

Kaspersky Certification



Kaspersky hereby confirms that

Carlos Souza

has successfully completed all the requirements
to acquire the certificate:

**Certified Professional: Kaspersky Endpoint Security
and Management (002.11.1)**

Issued on: **10 January 2020**
Certificate number: **002.11.1-AAS-0046790**

Eugene Kaspersky,
Chief Executive Officer

A stylized, handwritten signature in black ink, appearing to read "Eugene Kaspersky".

Kaspersky Endpoint Detection and Response Optimum

91% de todas as organizações foram afetadas por ataques cibernéticos durante 2019, sendo que **1 a cada 10** sofreu um ataque direcionado¹.

"Uma solução de EPP frágil destruirá o valor de uma ferramenta de EDR"²

"As pessoas e o tempo tornaram-se a nova métrica de retorno do investimento para ferramentas de EDR"²

Principais benefícios

- Proteja-se das ameaças avançadas e complexas mais frequentes e mais perturbadoras
- Economize tempo e recursos com uma ferramenta simples e automatizada
- Veja o escopo integral das ameaças complexas em toda a rede
- Entenda a causa básica da ameaça e como ela realmente ocorreu
- Evite mais danos com a rápida resposta automatizada

O problema

Ameaças complexas causam distúrbios

A época do malware simplista já se foi, e as ameaças tornaram-se muito mais complicadas, trazendo mais distúrbios e prejuízos para as empresas e ficando despercebidas por mais tempo

Você está sofrendo um ataque

Essas ameaças complexas tornaram-se muito mais baratas e frequentes, então as organizações que acreditam estar fora do radar delas agora precisam se proteger.

Eficiência é fundamental

Para aumentar ainda mais o problema, as organizações enfrentam grande falta de recursos, inclusive dois dos mais valiosos: tempo e pessoal qualificado.

Como podemos ajudar

O Kaspersky Endpoint Detection and Response (EDR) Optimum ajuda você a se manter em segurança diante de ameaças complexas e avançadas, fornecendo detecção avançada, investigação simplificada e resposta automatizada.

Além das funcionalidades essenciais

Oferece visibilidade detalhada, ferramentas simples de investigação e opções de resposta automatizada para não apenas detectar a ameaça, mas também revelar seu escopo completo e sua origem, além de reagir imediatamente, evitando a interrupção dos negócios.

Defesa aprofundada real

Apresenta um kit de ferramentas de detecção e resposta altamente automatizadas fácil de usar, juntamente com as funcionalidades inigualáveis de proteção de endpoints e detecção avançada do Kaspersky Endpoint Security for Business, formando uma solução unificada.

Uma ferramenta inteligente garante a eficiência

Libera seu tempo e otimiza recursos de mão-de-obra e sobrecargas de TI por meio de controles simples centralizados e um grande nível de automação. Fluxo de trabalho simplificado em um único console, disponível no local e na nuvem³.

Casos de uso essenciais de EDR

Responda a perguntas importantes

- Qual é o contexto do alerta?
- Quais as ações já foram tomadas em relação ao alerta?
- A ameaça detectada ainda está ativa?
- Há outros hosts sendo atacados?
- Qual foi o caminho que o ataque seguiu?
- Qual é a verdadeira causa básica da ameaça?

Conheça o escopo completo da ameaça

- Assim que souber que está em risco de uma ameaça global, por exemplo, se uma autoridade regulatória solicitar que você verifique um Indicador de comprometimento (IoCs, Indicator of compromise) específico, você poderá:
 - Importar IoCs de fontes confiáveis e realizar verificações periódicas de sinais de ataque
 - Investigar um alerta detalhadamente, gerar IoCs com base nas ameaças detectadas e executar verificações em toda a rede para descobrir se outros hosts foram afetados

Responda a ameaças prolíficas imediatamente

- Coloque automaticamente em quarentena os arquivos associados a ameaças complexas em todos os endpoints
- Isole automaticamente os hosts infectados ao encontrar um IoC associado a uma ameaça de disseminação rápida
- Evite que o arquivo malicioso seja executado e se espalhe pela rede durante a investigação

¹ Relatório Global de Riscos de TI, Kaspersky, 2019

² IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, Doc # US45794219, 2020

³ Há algumas restrições em relação à série de recursos e funcionalidades que podem ser gerenciados pelo console na nuvem. Para obter todas as informações, visite <https://kas.pr/epp-management-options>

Agora é possível:

Conheça o escopo completo da ameaça

Receba os alertas de segurança de seus endpoints e os analise melhor para endpoints toda a amplitude e profundidade da ameaça. Isso ajuda a garantir que os incidentes sejam tratados na íntegra e não seja deixada qualquer resíduo da ameaça no endpoint.

Simplifique seu fluxo de trabalho

O fluxo de trabalho simplificado em um único console disponível no local e na nuvem é integrado a cenários e controles de EDR simples, inclusive a visualização detalhada, a verificação de IoCs e opções de resposta que não exigem muito tempo ou experiência em cibersegurança.

