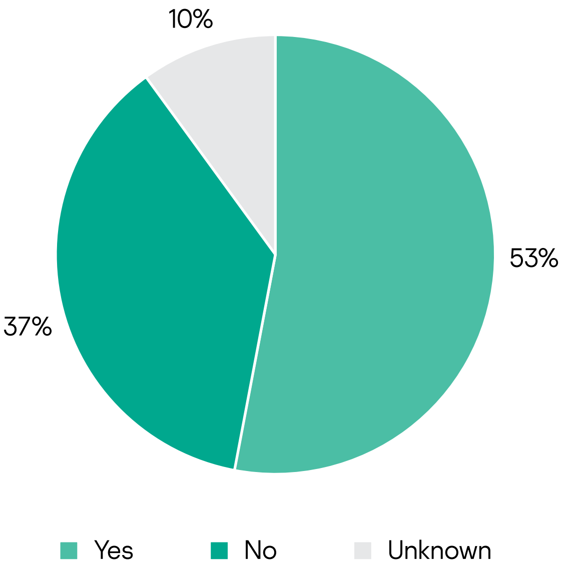
That said, commodity threats also remain an issue: the sheer volume of these is a huge problem in today's world.

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], 53% of organizations endpoints and 10% didn'tknow 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.

- **53%**[2] of organizations know their endpoints have been compromised
- **30%**[1] of organizations have still not fully implemented anti-malware software
- **56%**[3] of breaches take months or longer to uncover

2 out of 3[4] organizations are experiencing a lack of information security personnel.

It's projected that by 2021 **3.5 million**[5] cybersecurity jobs are going to be unfilled.

[1] The Kaspersky Lab Global IT Risk Report, Kaspersky, 2019

[2] Next-Gen Endpoint Risks and Protections, The SANS Institute, 2017

[3] 2019 Data Breach Investigations Report, Verizon, 2019

[4] Cybersecurity workforce study, (ISC)^2 2019,

[5] 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

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** – 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 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.

EDR (Endpoint Detection and Response) provides the next critical security layer. EPP (Endpoint Protection Platform) 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. Beside detection, EDR also provides proactive 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

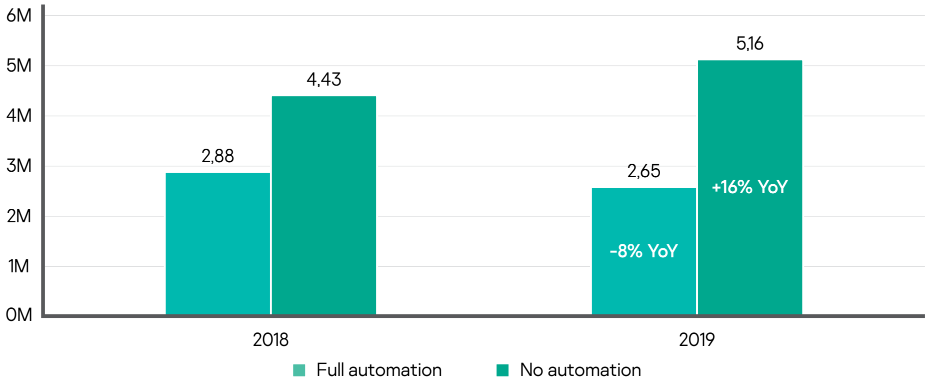
In view of the escalating volumes of threats, and the industry shortage of security specialists available to work on them, **automating security tasks** where possible becomes critical. This leaves your security specialists free to use their valuable time and skills in dealing with those incidents which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

Automating tasks also removes risk of human 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.

Containment costs for organizations without security automation rose 16%[6] and for those with employing automation – decreased by 8%[6].

Costs
depending on security automation level



[6] Cost of a Data Breach Report 2019, Ponemon Institute, 2019

A note on multi-layered protection

We’ve said that any solution aimed at protecting against all forms of cyberthreat, 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 routing 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 it. Some of today’s sandboxes also provide a fast, automated response to the threat detected.

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 analysts need 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

With Kaspersky Endpoint Security, we’ve created a highly automated integrated solution consisting of endpoint protection and controls, an automated sandbox, and EDR, complemented by an optional cybersecurity awareness training platform.

