Malwarebytes

FOLHA DE DADOS

Malwarebytes Incident Response

Detecção e correção centralizada de ameaças

RECURSOS TÉCNICOS

Ferramenta Incident Response
Verificação de ameaças rápida, extremamente efetiva com opções sob demanda, agendada e automática

Múltiplos modos de verificação
Modos de verificação Hiper, Ameaça e Personalizado que não interrompem os usuários

Linking Engine
Tecnologia sem necessidade de assinatura que identifica e remove completamente as ameaças vinculadas à carga útil da ameaça primária

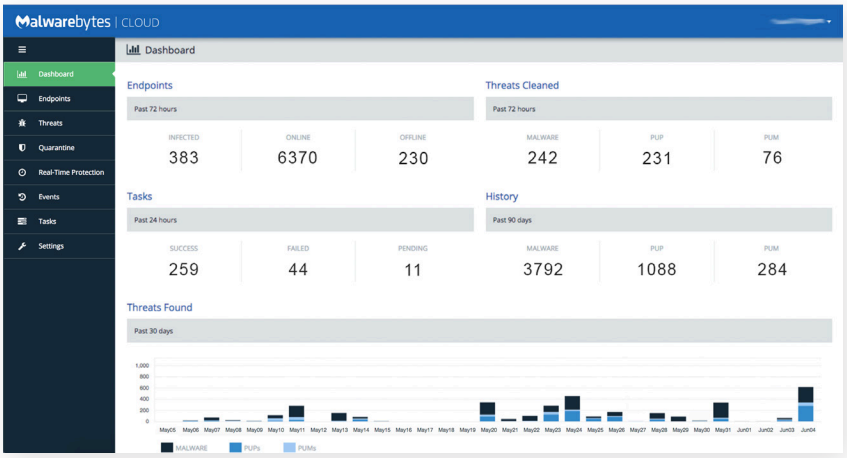
Plataforma de nuvem da Malwarebytes
O painel de gestão com base na nuvem oferece uma gestão da política de segurança de forma facilitada e centralizada, implantações e relatórios de ameaça

Gestão de ativos
Oferece detalhes úteis sobre o sistema endpoint, incluindo objetos de memória, software instalado, programas de inicialização, entre outros

Forensic Timeliner
Coleta e organiza os registros de eventos Windows em uma única visualização cronológica

Os invasores modernos estão cada vez mais sofisticados na forma com que escolhem seus alvos, obtêm informações sobre suas vítimas e executam seus ataques cibernéticos. Ameaças maliciosas continuam a penetrar nas defesas de rede e de endpoint, mesmo que as empresas, escolas e agências do governo invistam bilhões no fortalecimento de seus conjuntos de segurança. O tempo e o esforço necessários para responder a estes incidentes[1] são demorados, exigindo de 6 a 8 horas para remediar ou reimaginar um único endpoint. De acordo com uma pesquisa do Ponemon Institute, ataques maliciosos ou criminais levam em média 229 dias para serem identificados e 82 dias para serem contidos[2]. Os negócios precisam equipar suas equipes de segurança com a telemetria mais informada e com a melhor correção.

Malwarebytes Incident Response é uma ferramenta de detecção e correção de ameaças, construída em uma plataforma de gestão altamente expansível e com base na nuvem. Ela faz a verificação dos endpoints conectados em rede em busca de ameaças avançadas, incluindo malware, PUPs e adware, removendo-as completamente. Malwarebytes Incident Response melhora sua detecção de ameaça e o tempo necessário para responder a um ataque, com os benefícios adicionais de expansibilidade, flexibilidade e automação.



Painel de controle Malwarebytes com base na nuvem

Referências

[1] *A resposta a incidentes refere-se geralmente à ferramentas, processos e talentos que as organizações utilizam para abordar e mitigar um cyberataque identificado.*

[2] *Fonte: Ponemon Institute, 2016 Cost of Data Breach Study (Estudo sobre custo na violação de dados), junho de 2016.*