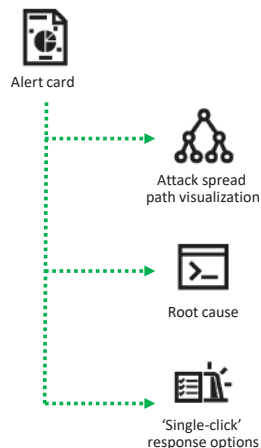
Incremente suas defesas

A adição da Kaspersky Sandbox cria uma solução completa de segurança integrada de endpoints, defesas multicamadas eficazes e extremamente automatizadas contra ameaças a commodities, complexas e evasivas.

Análise dados de alertas aprimorados

O Kaspersky EDR Optimum aprimora as informações necessárias dos incidentes e ajuda a entender as conexões entre eventos diferentes por meio da visualização do caminho de disseminação do ataque.

É fornecida visibilidade de todos os hosts na rede com a verificação de Indicadores de comprometimento (IoCs) importados ou gerados.



Responda automaticamente

Configure respostas automatizadas a ameaças descobertas em todos os endpoints com base em verificações de IoCs ou reaja imediatamente a incidentes detectados com opções de 'clique único'.

As opções de resposta incluem: isolar o host, colocar o arquivo em quarentena, executar a verificação do host e evitar a execução do arquivo.

Outras opções de EDR

O Kaspersky Endpoint Detection and Response Optimum é uma das várias opções de EDR que oferecemos, cada uma adaptada a necessidades específicas de clientes. Talvez você também queira considerar:

Kaspersky Endpoint Detection and Response

Solução de EDR especializada aprovada pelo setor e pelos clientes, ideal para organizações de TI com equipes de segurança de TI maduras, que ajuda a chegar ao fundo dos ataques avançados e direcionados mais sofisticados. Fornece descoberta aprimorada de ameaças, investigação eficiente, busca proativa de ameaças e resposta centralizada a incidentes. <https://www.kaspersky.com/enterprise-security/endpoint-detection-response-edr>

Kaspersky Managed Detection and Response

Solução totalmente gerenciada e adaptada individualmente de detecção, priorização e resposta 24 horas por dia com o respaldo de mais de 20 anos de pesquisa de ameaças consistente, permite obter todos os principais benefícios de ter seu próprio Centro de operações de segurança sem precisar realmente instituí-lo. <https://www.kaspersky.com/enterprise-security/managed-detection-and-response>

Para saber mais sobre como o Kaspersky Endpoint Detection and Response Optimum lida com as ameaças cibernéticas e, ao mesmo tempo, facilita o trabalho de sua equipe de segurança e seus recursos, acesse <http://www.kaspersky.com/enterprise-security/edr-security-software-solution>

Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias sobre segurança de TI: business.kaspersky.com/
Segurança de TI para grandes empresas: kaspersky.com/enterprise
Portal de inteligência de ameaças: opentip.kaspersky.com

www.kaspersky.com

2020 AO Kaspersky Lab. Todos os direitos reservados.
As marcas registradas e de serviço são propriedade dos respectivos titulares.



Nós somos comprovados. Somos independentes. Somos transparentes. Temos o compromisso de construir um mundo mais seguro, onde a tecnologia melhora nossas vidas. Por isso, nós a protegemos. Para que todos possam aproveitar as infinitas oportunidades que ela proporciona. Garanta a cibersegurança para um futuro mais seguro.



Proven.
Transparent.
Independent.



Aumente sua segurança Endpoint sem aumentar seus recursos

As tecnologias de cibersegurança aprovadas pelo mercado e pelos clientes, com o EDR no centro, capacitam você a detectar e evitar ataques evasivos muito rapidamente sem exigências adicionais sobre sua equipe.

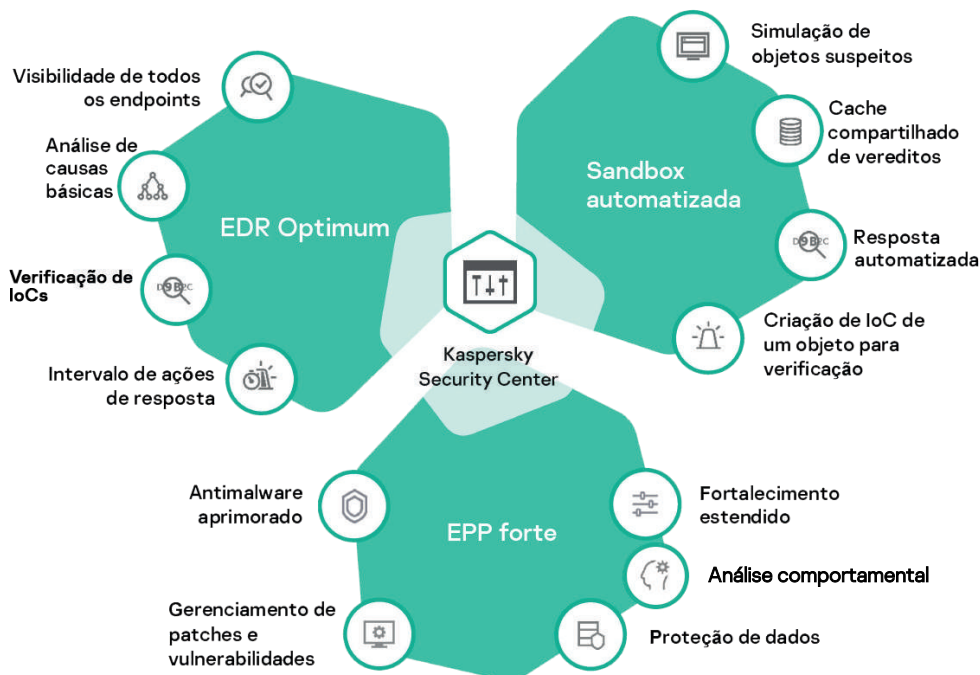
Uma solução totalmente automatizada com o EDR no centro

