Solução integrada de segurança de endpoints

Desenvolvendo defesas robustas com recursos limitados

kaspersky

Saiba mais em kaspersky.com
#bringonthefuture

Introdução

A maior parte das organizações, independentemente de seu tamanho, localização ou setor, hoje entende que quando se pensa em um ataque cibernético, a questão não é mais se ele acontecerá, mas quando ele acontecerá. Atualmente, ninguém pode se considerar imune.

Porém, ter tempo, recursos ou (sinceramente) motivação para navegar efetivamente pelo atual cenário de ameaças e segurança — é outra questão.

A maioria dos analistas de segurança de informações — e não há um número deles nem perto de suficiente — tem excesso de trabalho. Cuidar dos novos funcionários e seus dispositivos, entender as novas leis e questões de conformidade, informar-se sobre as ameaças mais recentes – tudo isso precisa ser feito antes de realmente entrar no negócio real da proteção corporativa.

Basicamente, pouquíssimos profissionais de segurança, se houver algum, podem se dar ao luxo de investir todo seu tempo perseguindo ameaças novas e exóticas e reagindo a elas.

É nesse ponto que entram os fornecedores de cibersegurança e seus produtos e soluções. Nosso trabalho é ajudar você a proteger sua infraestrutura integralmente e manter seus usuários seguros, com a menor despesa possível em termos de recursos, inclusive tempo e dinheiro, além de especialistas caros e difíceis de obter.

Os desafios

Primeiro, vamos examinar alguns dos problemas que os gerentes de TI e de segurança de TI enfrentam hoje.

Maior ameaça de ataques avançados ou direcionados

Os ataques direcionados e as ameaças complexas são um problema enorme, e estão crescendo. As ferramentas dos cibercriminosos estão se tornando tão baratas e acessíveis que praticamente qualquer pessoa que tem um computador pode realizar um ataque avançado. Isso significa que as organizações que achavam estar 'fora do radar' em termos de ameaças avançadas estão descobrindo que as coisas mudaram do jeito mais difícil.

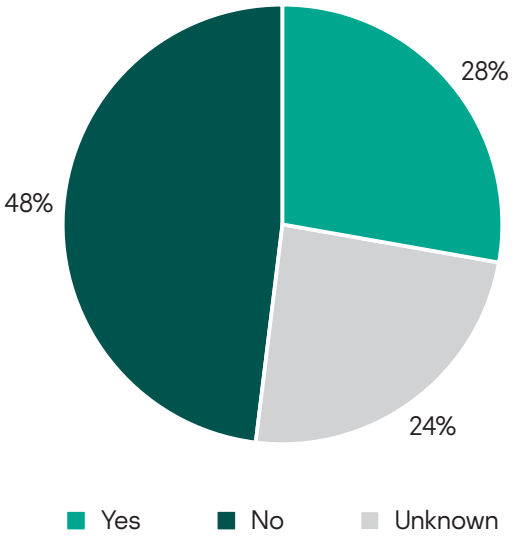
Considerando isso, as ameaças de commodities também continuam sendo um problema: o simples volume delas é um problema enorme no mundo atual.

A grande maioria das ameaças cibernéticas entra pelo endpoint ou é criada para ser ativada nele (ou ambos).

Assim, uma das melhores maneiras de proteger seus ativos é protegendo seus endpoints.

Segundo um estudo do SANS Institute[2], 28% das organizações pesquisadas tiveram endpoints acessados por atacantes, e 24% não sabem se houve violações.

Endpoint compromise rates



91%[1] das organizações sofreram pelo menos um ataque no intervalo de um ano.

1 a cada 10[1] organizações enfrentou um ataque direcionado (na medida em que estão cientes) durante o mesmo período.

30%[1] das organizações ainda não implementaram integralmente nenhum software antimalware

1 Relatório Global de Riscos de TI da 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

Falha humana

Infelizmente, acoplado à maioria de seus endpoints encontra-se o componente mais vulnerável da infraestrutura de qualquer organização, o usuário. Os usuários podem acessar regularmente seus dados corporativos remotamente e em seus próprios dispositivos e, durante esse processo, muitos crescerão on-line, desenvolvendo vícios e excesso de confiança. E, como todo o restante, eles também precisam ser mantidos seguros.

