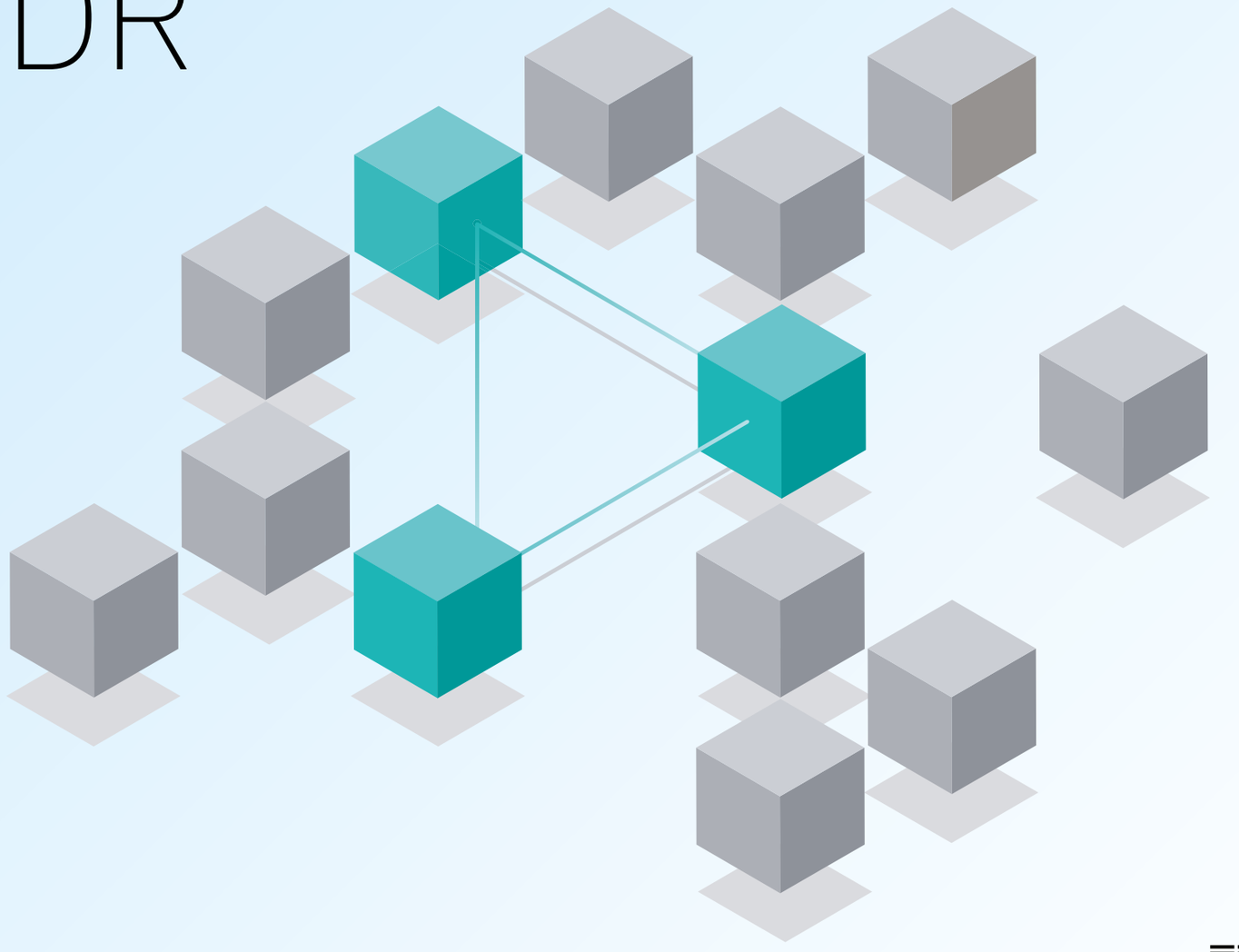
Guia do comprador de soluções EDR

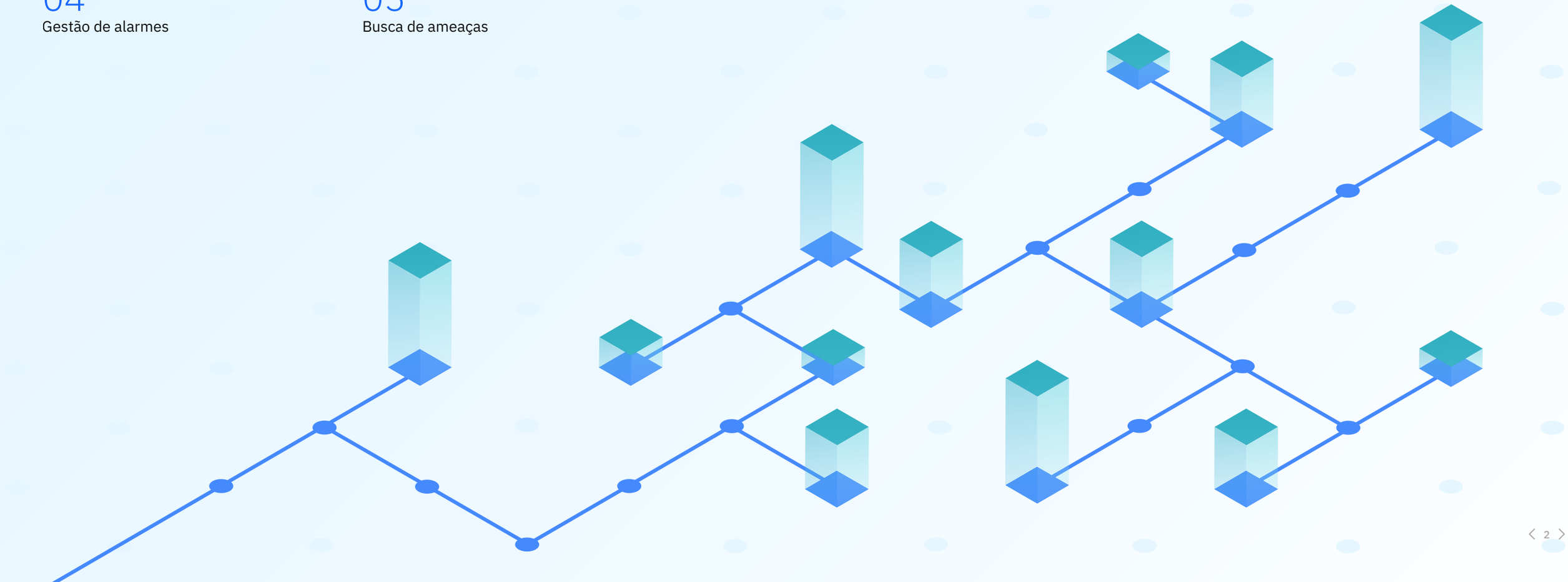
Como escolher a melhor solução de detecção e resposta de endpoints (EDR) para sua empresa



REAQTA
an IBM Company

IBM

Sumário



01
Introdução

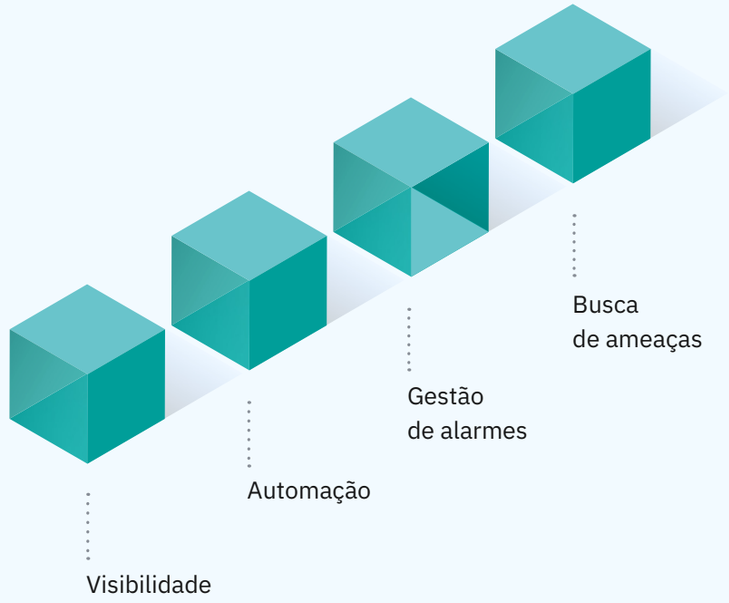
O que é EDR e por que preciso disso?
Estamos vendo uma crescente proliferação e interconectividade de endpoints e dados nos últimos anos, juntamente com o aumento de atividades maliciosas de agentes hostis. Estes fatores criaram uma ameaça substancial à continuidade dos negócios para grandes e pequenas organizações. Cada vez mais empresas estão sendo vítimas de ataques de cibercriminosos e hackers com aval governamental.

Os métodos tradicionais de proteção combatem ameaças conhecidas, mas são vulneráveis a técnicas de ataque sofisticadas e desconhecidas e não dão visibilidade aos ativos, que é um dos principais impedimentos para proteger esses sistemas. Habilidades especializadas em proteção de endpoints geralmente estão disponíveis apenas para as grandes organizações ou que dispõem de mais recursos financeiros. A isso se soma o fato de que agora os ataques estão acontecendo em grande velocidade e com um grande número de componentes móveis. Como resultado, as equipes humanas, confiando nas soluções tradicionais de proteção de endpoints, não conseguem acompanhar o ritmo.

