RESUMO DA SOLUÇÃO

Malwarebytes | minitel NEXT

MALWAREBYTES ENDPOINT DETECTION AND RESPONSE

Deteção, isolamento e remediação de nível empresarial para Windows, Mac e Linux

VISÃO GERAL

Num recente relatório de investigação do Ponemon Institute, 68% dos inquiridos relataram um ou mais ataques nocivos aos terminais, que comprometeram informações valiosas ou a infraestrutura. Uma pesquisa semelhante demonstra que quase 60% dos terminais hospedam ameaças ocultas, incluindo perigosos trojans, rootkits e backdoors. Estas ameaças são sofisticadas e persistentes e, muitas vezes, escapam mesmo à melhor proteção de terminais; é por isso que mais de metade de todas as empresas reportam uma incapacidade de detetarem eficazmente e lidarem com ataques avançados.

Outra questão igualmente preocupante são as mudanças recentes nas exigências de conformidade que requerem uma proteção mais rigorosa de Informações de Identificação Pessoal (PII). As diretivas do New York Department of Financial Services (NYDFS) e a lei California Consumer Privacy Act (AB 375) são algumas das mais exigentes, mas quase todos os EUA têm, agora, diretivas mais exigentes. Se as empresas de segurança não conseguirem provar que os alertas de "falsos positivos" não constituem ameaças ou ataques positivos, as suas empresas podem ser multadas, forçadas a fazer anúncios públicos e processadas por Procuradores Gerais ou entidades privadas. A nível internacional, o novo Regulamento Geral sobre a Proteção de Dados (RGPD) e as regulamentações da Diretiva Serviços de Pagamento 2.0 (PSD2) também estão a gerar desafios.

Aquilo de que as organizações precisam é da capacidade de detetarem imediatamente ameaças conhecidas ou desconhecidas, responderem ativamente em tempo real e de as isolarem e investigarem meticulosamente. Se os dados se perderem ou ficarem reféns, as empresas têm de remediar, reverter e recuperar rápida e completamente.

DESAFIOS AO EDR

Os ataques duplicaram
Mais de 68% das empresas sofreram ataques recentes e, destes, 80% eram novas ameaças "dia zero".

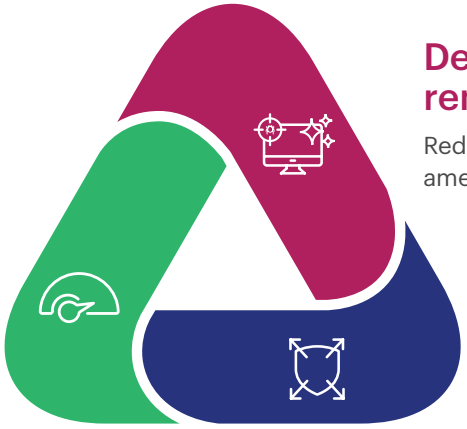
Muitos falsos positivos
Quase 60% das empresas necessitam de deteção dia zero, mas o elevado número de falsos positivos é uma preocupação acrescida.

Soluções complexas
Mais de 61% das empresas afirmam que a complexidade e a falta de recursos dificultam significativamente a EDR.

Fonte: 2020 EDR Study, Ponemon Institute

Implementação rápida e gestão simples

Implementação em alguns minutos e gestão com uma consola intuitiva na nuvem



Deteção, isolamento e remediação de ameaças

Redução de riscos e falsos positivos; fim das ameaças com múltiplos modos de isolamento

Deteção de ameaças e reversão de ransomware

Deteção orientada de ameaças e reversão de ransomware para Windows

FÁCIL

O Malwarebytes Endpoint Detection and Response (EDR) para Windows, Mac e Linux consegue substituir ou aumentar facilmente outras soluções de segurança de terminais, incluindo o Microsoft Defender. Conquistámos uma forte lealdade e apreço dos clientes, porque apresentamos soluções não-disruptivas, objetivas e económicas para implementar através de um agente terminal único e oferecemos integrações e compatibilidades robustas.

- Implementação não-disruptiva em minutos
- Um agente terminal, integração simples
- Consola de gestão intuitiva em nuvem

EFICAZ

O Malwarebytes EDR usa um sistema de aprendizagem automática de deteção de anomalias para detetar proativamente ataques baseados na web, malware dia zero, ransomware, programas potencialmente indesejáveis ou modificações (PPI e MPI), bem como infeções a partir de periféricos USB. O Malwarebytes EDR apresenta uma maior precisão, motivo pelo qual temos uma das mais baixas taxas de falsos positivos do setor. As nossas capacidades de isolamento granular previnem o movimento lateral de um ataque, permitindo-lhe conter máquinas, sub-redes ou grupos individuais e continuar atividades de resposta ativas.

- Deteta ameaças "dia zero" com poucos falsos positivos
- Isolamento granular para processos, redes e ambientes de trabalho Windows
- Remove executáveis, artefactos e mudanças

EFICIENTE

O Malwarebytes EDR oferece reversão de ransomware for Windows e, para evitar impactos no desempenho, utiliza um agente leve que apenas requer três processos em segundo plano, em comparação com outras soluções da sua magnitude.