Assim, detectar e evitar o comportamento inseguro nos atuais ambientes de TI complexos torna-se mais uma tarefa para os ocupados especialistas em segurança.

E os profissionais de TI também podem cometer erros; no final, somos todos humanos. Esses erros podem resultar, por exemplo, em ataques por meio de vulnerabilidades em dispositivos corporativos ou pessoais sem os patches regulares.

Recursos e falta deles

2 em cada 3[3] organizações sofrem com a falta de pessoal de segurança de informações.

Segundo as projeções, até 2021, haverá **3,5 milhões**[4] de vagas não preenchidas no setor de cibersegurança.

É evidente que os especialistas em TI têm muitas tarefas.

Mesmo em organizações menores, eles precisam cuidar, analisar e responder diariamente a um volume cada vez maior de eventos de segurança, o que é difícil fazer continuamente de modo eficiente e rápido. Os cibercriminosos sabem que as empresas estão com dificuldades nesse setor e estão tirando proveito disso.

E, mesmo para aqueles que têm a sorte de contar com mais recursos, há uma escassez global de profissionais de cibersegurança capacitados. Esse problema não é novo, mas, com base no número de especialistas que são treinados a cada ano, não vai acabar logo.

Nessas circunstâncias, é um desafio manter seus especialistas em segurança satisfeitos e focados, ou simplesmente mantê-los. O esgotamento é um grande problema, especialmente a sua equipe altamente qualificada e que passou por treinamentos caros passa todo o tempo arrastando-se por tarefas triviais.

Além disso, claro, há a questão dos recursos financeiros. E de capacidade dos processadores. E tudo o mais que é necessário para otimizar sua segurança sem afetar a velocidade de processamento, a produtividade dos funcionários, a satisfação dos usuários ou os orçamentos.

A solução

Então quais são as respostas?

Proteção eficiente

Em primeiro lugar, tudo depende de uma **proteção de endpoints eficaz** e uma plataforma de proteção de endpoints (EPP) sólida. Simples assim. Evitar as ameaças no nível dos endpoints, antes que elas possam disparar alertas, reduz a pressão sobre os recursos, atenua o risco de sucesso de um ataque e ajuda a manter a empresa funcionando consistentemente e em segurança. Isso aplica-se a ataques a commodities, que absorvem a maior parte do tempo, e a ataques mais complexos e até direcionados, que têm mais probabilidade de ser bem-sucedidos e causar mais danos.

A abordagem que recomendamos é uma combinação de **defesas de endpoints multicamadas** – uma forte proteção de linha de base contra ameaças a commodities e defesas multifacetadas em camadas contra as ameaças mais recentes e complexas.

Também é importante lembrar que algumas ameaças são criadas especificamente para esquivar-se de EPPs. Para elas, devem ser usados métodos de detecção diferentes, como a **Sandbox automatizada**.

O **EDR (Endpoint Detection and Response)** fornece a próxima camada de segurança fundamental. O EPP fornece a identificação e proteção inicial, enquanto o EDR proporciona visibilidade e opções de análises mais detalhadas, permitindo que você veja como o ataque foi iniciado e em que estágio se encontra no momento. Além da detecção, o EDR também oferece múltiplas opções de resposta, de modo que seja possível conter a ameaça apresentada de modo rápido e eficiente.

O EDR só é eficaz quando associado com uma base de proteção sólida. Quanto mais incidentes a solução de EPP é capaz de evitar no início, menos a solução de EDR precisa fazer, e você fica com mais recursos para focar nos poucos incidentes que restam.

Cuidando do comportamento humano

Da perspectiva do usuário, uma das melhores maneiras de evitar a falha humana, claro, é eliminar as oportunidades e a tentação por meio de **controles de aplicativos, da Web e de dispositivos**. Controles eficazes, longe de serem uma restrição para os negócios, podem realmente incrementar a produtividade, impedindo o desperdício de tempo e também, por exemplo, mídias sociais e sites de entretenimento possivelmente perigosos.