Uma solução de detecção e resposta de endpoints (EDR) bloqueia e isola de forma proativa e automática os malwares, ao mesmo tempo em que dá munição para as equipes de segurança: as ferramentas certas para lidar com estes desafios de maneira confiante. Uma solução de EDR moderna pode assegurar a continuidade dos negócios, mitigando de forma eficaz as ameaças crescentes, automatizadas e avançadas, tais como ransomware ou ataques sem arquivos, sem aumentar a carga de trabalho dos analistas ou exigir especialistas em segurança altamente qualificados.

Você enfrenta algum desses desafios?
- Falha das soluções existentes
- Visibilidade limitada
- Falta de pessoal qualificado
- Fadiga de alarme
- Ameaças inativas

Uma solução de EDR moderna e eficaz compreende quatro elementos-chave que discutiremos nos próximos capítulos:



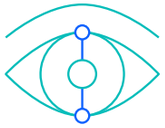
02
Visibilidade total do seu acervo de endpoints

Um dos principais impedimentos para proteger os endpoints é a falta de visibilidade. Sendo assim, uma solução de EDR moderna deve proporcionar uma visibilidade total e profunda das aplicações e processos em execução.

Quando surge uma ameaça, um alarme em tempo real deve ser criado automaticamente, mostrando o comportamento de maneira gráfica à medida que o ataque se desdobra, o que inclui o mapeamento MITRE ATT&CK possibilitando aos analistas total visibilidade e compreensão do que está acontecendo.

A maioria, se não todas as soluções de software de segurança de endpoint, trabalha dentro do sistema operacional, o que cria um limite para o agente do endpoint. Isto limita as capacidades e a visibilidade do agente ao mesmo tempo em que consome mais recursos computacionais. Ter um agente que trabalha na camada do hypervisor e é projetado para ser indetectável não só minimiza o uso de recursos, mas também proporciona uma visibilidade excepcional para monitorar todos os comportamentos do processo ao mesmo tempo em que permanece invisível para os invasores.

O que procurar:
- Visibilidade total do endpoint
- Alarmes em tempo real
- Criação do enredo (storyline)
- Agente sem atrito
- Fluxo de trabalho unificado



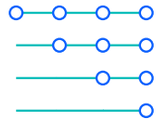
O que perguntar:

→ A sua solução proporciona visibilidade total e profunda das aplicações e processos em execução?

→ À medida que um ataque se desdobra, como a sua solução fornece informações relevantes, em tempo real, para compreender a ameaça?

→ Além de detectar uma violação e emitir um alarme, seu MSSP oferece resposta e correção de ponta a ponta?

03
Automação e facilidade de uso



Com a previsão de crescimento das sofisticadas ameaças e superfícies de ataque a partir de 2022, muitas organizações são extremamente pressionadas a se manter à frente dos cibercriminosos. Uma solução de EDR moderna deve aliviar uma carga de trabalho crescente por meio da automação inteligente e ao mesmo tempo fácil de usar para limitar a necessidade de especialistas em segurança altamente qualificados.

O segredo para que os compradores obtenham valor de uma EDR rapidamente é automatizar e simplificar. Com automação por IA, a maior parte do trabalho é deixada para os algoritmos, minimizando a interação humana. Por meio desses algoritmos de IA, o software passa a ser mais fácil de usar e as equipes podem ser colocadas em funcionamento rapidamente, sem longas capacitações.

Enquanto um ataque está acontecendo, os tempos de resposta são críticos: o tempo de investigação deve ficar bem abaixo de um minuto para eliminar as ameaças avançadas antes que elas possam causar danos à sua infraestrutura.

Os compradores devem procurar uma EDR que possa funcionar de forma autônoma e oferecer capacidades de detecção e resposta automatizadas. Isto proporciona aos analistas uma visão clara e em tempo real de um ataque, à medida que ele evolui, e pode oferecer uma correção guiada para voltar rapidamente ao normal.

O que procurar:
- Detecção autônoma
- Correção guiada
- Análise de agentes
- Tempos de resposta baixos
- Facilidade de uso

O que perguntar:

→ Existe a necessidade de qualificação avançada para usar uma EDR?

→ Para reduzir a carga de trabalho dos analistas, a EDR pode funcionar de forma autônoma?

→ Quanto aos tempos de resposta, as ameaças são analisadas na nuvem ou no agente?

→ Se as ameaças forem analisadas na nuvem, o que acontece se não houver conexão de internet?