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
- Ransomware detection and protection
- Behavioral Detection with Automatic Rollback - identifying and blocking advanced threats including fileless malware and admin account takeover, and reversing any changes already made.
- Mobile threat defenses and EMM integration
- IPS/HIPS
- Firewall and OS firewall management
- Kaspersky Security Network threat intelligence
- Encryption - including OS-embedded encryption management
- Security Advisor - monitoring modifications to optimized security settings
- Automated vulnerability and patch management
- OS & 3rd party software installation
- SIEM systems Integration

Granular controls

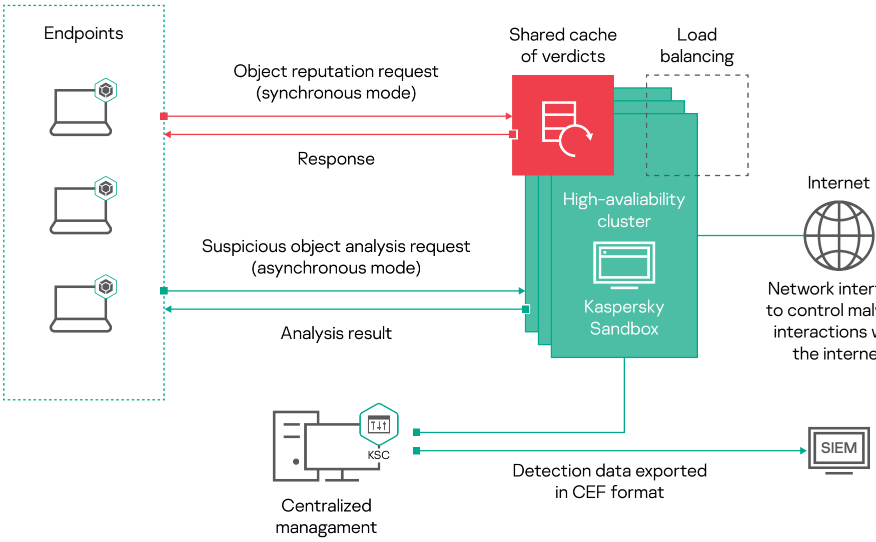
Systems Hardening and human error mitigation is provided though controls including:

- Application Control with category-based whitelisting
- Adaptive Anomaly Control - automatically raising security to the highest level appropriate to everyone in the organization
- 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 https://www.kaspersky.com/small-to-medium-business-security/endpoint-advanced

Automated sandbox

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


Endpoints
Shared cache of verdicts
Load balancing
Object reputation request (synchronous mode)
Response
High-avaliability cluster
Internet
Suspicious object analysis request (asynchronous mode)
Kaspersky Sandbox
Network interface to control malware interactions with the internet
Analysis result
KSC
SIEM
Detection data exported in CEF format
Centralized managament

Kaspersky Sandbox workflow

Objects being scanned are run by the clustered sandbox servers in an isolated virtual machine that simulates a workstation.

The sandbox analyzes the data for malicious and suspicious activity, and returns the verdict to the endpoint agent that requested the scan, as well as to the operational cache, allowing other hosts to quickly retrieve information about the scanned object without having to reanalyze it.

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

Techniques used by Kaspersky Sandbox include:

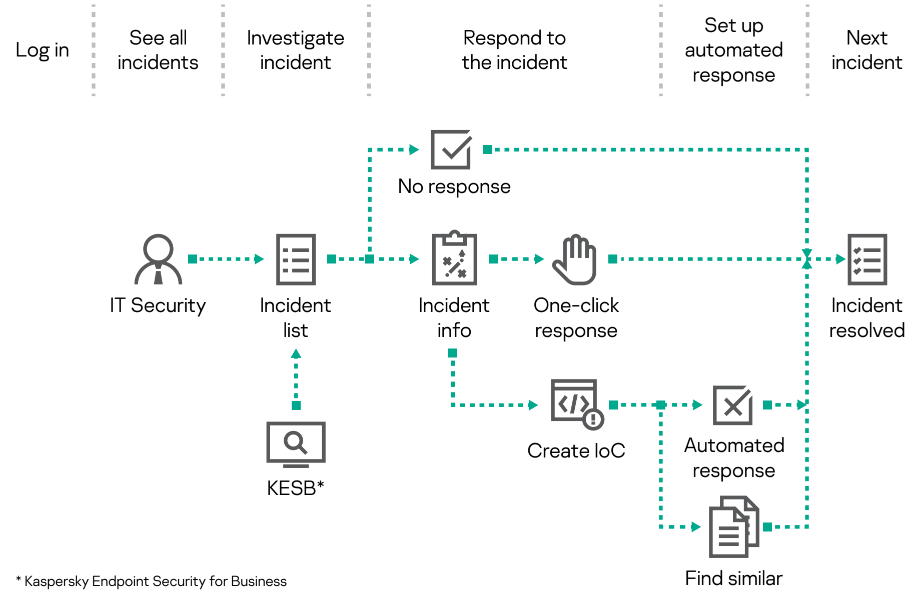
- Monitoring interaction with internet resources
- Module loading
- Synchronous and asynchronous scanning modes
- Counter evasion techniques
- Applying different emulation modes
- User action modelling
- Automatic IoC generation and infrastructure scanning
- Automatic prevention

For more information about Kaspersky Sandbox, please visit https://www.kaspersky.com/enterprise-security/malware-sandbox

Optimized EDR

Kaspersky EDR Optimum provides for both automated and manual analysis and responses to advanced threats arising at endpoint level.