Mas, nessa questão, a educação dos usuário é realmente fundamental. O **treinamento de conscientização sobre cibersegurança** certo pode ter um efeito profundo sobre o comportamento dos funcionários, alterando a cultura corporativa, reduzindo significativamente o risco corporativo e reduzindo drasticamente a carga de trabalho do departamento de TI.

O retorno do investimento

Por fim, qualquer abordagem precisa se justificar financeiramente em termos de retorno do investimento e para funcionar agora e no futuro em ambientes com recursos finitos, o que pode incluir o conhecimento limitado dos especialistas em segurança.

Automação e agilidade

Considerando o volume crescente de ameaças e a falta de especialistas em segurança disponíveis para trabalhar com elas, quando possível, a **automação das tarefas de segurança** é fundamental. Ela deixa seus especialistas em segurança disponíveis para investir seu valioso tempo e suas habilidades em incidentes que realmente precisam da intervenção e do conhecimento humanos (além de mantê-los mais satisfeitos e motivados).

A automação de tarefas também elimina o risco de falha humana, a priorização e implementação automática de patches de vulnerabilidades dos sistemas, por exemplo, é muito mais eficaz do que depender de operadores humanos terem tempo para realizar essa atividade crítica, mas enfadonha.

A **implementação direta** e um **console de gerenciamento** simples e centralizado também economizam tempo e recursos. A troca de consoles para cada operação e a procura de comandos, além de demorar e ser frustrantes, também introduzem oportunidades de erros administrativos e omissão.

Sobre a proteção em vários níveis

Nós colocamos que qualquer solução que visa a proteção contra todas as formas de ameaças cibernéticas, inclusive ataques avançados e direcionados, precisa ter várias camadas.

Primeiramente, a solução precisa oferecer **proteção de endpoints básica robusta**, inclusive controles de endpoints (com funcionalidades de bloqueio e restrição da Web, de aplicativos e de dispositivos) e um mecanismo antimalware reforçado. Também é preferível ter recursos automatizados de avaliação de vulnerabilidades e gerenciamento de patches funcionando para economizar o tempo e o esforço do pessoal de TI na realização de tarefas de rotina.

Porém, o malware avançada estabelece outros desafios, que exigem mais camadas de segurança. O malware pode ser criado especificamente para burlar até os mecanismos de detecção nos endpoints mais sofisticados, ficando ocultos e inativos até que surja a oportunidade certa de execução. A resposta, nesse caso, é fazer com que o malware se apresente e seja ativado em um ambiente seguro controlado. Esse é o papel da **Sandbox**; preferivelmente, do tipo capaz não apenas de detectar, mas também de reagir a ameaças de maneira extremamente automatizada.

A detecção de comportamentos complexos nos endpoints também faz parte do foco do **EDR**. Da mesma forma que o EPP, em condições ideais, o EDR deve associar a automação com as ferramentas e a visibilidade para respaldar a intervenção humana, quando necessário. O agente de segurança deve ser capaz de analisar a causa básica de incidentes e responder a ameaças rapidamente, seja manualmente ou usando opções de resposta automatizada.