04
Gestão de alarmes

O principal diferencial de uma EDR em relação às tradicionais soluções de antivírus (AV) é que um AV depende das assinaturas disponíveis para detecção e precisa ter conhecimento sobre uma ameaça a fim de bloqueá-la. Uma EDR, por outro lado, usa uma abordagem comportamental para identificar malwares e outras ameaças potenciais pela forma como elas se comportam em um endpoint. Além disso, ao contrário de um AV, uma EDR é leve por natureza e não requer atualizações frequentes.

A IA empregada em uma EDR moderna deve, portanto, ser capaz de detectar ameaças imediatamente, com grande precisão e alta fidelidade para manter o volume de alarmes – e a carga de trabalho dos analistas – em níveis mínimos. Os compradores devem se informar sobre o componente de IA e as técnicas de aprendizagem de máquina utilizadas. Em comparação com os mecanismos de IA que dependem de modelos e análises pré-treinados para detecção, uma EDR que utiliza um modelo de aprendizagem inicial para identificar o comportamento normal de cada endpoint permite maior precisão nas detecções e alarmes quando há desvios da normalidade.

Para reduzir o tempo de resposta e aliviar a fadiga de alarme para analistas, uma solução de EDR moderna deve ser equipada com um sistema de gestão de alarmes robusto e acionado por IA, capaz de aprender com o analista e depois aplicar de forma autônoma a tomada de decisões do analista no tratamento de alarmes do dia a dia. A implantação de um sistema de gerenciamento de alarmes totalmente automatizado e orientado por IA é fundamental para combater a fadiga de alarmes, reduzindo a rotatividade dos funcionários e voltando a ter o controle.

O que procurar:
- Alarmes de alta fidelidade
- Uso de modelos de IA
- Prevenção da fadiga de alarmes
- Gestão automatizada dos alarmes

O que perguntar:

→ Sua solução oferece uma forma de lidar automaticamente com alarmes e desativá-los?

→ De que modo a sua solução poupa o tempo do analista?

→ Como a sua solução diminui a incidência de falsos positivos?

→ Se um funcionário sair, como será retido o conhecimento da pessoa sobre a nossa infraestrutura?

05
Busca de ameaças

A busca de ameaças é uma parte importante de uma EDR moderna e é necessária para manter um ambiente limpo e livre de ameaças. A busca de ameaças pode determinar rapidamente se novas ameaças entraram em um ambiente e identificar pontos fracos. A mineração de dados permite que você procure e elimine ameaças latentes que podem passar despercebidas, mas que poderiam permanecer em um ambiente durante meses ou até anos, esperando para serem usadas por um invasor.

Por natureza, as ameaças in-memory e sem arquivos são difíceis de rastrear e são ainda mais difíceis de seguir quando os invasores utilizam variantes diferentes, à medida que se movimentam dentro de uma grande infraestrutura. Uma EDR moderna deve automatizar o trabalho de busca e usar a mineração de dados para permitir que as equipes de segurança procurem automaticamente ameaças com as mesmas semelhanças nos níveis comportamental e funcional com outros incidentes, entregando resultados em apenas alguns segundos.

A flexibilidade na busca de ameaças é muito importante. Os compradores devem procurar uma EDR que não apenas ofereça uma grande biblioteca de playbooks de detecção predefinidos que possam ser implantados imediatamente, mas também playbooks personalizados que possam ser facilmente criados, sem exigir conhecimentos de scripting, para cenários específicos exclusivos para as necessidades de segurança de uma organização.

Geralmente se compara a busca de ameaças a procurar agulha no palheiro. As buscas da EDR devem fornecer resultados abrangentes e granulares em tempo real, sendo capazes de detalhar parâmetros específicos de busca e combiná-los de forma inclusiva ou exclusiva. Para ajudar ainda mais os analistas e poupar seu tempo, os resultados devem ser exibidos em uma interface gráfica de usuário (GUI) de fácil compreensão, para que possam buscar fácil e intuitivamente qualquer evento, a partir de qualquer endpoint, a qualquer momento.

O que procurar:
- Busca de ameaças inativas
- Busca automatizada
- Criação de playbooks personalizados
- Não é necessário script
- Mineração de dados
- Capacidade em tempo real
- Síntese gráfica

O que perguntar:

→ Os usuários podem criar suas próprias estratégias e playbooks de detecção?

→ Dá para automatizar os cenários de busca de ameaças?

→ Você fornece uma síntese gráfica da busca de ameaças para fins de triagem rápida?

→ É necessário o conhecimento de criação de scripts para produzir os playbooks?

Próximas etapas

Saiba mais sobre a IBM Security ReaQta e solicite uma demonstração.

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo, SP

Produzido nos Estados Unidos da América
abril de 2022