kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

O problema

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

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 desapercebidas 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 atora 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.

"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]

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 nuvem[3].

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

Casos de uso essenciais de EDR

Responda a perguntas importantes

- Qual é a 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 e 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.

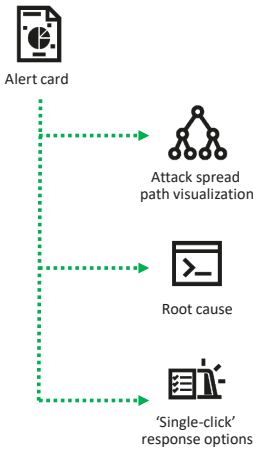
Incremente suas defesas

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.

Analise 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

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.