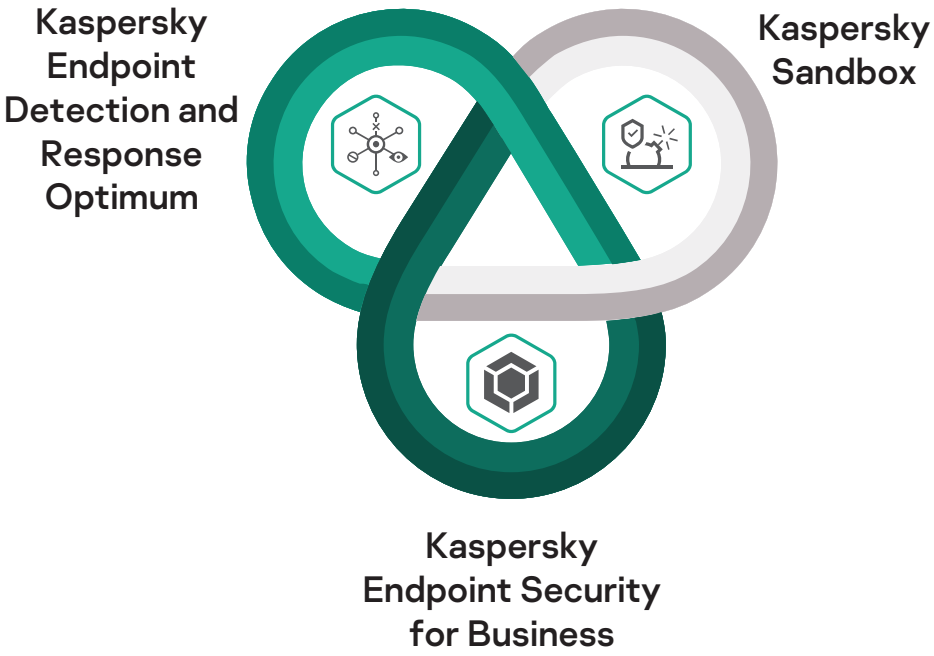
A reunião das tecnologias de EPP, Sandbox e EDR permite o combate rápido e eficiente de malware de commodities, limita as oportunidades de falha humana e reduz o risco de ataques avançados ou direcionados bem-sucedidos por meio da detecção e reação até a ameaças novas, desconhecidas e de "dia zero".

E, com uma solução integrada para tudo, não há lacunas entre as diferentes ferramentas que poderiam ser exploradas por hackers e atacantes.

Solução da Kaspersky

Todos os problemas mencionados acima são resolvidos de maneira ideal pela solução integrada de segurança de endpoints da Kaspersky, uma solução extremamente automatizada que consistem em proteção e controles integrados de endpoints, uma Sandbox automatizada e EDR. Os três componentes trabalham em conjunto a partir da base de um EPP forte. Vamos examinar cada componente de maneira mais detalhada, pois eles oferecem muito mais do que a resolução dos problemas descritos acima.

Forte proteção de endpoints básica



O Kaspersky Endpoint Security for Business é conhecido por fornecer um EPP excepcionalmente eficiente (que inclui proteção contra ataques de ransomware e sem arquivo) que utiliza o mecanismo antimalware mais testado e mais premiado do mercado.

As camadas de proteção de endpoints fornecidas pelo Kaspersky Endpoint Security for Business incluem:

- Nosso premiado mecanismo antimalware, aprimorado com Machine Learning
- Detecção de ransomware
- Detecção de comportamento com reversão automática — que identifica e bloqueia ameaças avançadas, inclusive malware sem arquivo e tomada de controle de contas de administrador, além de reverter todas as alterações já feitas.
- Prevenção de exploits
- Defesa contra ameaças em dispositivos móveis e integração de EMM
- Prevenção de invasões baseada em host (HIPS)
- Firewall e gerenciamento do firewall do sistema operacional
- Inteligência de ameaças automatizada (Kaspersky Security Network)
- Criptografia — incluindo gerenciamento da criptografia incorporada no sistema operacional
- Consultor de Políticas de Segurança — monitoramento de modificações das configurações de segurança otimizadas
- Avaliação de vulnerabilidades e gerenciamento de patches
- Instalação de sistemas operacionais e software de terceiros
- Integração de sistemas de SIEM

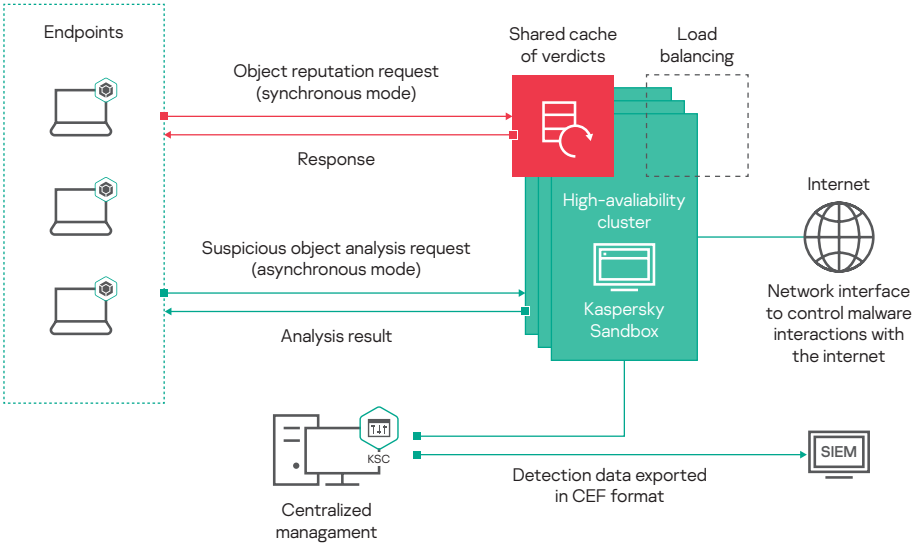
O fortalecimento do sistema e a redução de falha humana são fornecidos por controles como:

