

MALWAREBYTES ENDPOINT DETECTION AND RESPONSE FOR SERVERS

Proteção, detecção e resposta integradas.
Criado para ser simples e rápido.

Visão geral

Os servidores das empresas e os dados que albergam são a espinha dorsal das atividades empresariais modernas. Um ciberataque bem sucedido pode pôr um sistema crítico offline e levar a uma paralisação da produtividade. Como os servidores estão no centro de todas as atividades organizacionais, eles requerem uma segurança abrangente que os torne resistentes a qualquer ataque.

O Malwarebytes Endpoint Detection and Response for Servers é rápido, leve e concebido propositadamente para proteger os seus dados mais valiosos. Esta solução proporciona uma proteção integrada e proativa e uma remediação "one-and-done" focada em laser para manter a infraestrutura do seu servidor online e operacional. E a sua funcionalidade Ransomware Rollback reverte os servidores afetados para um estado realmente saudável, sem a dispendiosa recriação de imagem, perda de produtividade ou necessidade de pagar o resgate.



PRINCIPAIS

Visibilidade abrangente

Uma gestão centralizada em nuvem proporciona uma visibilidade abrangente da sua postura de segurança.

Eficiência

Permite a deteção e resposta contínuas a ameaças de segurança avançadas para uma eficiência operacional sem precedentes.

Vereditos precisos

Deteção integrada em toda a cadeia de ataques apresenta um veredito com precisão.

Necessidades de plataforma

De servidores a estações de trabalho, o Malwarebytes proporciona proteção avançada para as necessidades da sua plataforma organizacional.

PLATAFORMAS

Servidores Windows
Servidores Linux

Funcionalidades

Implementação rápida. Gestão simples.

O Malwarebytes foi concebido para ser rápido, desde a implementação, à gestão e à manutenção contínua. Organizações com poucos recursos de segurança obtêm rapidamente uma resposta ativa e uma postura de segurança forte.

Base em nuvem onde importa

Aproveitando o poder da plataforma em nuvem Malwarebytes Nebula, as capacidades de deteção e resposta nos terminais evoluem à velocidade da inovação dos ataques. E a nossa baixa pegada no servidor aproveita a nuvem para detetar com eficiência ameaças avançadas com base no comportamento.

Gestão concebida para terminais

A nossa solução permite-lhe gerir eficientemente a segurança do servidor à escala empresarial e, com apenas alguns cliques, obter uma ampla visibilidade desde o painel global até indicadores individuais de problemas (Indicators of Compromise - IOC) descobertos num servidor.

Amplie a sua proteção contra ameaças.

O Malwarebytes integra proteção com deteção, protegendo os seus servidores e proporcionando-lhe total visibilidade e controlo em toda a cadeia de ataques.

Proteção proativa integrada

A deteção e proteção contra ameaças automatizadas na web, memória, aplicação, ficheiros e periféricos de armazenamento USB aplica tecnologias de deteção adaptativas, incluindo monitorização de comportamentos e aprendizagem automática em nuvem.

Monitorização de atividade suspeita

Analisa continuamente processos dos terminais, registo, sistema de ficheiros e atividade da rede na nuvem, recorrendo a análise de comportamentos e aprendizagem automática para identificar atividade potencialmente suspeita.

Sandbox na nuvem

A análise profunda de ameaças desconhecidas é realizada em segurança na nuvem. Também testamos códigos maliciosos e maus comportamentos em todas as fases, incluindo investigação remota de códigos suspeitos sem perturbação da produtividade do utilizador final. Isto proporciona uma deteção altamente precisa através de informações sobre ameaças, apresentando IOC acionáveis.

Pesquisa por Flight Recorder

O Flight Recorder capta alterações nos ficheiros, processos, domínio de rede e endereço IP ao longo do tempo. Isto permite a deteção livre de ameaças para IOC específicos, como hashes MD5, nomes de ficheiros, domínios de rede e endereços IP.

Investigar, isolar e recuperar.

