

Malwarebytes Endpoint Protection & Response

Nós não alertamos apenas, nós consertamos

A realidade no panorama de ameaças atual é que nenhum fabricante oferece total proteção: br.malwarebytes.com/remediationmap.

Violações são inevitáveis. Correção é essencial.

As organizações de hoje buscam maneiras de abordar incidentes que não foram devidamente trabalhados pelas defesas existentes. Quando os atacantes desviam das defesas, geralmente, ficam imperceptíveis por semanas ou meses. Em 2007, um estudo realizado pelo Ponemon Institute concluiu que o tempo médio para identificar (MTTI) uma violação era de 191 dias.

Os recursos de Endpoint Detection and Response (EDR) visam agilizar a detecção da ameaça e reduzir o tempo de espera. Quanto mais rápido uma violação de dados for detectada e bloqueada, menor será o prejuízo. As soluções EDR atuais identificam uma ameaça que desviou a proteção tradicional e uma resposta é gerada geralmente em forma de registros, alertas e e-mails. Um analista de ameaças usa ferramentas para avaliar o código e a imagem das máquinas infectadas é refeita.

O Malwarebytes Endpoint Protection and Response tem uma abordagem diferente. Ao usar as correções proprietárias Linking Engine e Ransomware Rollback, o Malwarebytes vai além de alertar e refazer a imagem para reparar o dano. Com o Endpoint Protection and Response, você não precisa negociar entre custo e complexidade.

RECURSOS TÉCNICOS

Proteção Web

Previne o acesso a websites maliciosos, redes de publicidade, redes scammer e áreas perigosas

Proteção de aplicativos

Reduz vulnerabilidade a exploits e detecta proativamente as tentativas de rastreamento feitas por ataques avançados

Mitigação de exploit

Detecta e bloqueia proativamente tentativas de abuso das vulnerabilidades e executar códigos remotamente no endpoint

Proteção por comportamento de aplicativos

Impede que as aplicações sejam influenciadas a facilitar a infecção dos endpoints

Deteção de anomalias por Machine Learning

Identifica malwares e vírus proativamente usando tecnologia de machine learning

Análise de payload

Identifica famílias completas de malware conhecidos e relevantes por meio de regras heurísticas e comportamentais

Mitigação de ransomware

Detecta e bloqueia ransomware através da tecnologia de monitoramento comportamental