- Controle de Aplicativos com listas de permissão baseadas em categorias
- Controle Adaptativo de Anomalias, que monitora e bloqueia ações suspeitas que não são típicas de computadores em uma rede corporativa
- Controle de Dispositivos – controla e bloqueia a conexão de dispositivos externos
- Controle da Web – bloqueia ou restringe o acesso a sites possivelmente perigosos, que desperdiçam tempo ou inadequados

Para obter mais informações sobre o Kaspersky Endpoint Security for Business, acesse o nosso site.

Sandbox automatizada

A Kaspersky Sandbox detecta e responde automaticamente a ameaças projetadas para burlar a proteção de endpoints, sem necessidade de intervenção humana.



Fluxo de trabalho da Kaspersky Sandbox

Os objetos verificados são executados pelos servidores da sandbox em cluster em uma máquina virtual isolada que simula uma estação de trabalho. O componente recebe uma solicitação de análise do arquivo do agente do Kaspersky Endpoint Security for Business instalado no computador do usuário final, e o objeto entra na fila em um dos servidores em cluster. Quando o arquivo é enviado para processamento, a Kaspersky Sandbox o executa e registra todas as ações que ele realiza. O componente analisa os dados obtidos de atividades maliciosas e suspeitas e retorna o veredito para o agente do Kaspersky Endpoint Security for Business que solicitou a verificação. O veredito também é enviado para o cache operacional, permitindo que outros hosts recuperem rapidamente informações sobre o objeto verificado sem precisar analisá-lo novamente. Isso reduz a carga sobre os servidores da Kaspersky Sandbox e melhora o tempo de resposta a ameaças.

Depois da detecção do arquivo como malicioso, seu Indicador de comprometimento (IOC) pode ser usado para executar uma tarefa de neutralização remota pelo mecanismo do Kaspersky Endpoint Security for Business a fim de excluir o arquivo de todas as outras máquinas da rede.

As técnicas usadas pela Kaspersky Sandbox incluem:

- Monitoramento da interação com recursos da Internet
- Carregamento de módulos
- Modos de verificação síncrona e assíncrona
- Técnicas de reação à evasão
- Aplicação de diferentes modos de simulação
- Modelagem de ações do usuário
- Geração automática de IoCs e verificação da infraestrutura
- Prevenção automática

Para obter mais informações sobre a Kaspersky Sandbox, acesse o nosso site.

EDR otimizado

O Kaspersky Endpoint Detection and Response Optimum complementa o Kaspersky Endpoint Security for Business, proporcionando visibilidade total e a possibilidade de analisar causas básicas para entender completamente o status das defesas corporativas contra ameaças avançadas.

Os especialistas em segurança de TI recebem as informações e os insights necessários para uma investigação efetiva e uma resposta rápida e precisa a incidentes antes que ocorra qualquer dano.

Sendo parte de nossa solução integrada de segurança de endpoints, o Kaspersky Endpoint Detection and Response Optimum possibilita a análise de causas básicas usando:

- Visualização do caminho de disseminação do ataque, mostrando como a ameaça se desenvolveu no endpoint
- Informações sobre o arquivo, inclusive metadados, origem do arquivo, dados de modificações, assinatura digital, etc.
- Informações sobre o host e o usuário
- Informações sobre a detecção
- Injeção do processo
- "Drops" de arquivos
- Modificações de chaves do Registro
- Conexões

Depois de detectar uma ameaça, ficam disponíveis várias opções de resposta automatizadas e com um único clique, como:

- Isolar o host
- Executar a verificação do host
- Remover o arquivo (quarentena)
- Encerrar o processo
- Impedir a execução do processo

Para aprofundar a investigação, estão disponíveis funcionalidades como a importação de IoCs ou sua geração com base nas detecções e a verificação desses IoCs com opções predefinidas de resposta automatizada.