- Agente leve único, sem impacto no desempenho
- Reversão de ransomware de 72 horas para Windows
- Custo total de propriedade reduzido

PROTEÇÃO PROATIVA DE TERMINAIS INTEGRADA

O Malwarebytes EDR inclui uma proteção de terminais integrada e tecnologias de deteção adaptativas automatizadas, com aprendizagem ao longo de cada fase do funil de deteção de ameaças. Ao contrário de soluções mais reativas, baseadas em assinatura, que permitem que o malware seja executado antes de atuarem, a nossa proteção de terminais encontra e bloqueia ameaças antes de os dispositivos serem infetados. O Malwarebytes EDR reconhece e evita, de forma proativa e precisa, tanto códigos hostis, como comportamentos suspeitos.

MODOS OPERACIONAIS DE ISOLAMENTO ESPECÍFICOS DO SISTEMA

O Malwarebytes EDR é a primeira solução a proporcionar múltiplos modos combinados de isolamento de terminais. Se um terminal for atacado, pode facilmente impedir que o malware se propague e cause danos, mitigando a TI e perturbando os utilizadores durante o ataque.

- O **isolamento de rede** limita as comunicações do dispositivo para garantir que os atacantes são bloqueados e o malware não consegue "ligar para casa".
- O **isolamento de processo** restringe as operações que podem ser executadas, parando o malware mas permitindo que os utilizadores se mantenham produtivos.
- O **isolamento de computador** para estações de trabalho Windows alerta os utilizadores sobre ameaças e bloqueia temporariamente o acesso, mas mantém o dispositivo online para fins de análise.

REMEDIAÇÃO AUTOMATIZADA E METICULOSA

A nossa abordagem automatizada permite aos analistas de TI e de segurança eliminar esforços manuais de remediar ataques, libertando o precioso tempo dos recursos. Infeções por malware típicas podem deixar para trás mais de 100 artefactos, incluindo ficheiros, pastas e chaves de registo, que podem propagar-se para outros sistemas na rede de uma organização. A maioria das soluções apenas remedeia componentes de malware ativos, como executáveis, o que expõe o sistema a reinfeções.

O Malwarebytes Linking Engine patenteado deteta e remove artefactos dinâmicos e relacionados, mudanças e alterações de processo. O nosso motor aplica a sequenciação associada para garantir uma desinfeção meticulosa de mecanismos de persistência de malware.

SANDBOX NA NUVEM

Para aumentar a precisão da nossa deteção de ameaças, o Malwarebytes utiliza uma "sandbox" na nuvem, uma prisão virtual para isolar e detonar malware potencialmente perigoso, para fins de avaliação e análise.

A sandbox permite-lhe investigar códigos suspeitos, mesmo remotamente, sem perturbar a produtividade do utilizador final. Após a análise, o Malwarebytes apresenta um relatório abrangente, para que possa responder adequadamente a incidentes (IOC).

DETEÇÃO ORIENTADA DE AMEAÇAS

Uma prática interface de visualização apresenta um painel Kanban de resumo que classifica automaticamente a combinação de ações no quadro MITRE ATT&CK, informando-o rapidamente sobre o "porquê" de o nosso algoritmo de aprendizagem automática ter identificado a atividade suspeita merecedora da sua atenção. Adicionalmente, oferecemos uma visão detalhada para o analista forense que requer a emissão dos passos detalhados com utilização de uma cadeia interligada de ações e comandos, para que seja possível fornecer-lhe os IOC necessários. Além disso, a interface de visualização pode arrancar na janela subordinada da nossa Flight Recorder Search (FRS) sem perder o seu lugar. A FRS é uma interface de utilizador orientada que o acompanha sistematicamente na pesquisa de trilhos/pistas (indicadores) em todos os terminais geridos na sua empresa, procurando sinais precoces de um ator de ameaça em movimento lateral.

REVERSÃO DE RANSOMWARE PARA WINDOWS

Para plataformas Windows, o Malwarebytes EDR inclui uma tecnologia única de reversão de ransomware de 72 horas que permite voltar atrás no tempo e fazer a sua empresa regressar rapidamente a um estado saudável. Se um ataque afetar ficheiros do utilizador, o Malwarebytes consegue facilmente reverter estas modificações e recuperar ficheiros que foram encriptados, eliminados ou modificados num ataque de ransomware. E não se preocupe: a nossa tecnologia de armazenamento de dados patenteada minimiza o espaço necessário para a cópia de segurança dos seus dados.

MONITORIZAÇÃO CONTÍNUA

A funcionalidade de pesquisa Flight Recorder no Malwarebytes EDR proporciona uma monitorização e visibilidade contínuas do seu Windows e Mac, para que obtenha uma perspetiva sólida. Estão incluídas capacidades de pesquisa de nomes de ficheiros, domínios de rede, endereços IP, hashes MD5 e caminhos ou nomes de ficheiros/processos. Também pode visualizar automaticamente atividades suspeitas, ver detalhes completos de linhas de comando de processos executados e armazenar trinta dias de dados agregados na nuvem.

