Malwarebytes

FOLHA DE DADOS

Malwarebytes Breach Remediation

Remoção automatizada de ameaças

RECURSOS TÉCNICOS

- Correção avançada de malware com análise anti-rootkit
- Ferramenta de análise inteligente heurística e baseada em definições
- Descoberta e correção remota, automatizada, de malware
- Visualização dos eventos forenses em linha temporal
- Indicadores de ameaça OpenIOC customizados (Formato XML)
- Quatro tipos de análise do sistema (completo, ameaça, hiper, caminho)
- Modos opcionais de análise e correção ou somente análise
- Gerenciamento de quarentena das ameaças detectadas
- Registro de evento em um local central (Formato CEF)
- Não deixa volume no endpoint
- Ferramenta de análise de malware e adware específica para Mac
- Plataforma expansível suporta opções de implementação flexíveis

O pessoal de resposta a incidentes atualmente ficam limitados devido aos sistemas de detecção de violação tradicionais que produzem milhares de alertas por dia, mas não conseguem remover completamente o malware para evitar que se repitam ou se espalhem lateralmente. Esta abordagem reativa exige esforços de investigação manuais para encontrar a violação relevante, permitindo que os ataques maliciosos não permaneçam sem detecção por até 205 dias*. Assim que o malware for descoberto em um laptop ou servidor, um administrador de TI pode levar até seis horas de seu tempo para reconfigurar cada máquina comprometida.

O Malwarebytes Breach Remediation é uma plataforma automatizada de detecção e resposta nos endpoints (EDR) para pequenas e grandes empresas. Com Malwarebytes Breach Remediation, as organizações podem caçar os malwares de forma proativa para resolver incidentes remotamente, ao invés de ir fisicamente até cada computador infectado para corrigir ou reconfigurar a máquina. É uma plataforma auto-suficiente que se integra facilmente com ferramentas de segurança e gestão empresarial existentes. Malwarebytes Breach Remediation fornece a capacidade única de detectar e corrigir o malware simultaneamente - reduzindo consideravelmente o risco de ameaças persistentes.

Principais benefícios

Elimine completamente o malware

Remova todos os traços de infecções e artefatos relacionados, não apenas o conteúdo principal ou o que causou a infecção. Elimine o risco de novos ataques ou movimentos laterais que se aproveitam dos traços que ficaram do malware. Malwarebytes é a correção de malwares líder na indústria — que tem a confiança de milhões e comprovado pela AV-Test.org.

Reduza tempo de parada drasticamente

Permite direcionar os esforços para projetos mais importantes, evitando gastar horas solucionando incidentes relativos a malware e reconfigurando o hardware em toda a empresa.

**Gartner Security & Risk Management Summit Presentation, Defending Endpoints From Persistent Attack, Peter Firstbrook, 8-11 de junho de 2015*

Funciona de forma proativa e não reativa

Implanta a correção automatizada de detecção proativa, ao mesmo tempo em que resolve os incidentes. É como instalar um sistema de aspersão para solucionar pequenos incêndios antes que eles saiam do controle. Você tem o mérito ao conseguir resolver o problema em vez de reagir a milhares de alertas de segurança por dia.

Caça aos malware

Encontra atividades maliciosas e malwares novos e não-detectados, eliminando-os rapidamente. Usa regras e heurísticas comportamentais do Malwarebytes, além de indicadores de compromisso (IOCs) provenientes das ferramentas e repositórios de detecção de violação de terceiros.

Extrai eventos forenses

Monitora eventos forenses utilizando o recurso Forensic Timeliner de modo que sua equipe possa cuidar das lacunas de segurança ou comportamento inseguro por parte do usuário. Reúne eventos do sistema antes e durante uma infecção, apresentando dados em uma linha temporal para a análise compreensiva do vetor e da cadeia de ataques. Eventos abrangidos incluem modificações de registro e arquivos, execução de arquivos e websites visitados.

Melhora os investimentos existentes

Integra-se facilmente às ferramentas existentes de gestão de eventos e às informações de segurança (ex., Splunk, ArcSight, QRadar), aos sistemas de detecção de vulnerabilidade (ex. Lastline, Mandiant, Fidelis) e plataformas de gestão de endpoint (ex Tanium, ForeScout, Microsoft SCCM). É possível acionar a implementação e a correção através da plataforma de gestão de endpoint com base nos alertas recebidos de seu SIEM e alimentar automaticamente os detalhes da resolução no seu SIEM.

Fecha a lacuna de segurança da Apple

Remove rapidamente o malware e adware dos endpoints do Mac. Limpa os sistemas OS X em menos de um minuto do início ao fim. Os programas de linha de comando e GUI separados possibilitam a implantação flexível utilizando soluções de gestão Mac (ex. Apple Remote Desktop, Casper Suite, Munki). Permite a operação remota e automatizada utilizando comandos AppleScript ou shells. Os administradores do sistema e os entrevistados sobre os incidentes podem coletar informações do sistema utilizando comando Snapshot com conveniência.

REQUISITOS DO SISTEMA

Consulte malwarebytes.com/business/breachremediation para ver as especificações técnicas completas e os requisitos do sistema.

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

Endpoints
Sistemas operacionais compatíveis:
Windows 10, 8.1, 8, 7, Vista, XP
Windows Server 2012, 2008, 2003
Mac OS X (10.8 e mais recentes)

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

O Malwarebytes protege os clientes e as empresas contra as ameaças perigosas, tais como malware, ransomware e exploits que escapam à detecção através de soluções tradicionais de anti-vírus. O Malwarebytes Anti-Malware, principal produto da empresa, conta com um motor de detecção heurística altamente avançado que removeu mais de cinco bilhões de ameaças maliciosas de computadores em todo o mundo. Mais de 10.000 empresas de pequeno, médio e grande porte em todo o mundo confiam no Malwarebytes para proteger seus dados. Fundada em 2008, Malwarebytes está sediada na Califórnia e possui escritórios na Europa, além de empregar uma equipe global de pesquisadores e especialistas.