Para obter mais informações sobre o Kaspersky Endpoint Detection and Response Optimum, visite o nosso site.

O Kaspersky Endpoint Detection and Response Optimum está disponível no local e na nuvem*.

Segundo um estudo da Forrester, para as empresas entrevistadas, um dos principais requisitos é que a solução de segurança seja implementada com pouca ou nenhuma interrupção para os usuários. Esse princípio está no cerne da segurança integrada de endpoints

Gerenciamento e administração

Todos os componentes de nossa solução são desenvolvidos internamente e administrados no mesmo console, e utilizam o mesmo agente de endpoint multifuncional. Assim, o gerenciamento diário é centralizado, direto e eficiente.

Conscientização sobre segurança

- **52%** das empresas consideram seus funcionários como a maior ameaça à cibersegurança corporativa[6]
- **60%** dos funcionários têm dados confidenciais em seus dispositivos corporativos (dados financeiros, bancos de dados de e-mails, etc.)
- **30%** dos funcionários admitem que compartilham os dados de login e senha de seus computadores de trabalho com colegas[8]

Também oferecemos produtos de treinamento no computador que associam o conhecimento da cibersegurança com as mais conhecidas tecnologias e práticas educacionais. Essa abordagem muda o comportamento dos usuários e ajuda a criar um ambiente cibernético seguro em toda a organização.

O Kaspersky Security Awareness desenvolve uma cultura de comportamento seguro:

- educando os usuários sobre quando alertar os administradores sobre sinais de uma possível ameaça genuína
- reduzindo os erros de usuários decorrentes de ignorância ou ingenuidade
- diminuindo o número de alertas de alertas de segurança que os administradores precisam priorizar

Você pode seguir o progresso dos alunos pelo painel amigável, que apresenta o rastreamento de dados, tendências e previsões dinâmicos, juntamente com recomendações para incrementar seus resultados.

Para obter mais informações sobre o Kaspersky Security Awareness, acesse o nosso site.

6 O custo de uma violação de dados, Kaspersky, 2018

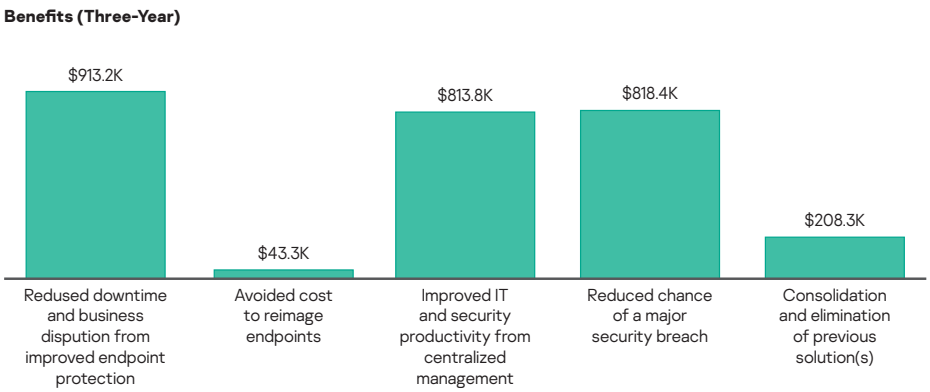
* Há algumas restrições em relação à série de recursos e funcionalidades que podem ser gerenciados pelo console na nuvem. Para obter todas as informações, consulte a ajuda on-line.

