Malwarebytes

FICHA DE DADOS

Malwarebytes Breach Remediation

Remoção avançada de ameaças

CARACTERÍSTICAS TÉCNICAS

- Remediação avançada de malware com verificação anti-rootkit
- Mecanismo de análise inteligente baseada -em heurística e em definições
- Descoberta e remediação remota automatizada de malware
- Vista de calendário dos eventos forenses
- Indicadores de ameaça OpenIOC personalizados (formato XML)
- Quatro tipos de verificação do sistema (Full (Completo), Threat (Ameaça), Hyper (Hiper), Path (Caminho))
- Modos "verificar e remediar" ou "verificar apenas" opcionais
- Gestão da colocação em quarentena de ameaças detetadas
- Registo de eventos numa localização centralizada (formato CEF)
- Nenhuma pegada duradoura no terminal
- Mecanismo de análise Mac malware e adware dedicado
- Plataforma ampliável suporta opções de implementação flexíveis

O pessoal de resposta a incidentes de hoje m dia é prejudicado pelos tradicionais sistemas de deteção de violação de segurança que produzem milhares de alertas por dia, mas não conseguem remover completamente o malware para evitar que esses se repitam ou se espalhem lateralmente. Esta abordagem reativa exige esforços de investigação manuais para encontrar a violação de segurança relevante, permitindo que ataques maliciosos vagueiem sem ser detetados durante, em média, 205 a 229 dias*. Uma vez o malware descoberto num laptop ou servidor, um administrador de TI pode demorar seis horas a recriar a imagem de todas as máquinas comprometidas.

O Malwarebytes Breach Remediation é uma plataforma avançada de deteção e remediação de próxima geração para pequenas e grandes empresas. Com o Malwarebytes Breach Remediation, as empresas podem procurar de forma proativa malwares para resolverem incidentes remotamente, em vez de irem fisicamente a cada computador infetado para remediar ou recriar a imagem da máquina. É uma plataforma autossuficiente que se integra facilmente com as ferramentas de gestão e segurança da empresa existentes. O Malwarebytes Remediation Breach fornece a capacidade única de detetar e remediar malware—reduzindo consideravelmente o risco de ameaças persistentes, em simultâneo.

Principais benefícios

Remedeia malware de forma exaustiva

Remove todos os vestígios de infeções e artefatos relacionados, não apenas o payload ou infetante principal. Elimina o risco de novos ataques ou movimentos laterais que se aproveitam de vestígios de malware sobejantes. Malwarebytes é o líder da indústria na remediação de malware – tem a confiança de milhões e é provado pela AV-Test.org.

Reduz drasticamente a inatividade

Permite-lhe direcionar esforços para projetos mais importantes, em vez de gastar um número infinito de horas na resolução manual de incidentes relacionados com malware e a recriar a imagem do hardware de uma ponta à outra da sua empresa.

Funciona proativamente, não reativamente

**Apresentação na "Gartner Security & Risk Management Summit", Defending Endpoints From Persistent Attack, Peter Firstbrook, 8 a 11 de junho de 2015.*

Ponemon Institute, 2016 Cost of Data Breach Study, junho de 2016

Implementa remediação automática que deteta proativamente e resolve simultaneamente incidentes. É como instalar um sistema de aspersão para parar pequenos incêndios antes que eles fujam de controlo. Transforma-o no herói, permitindo-lhe resolver o problema em vez de reagir a milhares de alertas de segurança por dia.

Caça malware

Descobre malware e atividades maliciosas novas e não detetadas e corrige-as rapidamente. Utiliza as regras heurísticas comportamentais da Malwarebytes, para além dos indicadores de compromisso (IOCs) de repositórios e ferramentas de deteção de violação de segurança de terceiros.

Extrai eventos forenses

Rastreia eventos forenses utilizando a funcionalidade Forensic Timeliner de propriedade para que a sua equipa possa resolver falhas de segurança ou comportamentos inseguros do utilizador. Compila eventos do sistema antes e durante uma infeção e apresenta dados numa cronologia conveniente para uma vasta análise do vetor e da cadeia do ataque. Os eventos abrangidos incluem modificações de ficheiros e registros, execução de ficheiros e websites visitados.

Melhora os investimentos existentes

Integra-se facilmente com infraestruturas de segurança existentes, e ferramentas de gestão de eventos (por ex., Splunk, ArcSight, QRadar), sistemas de deteção de violação de segurança (por ex., Mandiant, Crowdstrike, Fidelis) e plataformas de gestão de terminais (por ex., Tanium, ForeScout, Microsoft SCCM). Pode desencadear implementação e remediação através da sua plataforma de gestão de terminais com base em alertas recebidos do seu SIEM, sendo os detalhes de resolução tidos automaticamente em conta pelo SIEM.

Fecha a falha de segurança da Apple

Remove adware e malware rapidamente dos terminais Mac. Limpa sistemas de SO X em menos de um minuto do início ao fim. Programas da linha de comando e GUI separados permitem a implementação flexível utilizando soluções de gestão Mac populares (p. ex., Ambiente de Trabalho Remoto Apple, Casper Suite, Munki). Permite a operação remota, automática utilizando shell ou comandos AppleScript. Os administradores do sistema e os responsáveis pelas respostas de incidentes podem recolher informações do sistema utilizando o comando Snapshot conveniente.

REQUISITOS DO SISTEMA

Consulte malwarebytes.com/business/breachremediation para especificações técnicas e requisitos do sistema completos.

Componentes incluídos:
Programa CLI Windows
Programa Forensic Timeliner Windows
Programa CLI Mac
Programa CLI Mac

Terminais
Sistemas Operativos Suportados:
Windows 10, 8.1, 8, 7, Vista, XP
Windows Server 2012, 2008, 2003
Mac SO X Mac (10.8 e mais recente)

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

O Malwarebytes protege os consumidores contra ameaças perigosas, tais como malware, ransomware e exploits não detetados pelas soluções antivírus tradicionais. O Malwarebytes Anti-Malware, o produto principal da empresa, tem um mecanismo de deteção heurística altamente avançada que removeu mais de cinco mil milhões de ameaças maliciosas de computadores por todo o mundo. Mais de 10.000 PMEs e negócios empresariais confiam no Malwarebytes para proteger os seus dados. Fundada em 2008, a empresa está sediada na Califórnia, com escritórios na Europa e uma equipa mundial de investigadores e especialistas.