GESTÃO DE VULNERABILIDADES E PATCHES

O nosso módulo Vulnerability Assessment liga-se perfeitamente e baseia-se nas ferramentas de visibilidade e prevenção que lhe são oferecidas pela nossa solução EDR, ajudando-o a apoiar as suas defesas a partir da mesma plataforma de segurança na nuvem. Utilizando um inventário atualizado do seu software, drivers e sistemas operativos (SO), o nosso módulo Vulnerability Assessment identifica vulnerabilidades de software conhecidas, áreas que atores de ameaças poderiam usar para obterem acesso à rede. Então, prioriza ações recomendadas com base no nível de risco que cada vulnerabilidade identificada representa. O Malwarebytes Patch Management assume o controlo do processo de aplicação de patches do software. Combinado com o nosso módulo Vulnerability Assessment, o módulo Patch Management acelera a identificação, implementação, instalação e verificação de revisões ao terminal Windows e aos SO do servidor, bem como uma vasta gama de aplicações de terceiros.

FILTRAGEM DE DNS

O módulo Malwarebytes Domain Name System (DNS) Filtering ajuda a evitar que tanto utilizadores no local como remotos acedam a conteúdos web impróprios ou websites nefastos, e ajuda-o a reforçar as políticas de Código de Conduta da sua organização. Além disso, o nosso módulo DNS Filtering encripta todos os pedidos de nome de domínio para ajudar a mitigar os meios pelos quais os atores de ameaças exploram websites e aplicações baseadas na web. Para reduzir ainda mais o risco, o nosso DNS Filtering é apoiado pela proteção em tempo real do Malwarebytes contra transferências maliciosas.

DETEÇÃO E RESPOSTA GERIDAS

O Malwarebytes também oferece Managed Detection and Response (MDR) para empresas de todas as dimensões com recursos limitados de cibersegurança. Com o Malwarebytes MDR, o seu ambiente está protegido pelo Malwarebytes EDR e a nossa equipa de profissionais de cibersegurança com décadas de experiência monitoriza o seu ambiente 24h/dia para investigar os alertas que o Malwarebytes EDR gera em tempo real. Adicionalmente, a nossa equipa Malwarebytes MDR remedeia ameaças e fornece um guia de remediação à sua equipa, libertando tempo para que as suas equipas de TI e segurança trabalhem noutros projetos mais prementes.

ELEVADO RETORNO SOBRE O INVESTIMENTO, BAIXO CUSTO TOTAL DE PROPRIEDADE

Com a nossa solução em nuvem, o Malwarebytes EDR adapta-se facilmente para satisfazer requisitos futuros. A nossa experiência em ciberinteligência na remediação fornece-lhe uma solução baseada em inteligência sobre ameaças de milhões de terminais com proteção Malwarebytes, tanto de empresas, como de consumidores. O Malwarebytes API simplifica a integração com os sistemas SIEM, SOAR, ITSM, etc., para impulsionar ainda mais a automação e a compatibilidade. O Malwarebytes EDR assegura um elevado retorno sobre o investimento e um baixo custo total de propriedade, e também somos conhecidos pela qualidade superior dos nossos serviços e assistência.

A SUA ESCOLHA MAIS SEGURA PARA EDR

O Malwarebytes Endpoint Detection and Response para plataformas Windows, Mac e Linux de nível empresarial deteta atividades suspeitas, isola ataques, investiga ameaças e remedeia danos, de forma eficaz e eficiente.

Outras soluções podem ser de difícil implementação e gestão e, normalmente, não são compatíveis com outro software de segurança, como o Microsoft Defender. A maioria das outras soluções EDR apenas removem os executáveis e não fornecem camadas múltiplas de isolamento para parar as ameaças antes que causem prejuízos. Também são concebidas para alertarem sobre quase todas as ameaças, motivo que as leva a emitir muitos alertas de falsos positivos.

O Malwarebytes EDR integra-se perfeitamente e é compatível com a maioria das restantes soluções de segurança de terminais, incluindo o Microsoft Defender. Somos fáceis de implementar e gerir através da nossa consola em nuvem Nebula, detetamos atividades suspeitas com eficiência e isolamos processos e redes para mitigar os danos. O isolamento de computador também está disponível para estações de trabalho Windows. O Malwarebytes Linking Engine patenteado remove artefactos, mudanças e alterações de processo, enquanto permite uma exclusiva reversão de ransomware de 72 horas para estações de trabalho Windows. O Malwarebytes EDR para Windows, Mac e Linux usa um agente leve único, sem impacto no desempenho.
Não espere até ser demasiado tarde. Malwarebytes é a sua escolha mais segura para EDR em Windows, Mac e Linux.
Conquistámos uma forte lealdade e apreço dos clientes por uma solução EDR empresarial que é simples, eficaz e eficiente.

www.minitelnext.com
next@minitel.pt
+351 21 381 09 00