Seu retorno do investimento

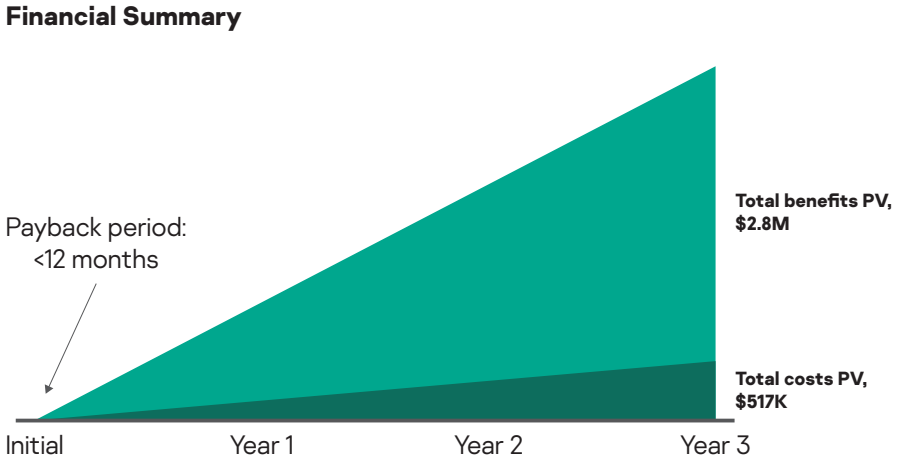
Como com qualquer solução, o custo é tão importante quanto os benefícios que fornecemos. Segue um exemplo de retorno do investimento das soluções Kaspersky, com base em um estudo da Forrester[7] sobre uma solução de segurança da Kaspersky desenvolvida com base no Kaspersky Endpoint Security for Business e no Kaspersky Endpoint Detection and Response.

Benefícios quantificados de valor atual (PV) com ajuste de risco obtidos pelas empresas entrevistadas no estudo da Forrester:

- **Quase US$ 1,0 milhão:** impacto na receita do aumento do tempo de atividade no endpoint por conta do menor número de interrupções.
- **Mais de US$ 40.000:** menos incidentes relacionados à segurança aumentaram a produtividade da TI reduzindo a necessidade de recriar os endpoints.
- **Mais de US$ 800.000:** o gerenciamento facilitado de várias soluções de segurança por meio do console de gerenciamento centralizado promoveu economias em produtividade.
- **Mais de US$ 800.000:** uma grande melhoria da conduta geral em relação à segurança reduziu a chance de uma violação de segurança "importante".
- **Mais de US$ 200.000:** economia de custo associada à mudança para a Kaspersky.



As entrevistas com clientes existentes e a análise financeira subsequente da Forrester mostraram que as organizações entrevistadas teriam benefícios da ordem de US$ 2,8 milhões ao longo de três anos, com custos de mais de US$ 500.000, resultando em um valor líquido atual (NPV) de US$ 2,3 milhões e um retorno do investimento de 441%.



7 The Total Economic Impact™ Of Kaspersky Security Solutions, estudo comissionado realizado pela Forrester Consulting, janeiro de 2020

8 Organizando a desordem digital, Kaspersky, 2019

Em resumo

A proteção de endpoints é fundamental para manter sua organização segura no cenário de ameaças atual. E a melhor maneira de proteger seus endpoints é uma solução em várias camadas, que utiliza técnicas diferentes para detectar e reagir a ameaças de modo altamente automatizado e, ao mesmo tempo, possibilita a intervenção humana para tarefas mais complicadas e decisões importantes.

A solução integrada de segurança de endpoints da Kaspersky foi projetada especificamente para cuidar da proteção das organizações contra ameaças a commodities, ameaças avançadas e complexas e falha humana:

- implementando uma estratégia **de proteção, detecção e resposta integradas em vários níveis**
- **automatizando** suas defesas, reduzindo o tempo e o trabalho necessários para reagira até a ataques direcionados e avançados
- alcançando as **maiores taxas de detecção**
- alimentando uma **cultura de cibersegurança por meio de controles e conscientização sobre segurança**
- garantindo um **retorno do investimento significativo**

Com tudo isso, você pode aproveitar os mais altos níveis de segurança contra as ameaças cibernéticas mais complexas sem comprometer recursos valiosos.

Para obter mais informações sobre como a segurança integrada de endpoints pode ajudar a proteger a sua organização de ataques complexos sem pressionar seus recursos, visite o nosso site.

www.kaspersky.com