Os ataques cibernéticos estão se expandindo ano a ano em termos de número, nível de complexidade e impacto financeiro. E esse problema não vai se resolver sozinho.

Isso é fato, e também é fato que o principal alvo dos cibercriminosos no momento são os seus endpoints.

E como você lida com isso?

Desenvolvendo uma segurança de endpoints forte e responsiva, o que acreditamos ser resultado do uso da automação de processos e da adoção de uma abordagem multicamadas:



As chances de capturar uma ameaça serão muito maiores se você se armar com vários métodos diferentes para detectar e evitar ataques. Nossas novas tecnologias de detecção e resposta automatizadas permitem lidar com números muito grandes de incidentes de modo rápido e eficaz, sem envolvimento de pessoas, liberando os especialistas em segurança de TI para que possam se concentrar nas tarefas que realmente exigem seus conhecimentos.

Com essa abordagem, você pode:



Reduzir os riscos de se tornar vítima de um ataque direcionado



Fortalecer seus sistemas e evitar que funcionários se exponham e exponham você a ataques



Maximizar o número de incidentes processados, sem aumentar seus custos de mão de obra

Nós criamos uma solução integrada de segurança de endpoints com três componentes: Endpoint Protection Platform (EPP), a Sandbox e o Endpoint Detection and Response (EDR).

Não estamos simplesmente dizendo que somos bons no que fazemos; para comprovar, temos resultados, avaliações de outras entidades e clientes satisfeitos.



O Gartner Peer Insights Customers' Choice é composto pelas opiniões subjetivas de análises, classificações e dados de usuários finais individuais aplicados com uma metodologia documentada; elas não representam a visão, nem constituem um endosso da Gartner ou de suas afiliadas. <https://www.gartner.com/reviews/customers-choice/endpoint-protection-platforms>

The Forrester Wave™: Endpoint Security Suites, terceiro trimestre de 2019. The 15 Providers That Matter Most And How They Stack Up' por Chris Sherman with Stephanie Balaouras, Merritt Maxim, Matthew Flug e Peggy Dostie.

Para garantir que você tenha o melhor desempenho e o maior retorno do investimento possíveis com sua nova solução, também oferecemos uma série de serviços, como:



Kaspersky Health Check Service

Depois que você instala a solução, nós verificamos se a implementação foi feita corretamente e se você está usando a configuração ideal para sua infraestrutura.



Kaspersky Maintenance Service Agreement

Tempo pré-pago de especialistas em segurança, que ficam de prontidão 24 horas por dia, 7 dias por semana, 365 dias por ano com a missão de assumir seus problemas e conseguir a resolução mais ágil possível.



Kaspersky Security Awareness

Uma família de treinamentos no computador que utilizam as técnicas de aprendizagem mais recentes para reduzir os riscos causados por falha humana, mudando o comportamento dos funcionários e garantindo que não sejam cometidos erros de segurança custosos durante o trabalho com dados e sistemas corporativos.

Expanda sua cibersegurança sem sobrecarregar seus recursos

Nossa solução Endpoint Security compreende camadas fortemente integradas de ferramentas e tecnologias essenciais para a proteção de endpoints, detecção e resposta eficazes.



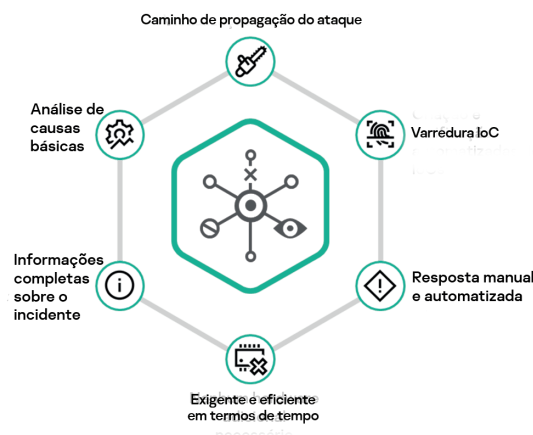
Proteção e controle de endpoints robustos

O **Kaspersky Endpoint Security for Business** oferece proteção robusta baseada em um dos melhores mecanismos antimalware do mercado. O risco de falha humana é minimizado pelo fortalecimento dos sistemas e pela automação de tarefas de rotina, como o gerenciamento de vulnerabilidades e patches, e a instalação de software de terceiros e do sistema operacional. E o recurso Consultor de Políticas de Segurança monitora modificações de configurações de segurança ideais, avisando os administradores sobre qualquer consequência potencialmente negativa.