O Malwarebytes Endpoint Detection and Response for Servers dá aos profissionais da segurança a capacidade de rapidamente investigar, isolar, remediar meticulosamente e recuperar de ameaças numa questão de minutos.

Isolamento granular de ataques

Agora, é fácil impedir o malware de se propagar em caso de ataque a um servidor. O Malwarebytes Endpoint Detection and Response for Servers maximiza a capacidade de resposta de TI, partindo de três modos de isolamento de dispositivos:

1. O isolamento de rede limita as comunicações do dispositivo, pelo que os atacantes são bloqueados e o malware não consegue "ligar para casa". Além disso, o isolamento de rede limita o movimento lateral do malware.
2. O isolamento de processo restringe a capacidade de o malware gerar novos processos, limitando o seu impacto. Os utilizadores também sofrem restrições na capacidade de iniciar novas aplicações que possam dificultar um esforço de resposta.
3. O isolamento do servidor permite que os administradores bloqueiem a máquina enquanto a equipa da TI gere a triagem. Adicionalmente, o isolamento do servidor pode ser aproveitado para impedir ameaças internas.

Com múltiplos modos de isolamento do servidor, as equipas de segurança são capazes de tomar medidas concretas para responder a ameaças.

Remediação metódica

Como verdadeira solução "one-and-done", a remediação Malwarebytes mapeia o caminho correto para remover todo o malware de forma permanente. As abordagens tradicionais concentram-se apenas na remoção do executável ativo, ignorando as mudanças residuais que conduzem à reinfeção.

O Malwarebytes Linking Engine patentado localiza todos os artefactos, mudanças e alterações de processo, incluindo executáveis de memória, que outros ignoram.

Ransomware Rollback

A nossa tecnologia Ransomware Rollback funciona de modo sincronizado com a monitorização de atividades suspeitas para detetar comportamentos de ransomware. Se se detetarem comportamentos de ransomware, o Malwarebytes ativa o processo de cópia de segurança de ficheiros, encriptando e reposicionando dados para restauro posterior.

O processo de cópia de segurança de ficheiros limita as cópias de segurança a ficheiros encriptados "just-in-time". Com um clique, as equipas de resposta a incidentes conseguem reverter os danos por ransomware através da reversão dos ficheiros afetados para o seu estado anterior ao ataque num período de até 72 horas antes de ficarem comprometidos.

Vantagens

Proteção abrangente para os seus recursos mais valiosos

Obtenha uma proteção inovadora e avançada para os recursos mais valiosos da organização. Com a monitorização de atividades suspeitas, o isolamento granular de processos e a funcionalidade Ransomware Rollback desta solução, as organizações podem manter os seus sistemas em funcionamento, mesmo sob o mais letal ciberataque.

Leve segurança do servidor concebida para empresas de todas as dimensões

O Malwarebytes Endpoint Detection and Response for Servers apresenta o equilíbrio perfeito entre proteção e desempenho. Implemente rapidamente a proteção de terminais para os seus servidores, sem qualquer impacto na capacidade de processamento do sistema.

Visibilidade granular, a partir de uma consola central na nuvem

A nossa consola central na nuvem proporciona uma visibilidade abrangente da sua postura de segurança. Através de um painel de vidro com uma IU intuitiva, obtenha visibilidade sobre todas as atividades da sua organização, desde servidores a estações de trabalho.

Resumo

Os servidores das empresas estão continuamente sob ataque. Fornecendo serviços, aplicações e outros recursos que são essenciais para manter a sua empresa em atividade, os servidores requerem nada menos do que a melhor proteção.

Desde proteção a deteção e resposta, o Malwarebytes Endpoint Detection and Response for Servers protege os dados mais valiosos de uma organização. Concebido para organizações de todas as dimensões que valorizem a eficiência, o Malwarebytes Endpoint Detection and Response for Servers foi concebido de base integrando e comunicando em todo o funil de deteção (tudo a partir de um agente único e uma consola de gestão), para permitir que as organizações façam uma gestão excepcional da segurança dos servidores, de forma rápida, adequada e fácil.



www.minitelnext.com



next@minitel.pt



+351 21 381 09 00