

# Malwarebytes Incident Response

A solução de remediação mais fiável e completa do mundo

## PRINCIPAIS BENEFÍCIOS

- Oferece remediação automática, precisa e minuciosa
- Liga silos operacionais
- Reduz o tempo de permanência de malware
- Fecha a lacuna em termos de falta funcionários e falta de competências
- Reduz custos e a complexidade de gestão da resposta a incidentes

## PRÉMIOS



Empresa Mais Promissora dos Estados Unidos



Produto do Ano



Inovação de Segurança do Ano

O número e o tipo de eventos de segurança que a sua equipa de resposta a incidentes cibernéticos (CIRT) enfrenta aumenta continuamente, a par dos custos e da complexidade de gestão da remediação.

Mais de 60 por cento dos ataques demoram acima de nove horas a ser remediados nas organizações.<sup>1</sup> Agora, mais do que nunca, face aos recursos limitados e às constantes barragens de ameaças avançadas, as organizações têm de passar de processos de resposta a incidentes reativos para os automáticos.

O Malwarebytes Incident Response é a nossa solução de confiança para uma remediação profunda e minuciosa que otimiza a nossa eficiência e eficácia na resposta a incidentes. A nossa abordagem automática ajuda a fortificar o seu modelo de segurança e ligar silos operacionais.

## Principais funcionalidades

### Remediação automática

A nossa remediação automática permite que a sua equipa CIRT elimine esforços específicos, manuais para limpar e recuperar os dispositivos de utilizadores após a infeção por malware—e liberta tempo e recursos valiosos. As tarefas automáticas demoram menos tempo, são mais precisas e reduzem o tempo de permanência do malware.

### Remediação minuciosa

A maioria das soluções só remedeia componentes de malware ativos—não oferece uma remediação completa. O Malwarebytes Linking Engine recorre uma abordagem de propriedade que também deteta e remove artefactos dinâmicos e associados. E o nosso motor aplica a sequenciação associada para garantir que os mecanismos de persistência do malware são removidos de forma a que desinfeção seja permanente. A nossa metodologia de remediação avançada permite às organizações a identificação expedita e remoção minuciosa de malware.



## Telemetria mais bem informada

Os nossos conhecimentos especializados sobre ameaças na remediação significam que compreendemos “as coisas más”— os ataques executados com sucesso em dispositivos de empresas. Com a ajuda dos nossos sistemas de análise de dados de grande volume e análises de pesquisa especializadas, processamos mais de 3 milhões de remediações de terminais por dia. Esta telemetria valiosa relativamente a malware de dia zero torna a nossa tecnologia mais responsiva perante ameaças emergentes e ajuda-nos a antecipar o malware de amanhã.

## Caça proativa

É provável que já existam ameaças no nosso ambiente. Quando um terminal é infetado, frequentemente, os atacantes inciam um movimento lateral para infetar outros terminais. A Malwarebytes habilita o seus elementos de resposta a incidentes a executar verificações agendadas para caçar proativamente indicadores de compromisso (IOC) recentemente detetados. A nossa solução facilita a adoção de um processo de “assumir o compromisso” que melhora significativamente a sua postura perante a segurança.

## Implementação e prontidão de integração flexíveis

A Malwarebytes oferece opções flexíveis que pode implementar da forma que pretender: escolha entre o nosso agente de terminal persistente gerido em nuvem ou o nosso agente de terminal não persistente (Breach Remediation). E o agente não persistente facilita a integração com o seu SIEM e sistema de gestão de terminais existentes. A nossa solução consegue tomar medidas, em tempo real, relativamente aos IOC que o seu SIEM deteta na rede. O Malwarebytes consegue, por exemplo, conduzir uma resposta a incidentes baseada num alerta das suas soluções Splunk ou ForeScout.



## Recursos no website

Para mais informações sobre Malwarebytes Incident Response, acesse a: [malwarebytes.com/business/incidentresponse/](https://malwarebytes.com/business/incidentresponse/)

As mais recentes novidades: [blog.malwarebytes.com/](https://blog.malwarebytes.com/)

Solicitar versão de avaliação: [malwarebytes.com/business/licensing](https://malwarebytes.com/business/licensing)

## Referências

<sup>1</sup> *Understanding the Depth of the Global Ransomware Problem*, Osterman Research



Santa Clara, CA



malwarebytes.com



corporate-sales@malwarebytes.com



1.800.520.2796

A Malwarebytes é a empresa de cibersegurança de próxima geração em que milhões de pessoas em todo o mundo confiam. O Malwarebytes protege pessoas e empresas contra ameaças perigosas, tais como malware, ransomware e exploits não detetados pelas soluções antivírus tradicionais. O produto principal da empresa, combina detecção heurística avançada com tecnologias sem assinatura para detetar e impedir um ataque informático antes que ocorram danos. Mais de 10 000 empresas em todo o mundo utilizam, confiam e recomendam Malwarebytes. Fundada em 2008, a empresa está sediada na Califórnia, com escritórios na Europa e na Ásia e uma equipa mundial de investigadores de ameaças e especialistas em segurança.

Copyright © 2017, Malwarebytes. Todos os direitos reservados. Malwarebytes e o logótipo Malwarebytes são marcas registadas da Malwarebytes. As outras marcas podem ser reivindicadas como propriedade de terceiros. Todas as descrições e especificações presentes estão sujeitas a alterações sem aviso prévio e são fornecidas sem qualquer tipo de garantia.