Defesa contra ameaças complexas

A **Kaspersky Sandbox** complementa a proteção de endpoints com funcionalidades capazes de detectar facilmente até ameaças novas, desconhecidas e complexas, criadas especificamente para burlar as tecnologias de proteção mais sofisticadas. Ela faz isso criando um ambiente virtualizado, para onde os objetos suspeitos são enviados para serem analisados por meio de vários métodos (como simular a atividade do usuário, analisar comportamentos, monitorar conexões de saída, etc), e a reputação deles registrada. Se objetos são identificados como maliciosos, toda a infraestrutura pode ser escaneada e todas as suas atividades maliciosas serem prevenidas, garantindo uma resposta automática através de todos os endpoints.



Visibilidade e resposta automatizadas

Kaspersky Endpoint Detection and Response Optimun é uma ferramenta EDR que trabalha em conjunto com a proteção endpoint e fornece a visibilidade de endpoint, funcionalidades de análise de causas básicas e diversas opções de resposta. Incluindo uma poderosa camada automática de defesa de soluções integradas, fornecendo a visualização dos caminhos que espalham ataques, e entregar um relatório completo do incidente, o host, objetos suspeitos, etc.

Destaques da solução



Protege das ameaças modernas

Evite interrupções e danos aos seus negócios, reduzindo o risco de ameaças a commodities e ameaças cibernéticas mais complexas



Reduz o risco de falha humana

Reduza a possibilidade de falha humana usando controles granulares e automação



Minimiza a carga de trabalho da equipe

Maximize o retorno do investimento automatizando tarefas para poder processar mais incidentes sem aumentar os custos de mão de obra



Alto retorno sobre o investimento

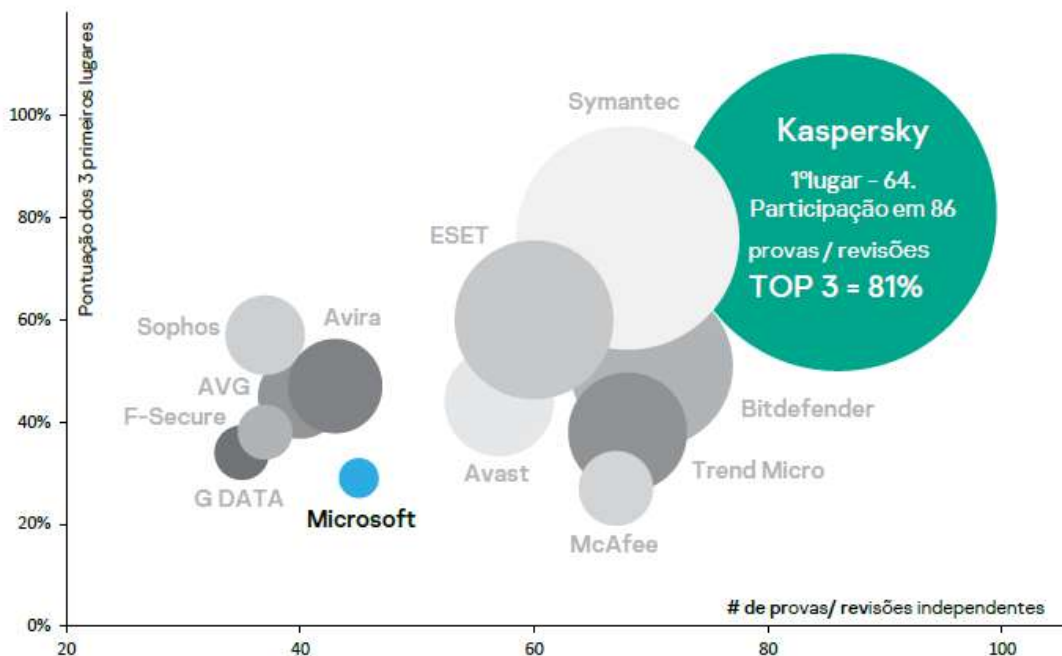
O relatório da Forrester sobre impacto econômico total baseado em entrevistas com clientes mostrou que as organizações que usam nossa solução tiveram, em média, um retorno do investimento de **441%**.

Experimente você mesmo

Visite [esta página](#) para solicitar a demonstração gratuita do Kaspersky Endpoint Security.

Visão global – produtos de segurança de TI da Kaspersky para empresas

A proteção de endpoints, embora crítica, é apenas o início. Não importa se você adota a melhor estratégia de segurança ou uma estratégia de fonte única; a Kaspersky Lab oferece produtos para infraestruturas na nuvem híbrida e para sistemas Windows XP mais antigos que se interconectam ou que funcionam de modo independente para que você possa escolher sem comprometer a eficiência de desempenho ou sua liberdade de escolha. Saiba mais em nosso [site](#).



Análise dos resultados anuais de todas as provas independentes das quais participaram a Kaspersky e produtos da competência: últimos dados disponíveis.

Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias sobre segurança de TI: business.kaspersky.com/
Segurança de TI para grandes empresas: kaspersky.com/enterprise

www.kaspersky.com.br

2020 AO Kaspersky Lab. Todos os direitos reservados.
As marcas registradas e de serviço são propriedade dos respectivos titulares.



Nós somos comprovados. Somos independentes. Somos transparentes. Temos o compromisso de construir um mundo mais seguro, onde a tecnologia melhora nossas vidas. Por isso, nós a protegemos. Para que todos possam aproveitar as infinitas oportunidades que ela proporciona. Garanta a cibersegurança para um futuro mais seguro.

Saiba mais em kaspersky.com/transparency



Proven.
Transparent.
Independent.



**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

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

1 in 10¹ 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

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.

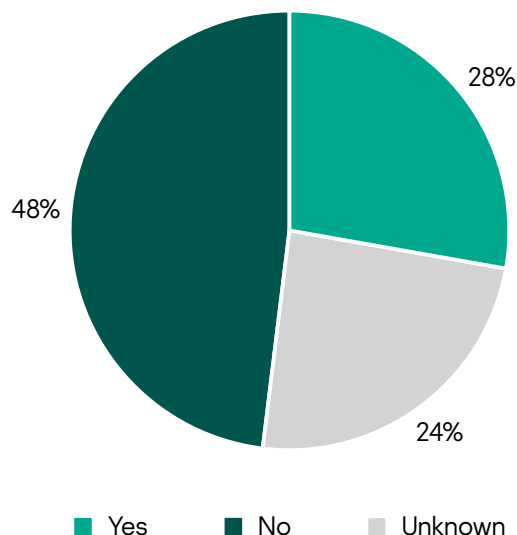
That said, commodity threats also remain an issue: the sheer volume of these is a huge problem in today's world.

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 study², 28% of the surveyed organizations have had endpoints accessed by attackers, and 24% don't know whether they'd been breached.

Endpoint compromise rates



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.

2 out of 3³ organizations are experiencing a lack of information security personnel.

It's projected that by 2021 3.5 million⁴ cybersecurity jobs are going to be unfilled.

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, of 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.

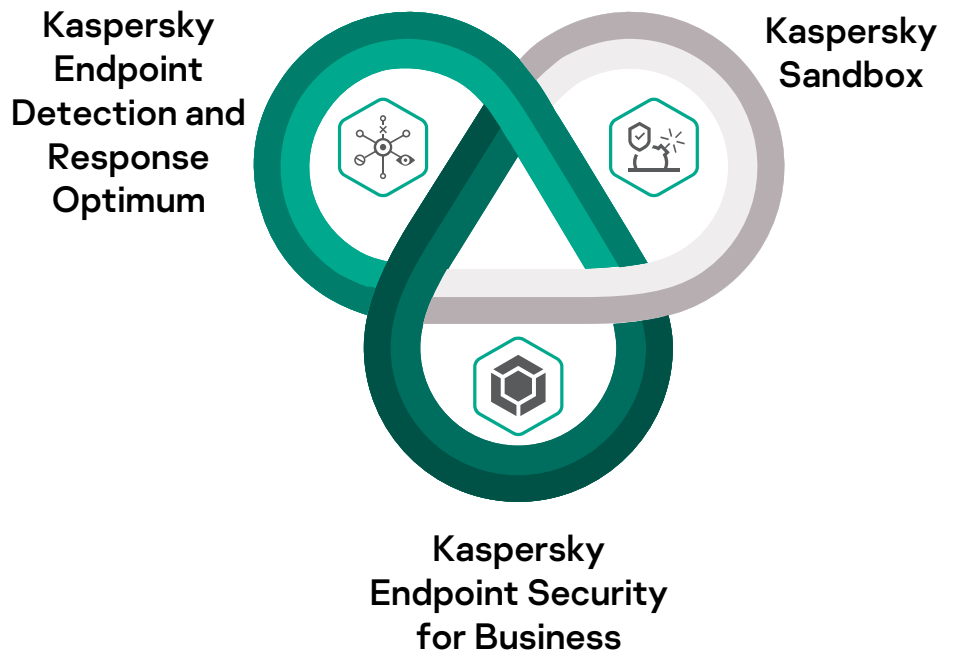
Bringing EPP, Sandbox and EDR technologies together allows commodity malware to be addressed fast and efficiently, limits the opportunities for human error, and reduces the risk of a successful advanced or targeted attack by detecting and responding even to new, unknown and zero-day threats.