Principais benefícios

Automação

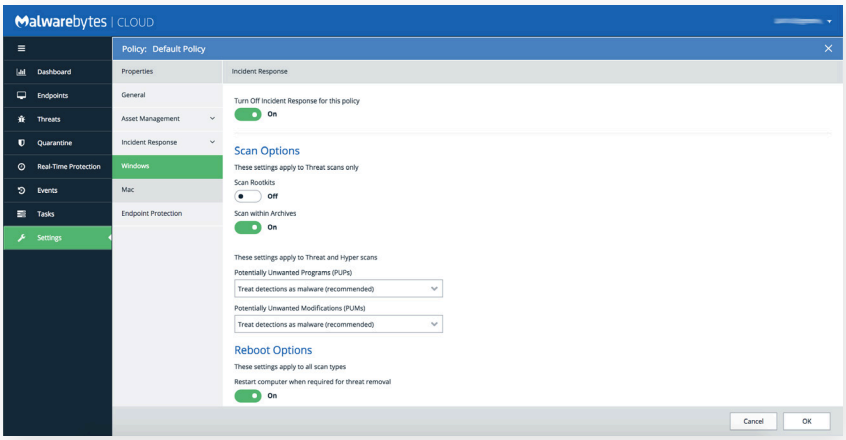
Faça a pré-implementação do Malwarebytes Incident Response em seus endpoints e conquiste a detecção e correção de ameaças avançadas imediatamente disponíveis ao toque de um botão. Ele é integrado à sua gestão de endpoint existente, SIEM e ferramentas de detecção de ameaças para responder automaticamente aos alertas de incidentes. As respostas automáticas às ameaças podem ajudar as empresas a acelerar seus fluxos de trabalho de resposta a incidentes ao mesmo tempo em que reduzem o tempo de duração do ataque.

Flexibilidade

Malwarebytes Incident Response usa agente persistente unificado, além de incluir opções de agente não persistente (Breach Remediation). Isto oferece opções de implantação flexíveis para diversos ambientes de TI de negócios. Malwarebytes se integra com facilidade em seu conjunto de segurança existente, ao mesmo tempo em que atende seu sistema operacional (Windows e Mac OS X), bem como os requisitos de infraestrutura.

Expansibilidade

Malwarebytes Incident Response é fornecida através de nossa nova plataforma de gestão de endpoint com base na nuvem da Malwarebytes. A plataforma de nuvem da Malwarebytes reduz a complexidade, facilitando a implantação e a gestão do Malwarebytes Incident Response e de outras soluções Malwarebytes, independentemente de haver um ou 1 milhão de endpoints. Este painel centralizado com base na nuvem elimina a necessidade de adquirir e manter equipamentos no local.



Configurações da política de segurança Malwarebytes Incident Response

REQUISITOS DE SISTEMA

Componentes inclusos

- Plataforma de nuvem da Malwarebytes
- Malwarebytes Incident Response (agentes persistente Windows e Mac OS X)
- Correção de violação (agentes não persistentes Windows CLI, Mac GUI, Mac CLI)
- Forensic Timeliner (Windows)
- Suporte por e-mail e telefone

Requisitos de hardware

Windows
CPU: 1 GHz
RAM: 1 GB (clientes); 2 GB (servidores)
Espaço em disco: 100 MB (programa + registros)
Conexão de internet ativa

Mac
Qualquer dispositivo Apple Mac compatível com Mac OS X (versão 10.10 ou mais recente)
Conexão de internet ativa

Sistemas operacionais suportados

Windows 10® (32 bits, 64 bits)
Windows 8.1® (32 bits, 64 bits)
Windows 8® (32 bits, 64 bits)
Windows 7® (32 bits, 64 bits)
Windows Vista® (32 bits, 64 bits)
Windows XP® com SP3 (somente 32 bits)
* Windows Server 2016® (32 bits, 64 bits)
* Windows Server 2012/2012R2® (32 bits, 64 bits)
* Windows Small Business Server 2011
* Windows Server 2008/2008R2® (32 bits, 64 bits)
* Windows Server 2003® (somente 32 bits)
Mac OS X (10.10 ou mais recentes)

Observe que servidores Windows que utilizem o processo de instalação Server Core são especificamente excluídos.

* *A integração do Windows Action Center não é compatível com os sistemas operacionais Windows Server.*

malwarebytes.com corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes é a nova geração de empresa de cyber-segurança na qual milhões de pessoas no mundo todo confiam. O Malwarebytes protege de forma proativa as pessoas e as empresas contra as ameaças perigosas, tais como malware, ransomware e exploits que escapam à detecção através de soluções tradicionais de antivírus. O principal produto da empresa combina detecção de ameaça heurística avançada com tecnologias signature-less para detectar e barrar um cyberataque antes que danos ocorram. Mais de 10.000 empresas em todo o mundo usam, confiam e recomendam Malwarebytes. Fundada em 2008, Malwarebytes está sediada na Califórnia e possui escritórios na Europa e na Ásia, além de empregar uma equipe global de pesquisadores de ameaças e especialistas em segurança.