Abnormal user behavior can be identified, and evasive and in particular fileless threats are automatically detected and remediated as they try to mimic common behavior. Visual information and the ability to conduct root-cause analysis help ensure a rapid reaction and swift neutralization.



* Kaspersky Endpoint Security for Business

Kaspersky EDR Optimum workflow

Working as a part of the Kaspersky Endpoint Security solution, Kaspersky EDR Optimum is able to use varied techniques to detect attacks and visualize them in the attack kill-chain, including such traces as:

- Process injection
- File drops
- Registry key modifications
- Connections
- Anomalies in user behavior

After detecting a threat, response options include:

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

Kaspersky EDR Optimum combines high levels of automation, including processes like importing and generating IoCs, initiating further scans and responding to incidents, with single-click manual response options.

For more information about Kaspersky EDR Optimum, please visit http://www.kaspersky.com/enterprise-security/edr-security-software-solution

According to Forrester[7], one of the main requirements for many organizations is for their security solution to be deployed with little to no disruption to users. This principle is at the heart of Kaspersky Endpoint Security

Management and administration

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

[7] The Total Economic Impact™ of Kaspersky Security Solutions, Forrester, 2020

- **52%** of companies regard employees as the biggest threat to corporate cybersecurity[7]
- **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]

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.

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 automated learning management platform takes just 10 minutes to launch, after which it builds an education schedule for each group of employees, providing interval learning with constant reinforcement, offered automatically through a blend of training formats, including:

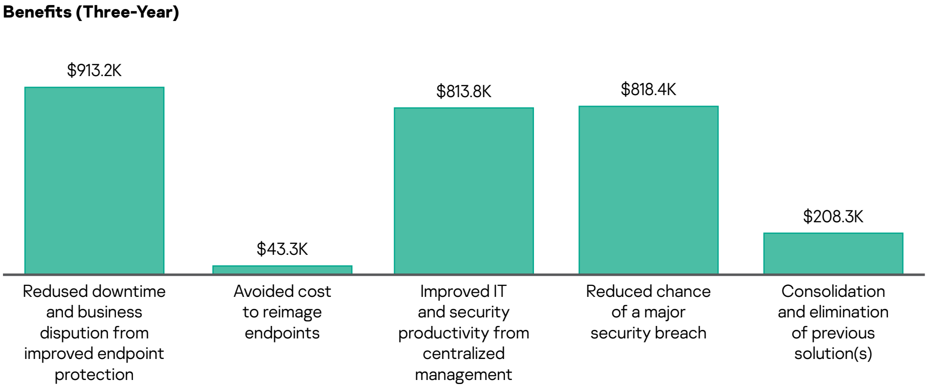
- learning modules
- email reinforcement
- tests
- simulated phishing attacks

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: https://www.kaspersky.co.uk/enterprise-security/security-awareness

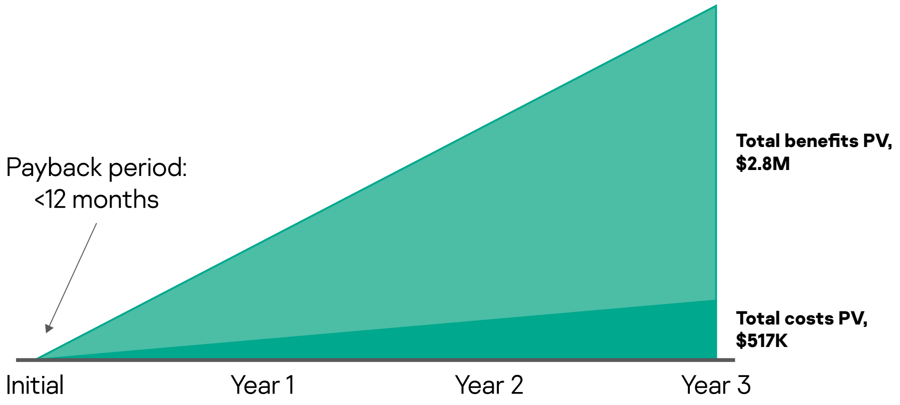
Your ROI

As with any solution, the costs are as important as the benefits we provide. Below is an example of what a typical Return on Investment in Kaspersky solutions looks like, based on a Forrester study[7] of a Kaspersky Security Solution with Kaspersky Endpoint Security for Business at its core:



Forrester's interviews with existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced 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, Forrester, 2020

[8] Sorting out a Digital Clutter, Kaspersky Lab, 2019

In summary

Endpoint protection is vital in keeping your organization safe in the modern 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 Endpoint Security integrated solution was designed specifically to address the need of organizations for protection against commodity threats, advanced and targeted attacks 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 Kaspersky Endpoint Security can help secure your organization against complex attacks without putting pressure on your resources, please visit
https://www.kaspersky.com/small-to-medium-business-security/endpoint-security-solution

www.kaspersky.com