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

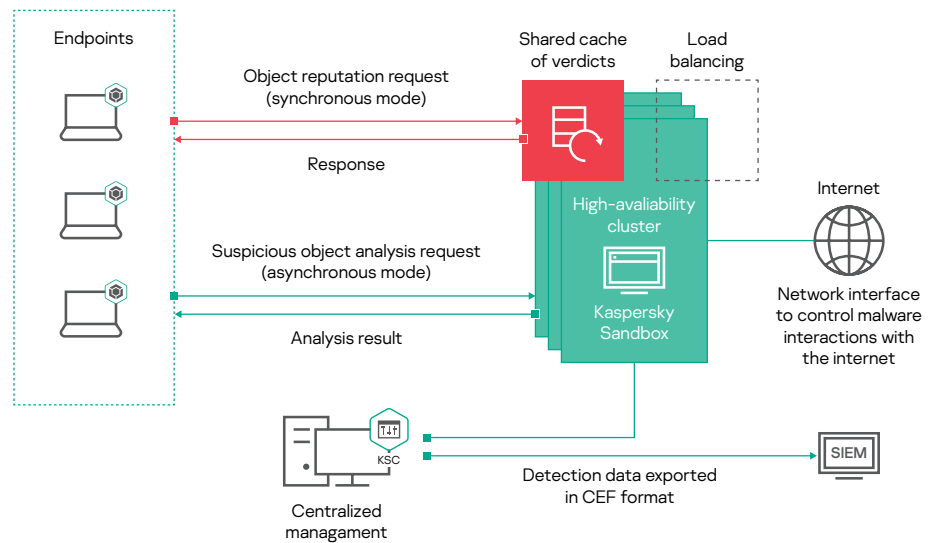
Systems hardening and human error mitigation is provided through controls including:

- 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*.

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](#).

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

- **52%** of companies regard employees as the biggest threat to corporate cybersecurity⁶
- **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 colleagues⁸

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](#).

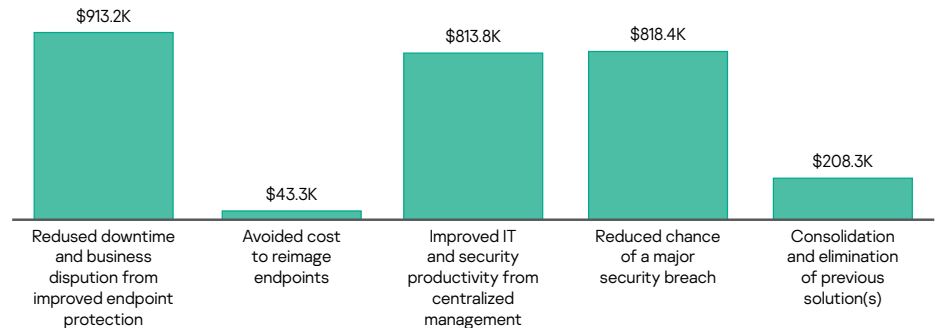
Your ROI

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 study⁷ 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:

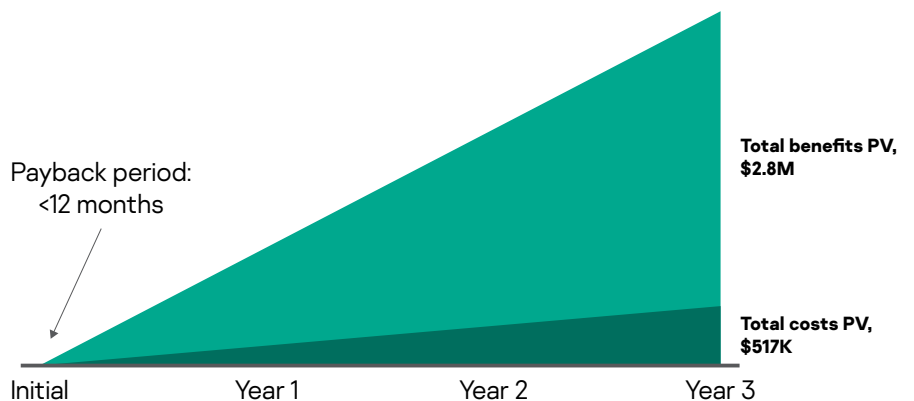
- **Nearly \$1.0 million:** the revenue impact of improved uptime at the endpoint from fewer instances of disruption.
- **Over \$40,000:** fewer security related incidents saved IT productivity by reducing the need to reimage endpoints.
- **Over \$800,000:** facilitated management of multiple security 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.

Benefits (Three-Year)



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

2020 AO Kaspersky Lab. All rights reserved.
Registered trademark and service marks are the
property of their respective owners.



Kaspersky Sandbox

Funcionalidades avançadas de detecção para proteger de ameaças desconhecidas e ambíguas sem a necessidade de contratar profissionais de segurança de TI

Os ataques cibernéticos atuais são capazes de paralisar empresas e devastar sua integridade financeira e sua reputação. Roubo de recursos financeiros e segredos comerciais, perda da confiança do cliente por causa de serviços inativos e inúmeros outros efeitos negativos de ameaças complexas têm um impacto enorme sobre a estabilidade e a prosperidade dos negócios. Para evitar os ataques cibernéticos em rápida evolução, as ferramentas tradicionais criadas para proteger o perímetro da rede (firewalls, gateways de e-mail/da Web, servidores proxy) e também estações de trabalho e servidores (proteção antivírus e soluções do tipo plataforma de proteção de endpoints com funcionalidade básica) isoladas não são mais suficientes. Por isso, as empresas com pensamento inovador precisam considerar seriamente ferramentas especializadas para detectar, investigar e responder a incidentes complexos.