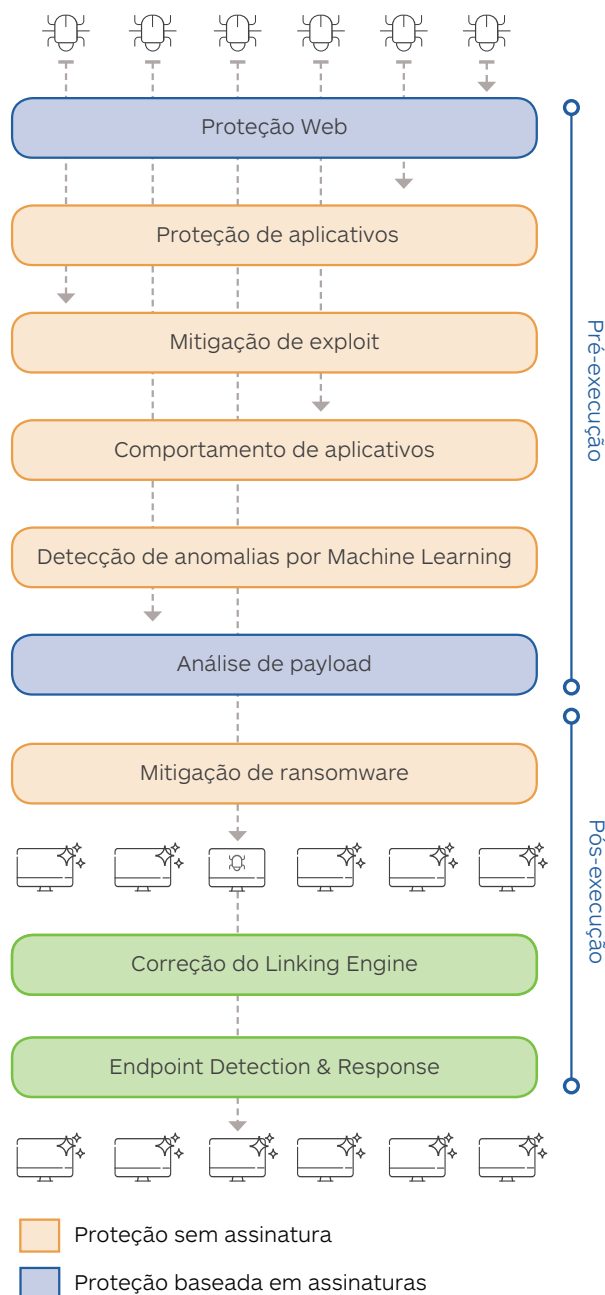
Linking Engine e correção

Fornecer uma correção completa e detalhada para retornar o endpoint para um estado realmente saudável, minimizando o impacto para o usuário final

Endpoint Detection and Response (EDR)

Visibilidade de endpoints para análise e investigação contínuas do comportamento. Reduz o tempo de permanência de ameaças de dia zero. Oferece opções de resposta além de alertas

ENDPOINT PROTECTION & RESPONSE



Principais benefícios

Proteção multicamada

A proteção multivetorial (MVP) da Malwarebytes usa uma abordagem em sete camadas, incluindo técnicas de detecção estática e dinâmica para proteção em todas as etapas do ataque. Esta abordagem fornece proteção contra todos os tipos de ameaças, de vírus tradicionais às ameaças avançadas de amanhã.

Visibilidade em endpoints para monitoração contínua

O Flight Recorder fornece monitoração e visibilidade contínuas em computadores Windows para descobertas rápidas. Você pode rastrear facilmente a atividade do sistema de arquivos, a atividade da rede, a atividade do processo e a atividade dos registros. Os eventos do Flight Recorder são armazenados localmente e na nuvem.

Três maneiras de isolamento do endpoint

Quando um endpoint está comprometido, o Malwarebytes interrompe o ataque ao isolar o endpoint. A rápida correção evita movimentos laterais. O malware é impedido de se comunicar e os ataques remotos são bloqueados. O Endpoint Protection and Response é o primeiro produto a oferecer três maneiras de isolar um endpoint. Isolamento da rede para restringir quais processos podem se comunicar. Isolamento do processo para restringir quais processos podem ser executados. Isolamento do computador para alertar o usuário final e impedir interação. Mantém o sistema online de forma segura para análise detalhada.

Remediação completa e minuciosa

Malwarebytes oferece a correção mais confiável da indústria como mostram os 500.000 downloads e correção de 3 milhões de infecções por dia em todo o mundo. Malwarebytes Endpoint Protection utiliza a tecnologia Linking Engine para remover todos os traços de infecções e artefatos relacionados - não apenas os vinculados ao payload da ameaça primária. Essa abordagem economiza o tempo gasto apagando e refazendo a imagem dos endpoints.

Ransomware Rollback

A tecnologia Ransomware Rollback permite que você retorne o relógio para anular o impacto do ransomware ao usar os backups just-in-time.

O Malwarebytes registra e associa as mudanças com processos específicos. Todas as alterações feitas por um processo são gravadas. Se um processo faz "coisas ruins", você podem bloquear facilmente as alterações para restaurar os arquivos que foram criptografados, excluídos ou modificados. O armazenamento dos dados é reduzido ao usar a tecnologia de exclusão dinâmica que memorizam o que os aplicativos "bons" fazem.

Gestão centralizada baseada em nuvem

Reduz a complexidade ao facilitar a implementação e o gerenciamento, independente da quantidade de endpoints. Além disso, elimina a necessidade de adquirir e manter equipamentos no local.



br.malwarebytes.com/business



corporate-sales@malwarebytes.com



+55.11.4280.6661

A Malwarebytes é a empresa de segurança cibernética em que milhões de pessoas em todo o mundo confiam. A Malwarebytes oferece proteção para pessoas e empresas contra ameaças maliciosas, incluindo ransomwares, que um software tradicional de antivírus pode não detectar. O principal produto da empresa usa tecnologia sem assinatura para detectar e barrar um ciberataque antes que danos ocorram. Saiba mais em br.malwarebytes.com.