A solução Kaspersky Sandbox é adequada para:

- Empresas que não têm uma equipe de segurança dedicada, onde a responsabilidade pela segurança de TI é do departamento de TI.
- Pequenas empresas que não querem agregar recursos adicionais de segurança de TI.
- Grandes organizações com uma infraestrutura geograficamente distribuída que não contam com especialistas em segurança de TI no local.
- Empresas que precisam garantir que seus analistas de segurança de TI em tempo integral foquem tarefas críticas.

Há mais de 20 anos, a Kaspersky desenvolve ferramentas de proteção para empresas de todos os tamanhos, setores e níveis de maturidade da segurança de TI. Com as pesquisas e o desenvolvimento contínuos, além dos avanços que fizemos na busca, investigação e resposta a ameaças, a Kaspersky continua na vanguarda do combate ao crime cibernético.

O portfólio de produtos e serviços da Kaspersky para deter ameaças complexas inclui:

- Kaspersky Anti Targeted Attack, uma solução de ponta para detectar e investigar ameaças complexas e ataques direcionados no nível de rede.
- Kaspersky Endpoint Detection and Response, uma solução para detectar, investigar e responder a ameaças cibernéticas complexas em estações de trabalho e servidores.
- Kaspersky Threat Intelligence Portal, que oferece acesso à Cloud Sandbox, com relatórios analíticos sobre ameaças de APTs e outros serviços

No entanto, para utilizar essas soluções e serviços com eficiência, as empresas precisam ter um departamento de segurança de TI completo com experiência e conhecimento apropriados. A escassez global de especialistas treinados para lidar com ameaças complexas e o custo de contratá-los muitas vezes é o principal fator que impede as empresas de adquirir esse tipo de soluções e serviços.

Baseada em uma tecnologia patenteada (patente nº US 10339301B2), a Kaspersky Sandbox ajuda as organizações a combater as ameaças modernas, que crescem em número e complexidade, capazes de burlar a proteção de endpoints existente. Complementando as funcionalidades do Kaspersky Endpoint Security for Business, a Kaspersky Sandbox permite que as organizações aumentem significativamente o nível de proteção de suas estações de trabalho e servidores contra malware previamente desconhecido, novos vírus e ransomware, exploits de "dia zero" e outras ameaças sem a necessidade de analistas de segurança de informações altamente especializados.

Isso poupa às pequenas empresas as despesas de recrutamento e contratação desses profissionais tão valiosos. E, no caso de grandes corporações com redes distribuídas, é possível otimizar custos para proteger seus escritórios remotos eficientemente e, ao mesmo tempo, aliviar a carga de trabalho manual dos analistas de segurança.

Opções de fornecimento e implementação

A Kaspersky Sandbox é fornecida como uma imagem ISO que inclui o CentOS 7 pré-configurado e todos os componentes necessários da solução. Ela pode ser implementada em um servidor físico ou em servidores virtuais baseados no VMware ESXi.

Integração

- Sistemas de SIEM podem receber informações sobre as detecções feitas pela Kaspersky Sandbox. Essas informações são enviadas via Kaspersky Security Center, no fluxo de eventos gerais.
- Uma API é implementada na Kaspersky Sandbox para integração com outras soluções, permitindo enviar arquivos para a Kaspersky Sandbox para verificação e solicitar reputações de arquivos.

Escalabilidade

A configuração básica dá suporte a até 1.000 endpoints protegidos, o que facilita o dimensionamento da solução, que oferece proteção contínua para grandes infraestruturas.

Clusterização

É possível clusterizar vários servidores para expandir sua capacidade e disponibilidade.

Licenciamento

A Kaspersky Sandbox é licenciada como um dispositivo de software. Uma licença inclui suporte para até 1.000 usuários do Kaspersky Endpoint Security for Business.

Como funciona

A Kaspersky Sandbox aproveita as práticas recomendadas de nossos especialistas para combater ameaças complexas e ataques em nível de APT, e está fortemente integrada ao Kaspersky Endpoint Security for Business. Ela é gerenciada pelo Kaspersky Security Center, nosso console de gerenciamento unificado baseado em políticas.

O agente do Kaspersky Endpoint Security for Business solicita dados sobre um objeto suspeito do cache operacional compartilhado de vereditos, localizado no servidor da Kaspersky Sandbox. Se o objeto já foi verificado, o Kaspersky Endpoint Security for Business recebe o veredito e aplica uma ou mais opções de neutralização:

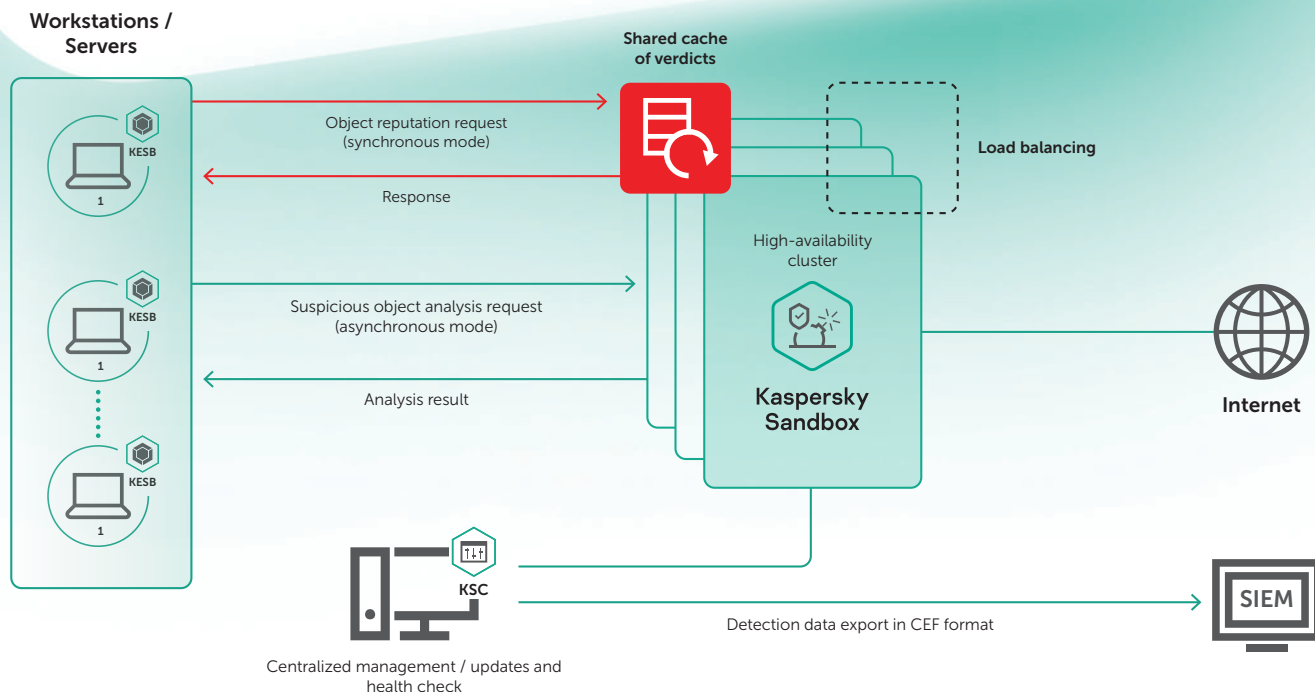
- Remover e colocar em quarentena
- Notificar o usuário
- Iniciar uma verificação de áreas críticas
- Pesquisar o objeto detectado em outras máquinas da rede gerenciada.

Se não for possível obter o veredito sobre a reputação de um objeto do cache, o agente do Kaspersky Endpoint Security for Business enviará o arquivo suspeito para a Sandbox e aguardará a resposta. A Sandbox recebe a solicitação para verificar o objeto, e o objeto de teste é executado em um ambiente isolado da infraestrutura real.

A verificação do arquivo é executada em máquinas virtuais equipadas com ferramentas que simulam um ambiente de trabalho típico (sistemas operacionais/aplicativos instalados). Para determinar a intenção maliciosa de um objeto, é realizada a análise de comportamento, artefatos são coletados e analisados e, se o objeto executar ações maliciosas, a Sandbox o reconhecerá como malware. Durante a análise da Sandbox, um veredito é atribuído ao objeto.

Quando o processo de simulação do objeto é concluído, o veredito resultante é enviado em tempo real para o cache operacional compartilhado de vereditos, permitindo que outros hosts que têm o Kaspersky Endpoint Security for Business instalado obtenham rapidamente dados sobre a reputação do objeto verificado sem precisar analisar o mesmo arquivo novamente. Essa abordagem garante o rápido processamento de objetos suspeitos, reduz a carga sobre os servidores da Kaspersky Sandbox e melhora a velocidade e a eficiência da resposta a ameaças.

A **Kaspersky Sandbox** é um complemento essencial do Kaspersky Endpoint Security for Business. Ela bloqueia automaticamente ameaças avançadas, desconhecidas e complexas sem a necessidade de recursos adicionais, e libera os analistas de segurança de TI para outras tarefas.



Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias sobre segurança de TI: business.kaspersky.com/
Segurança de TI para PMEs: kaspersky.com/business
Segurança de TI para grandes empresas: kaspersky.com/enterprise

www.kaspersky.com

2019 AO Kaspersky Lab. Todos os direitos reservados.
As marcas registradas e de serviço são propriedade dos respectivos titulares.



Nós somos comprovados. Somos independentes. Somos transparentes. Temos o compromisso de construir um mundo mais seguro, onde a tecnologia melhora nossas vidas. Por isso, nós a protegemos. Para que todos possam aproveitar as infinitas oportunidades que ela proporciona. Garanta a cibersegurança para um futuro mais seguro.

Saiba mais em kaspersky.com/transparency



Proven.
Transparent.
Independent.

Kaspersky Certification



Kaspersky hereby confirms that

Roberto Almeida

has successfully completed all the requirements
to acquire the certificate:

**Certified Professional: Kaspersky Endpoint Security
and Management (002.11.1)**

Issued on: **10 January 2020**
Certificate number: **002.11.1-AAS-0038041**

Eugene Kaspersky,
Chief Executive Officer

A handwritten signature in black ink, appearing to read "Eugene Kaspersky".