# Comparativo

## EDR x EDRi (Integrado)

**SentinelOne**

**N-able N-sight RMM**

**N-able N-Central**

# Introdução

Este documento tem como objetivo demonstrar as diferenças entre as soluções de **EDR StandAlone *(autônomo)*** e o EDR Integrado.

Utilize este documento para avaliar qual é a solução ideal para os teus parceiros.

Colocamos os tópicos abaixo em forma de perguntas para facilitar o entendimento da necessidade, além de uma tabela de comparação rápida entre as ferramentas.

Note que há informações separadas para cada solução da N-able que utiliza o EDR (**N-sight** e **N-Central**). Quando não é descrito qual solução significa que ambas atuam da mesma forma.

Queremos sua opinião! Ajude-nos a aprimorar este documento. Qualquer dúvida, crítica ou sugestão, por favor, encaminhe um e-mail para boaspraticas@addee.com.br.

# N-able EDR
# Integrado vs. StandAlone

## Qual solução é a certa para o teu parceiro?

A N-able fornece soluções de detecção e resposta de endpoints *(EDR)* líderes do setor, fornecidas pela SentinelOne®.

O **EDR integrado** é baseado no pacote ***Singularity Control*** da SentinelOne, que não inclui a busca de ameaças por padrão.

Os recursos de detecção de ameaças são oferecidos como parte da licença ***SentinelOne Singularity Complete***, que pode ser disponibilizada para parceiros MSP que fornecem ofertas de segurança avançadas aos clientes.

O N-able EDR está atualmente disponível como **StandAlone** *(autônomo)* e **Integrado** *(N-sight e N-central)*.

A tabela abaixo resume as diferenças entre as duas soluções.

| | EDR INTEGRADO (N-SIGHT & N-CENTRAL) | EDR STANDALONE |
|---|---|---|
| **Console de Gerenciamento** | • **Painel único** *(configurações de acesso integrado para implantação, política, monitoramento de métricas e gerenciamento de incidentes).*<br><br>• **Widgets do painel com acesso de leitura** | • **Acesso direto à conta** *(o parceiro deve gerenciar o acesso do usuário).*<br><br>• **Painel personalizável**<br><br>• **Funções personalizáveis baseadas em controles de acesso**<br><br>• **Acesso à API** |
| **Implantação do Agente** | **Instalação rápida** e baseada na política da árvore do cliente ou nas configurações do dispositivo | • **Instalação manual do agente** ou implementação baseada em política do gerenciador de automação (AMP).<br><br>• N-able disponibiliza **script de implantação** e instruções no site. |

| | | |
|---|---|---|
| **Alertas e Notificações** | Um subconjunto dos alertas e notificações independentes do EDR.<br><br>- **EDR no N-Central:** alertas para EDR não instalado, EDR sem execução, recurso anti violação desativado, evento de ameaça maliciosa ativa não mitigado.<br><br>- **EDR no N-Sight:** alerta se um dispositivo foi infectado, adulterado ou se requer reinicialização. | Acesso total a todos os tipos de recursos de notificação disponíveis na SentinelOne *(incluindo a exportação de eventos syslog para integrações SIEM, personalização de listas de destinatários de notificações e notificações granulares).* |
| **Relatórios** | • Relatórios N-Sight / N-Central nativos<br><br>• Exportações de dados para fins de relatórios | • Relatórios de EDR nativos do SentinelOne<br><br>• Exportações de dados para fins de relatórios |
| **Caça a ameaças (Visibilidade Profunda)** | **N/A** | Oferecido apenas com a licença **SentinelOne Singularity Complete** |
| **SO Suportados** | **• Windows**<br><br>• Atualmente, está disponível **suporte parcial macOS para N-central**. | **• Windows**<br><br>**• Linux**<br><br>**• Mac OS** |
| **Outros** | **N/A** | • **Página de automação** - tarefas automatizadas executadas por agentes<br><br>• **Página de atividade** - atividades de rede e dispositivos para fins de auditoria<br><br>• **Página de aplicativos** - todos os aplicativos instalados nos endpoints e seu nível de risco<br><br>• **Regras Personalizadas** *(disponível apenas na versão completa)* |

# Como Avaliar Suas Opções?

Enquanto o **N-able EDR StandAlone** oferece mais recursos, o **N-able EDR Integrado** traz benefícios exclusivos.

Para determinar qual solução é a certa para o teu parceiro, considere fazer as seguintes perguntas:

## + O que é EDR Integrado e o que é EDR StandAlone?

O **EDR Integrado** é baseado no pacote ***SentinelOne Singularity Control***, que foi integrado às soluções **N-able N-Sight RMM** e **N-central** para facilitar seu trabalho.

Já o **EDR StandAlone** está disponível separadamente do **N-able N-Sight RMM / N-central**, sob o modelo de licenciamento ***SentinelOne Singularity Control***.

## + Quais são as principais diferenças entre as duas versões?

Embora o **EDR StandAlone** forneça toda a gama de recursos de EDR do SentinelOne, alguns ainda não estão disponíveis ou estão disponíveis apenas parcialmente no **EDR Integrado**.

No entanto, o **EDR Integrado** vem com fácil implantação e um único painel transparente.

## + Qual método de implantação funciona melhor para você?

Cada versão do EDR vem com um método de implantação diferente. Você precisa avaliar qual atende melhor as suas necessidades:

• Com o **EDR Integrado ao N-sight RMM**, você pode implantar facilmente o EDR em vários dispositivos ao mesmo tempo usando as configurações de estrutura de árvore do cliente nativa da plataforma.

• Com **EDR Integrado ao N-central**, você pode criar regras com perfis para implantar facilmente o EDR em dispositivos novos e existentes na hierarquia do cliente ou local.

• Já com o **EDR StandAlone**:

- As tarefas de administração *(como usuários, cliente ou hierarquia do site)*, implantação e atualizações precisariam ser feitas via GUI ou via API, conforme aplicação.

- A N-able fornece um script de implantação pré-construído, bem como um recurso de gerenciamento de automação para criar facilmente seu próprio script; você também pode instalar agentes manualmente

## + Como a exibição do painel integrado do EDR difere do EDR StandAlone?

• A exibição do painel disponível no **EDR Integrado** é predefinida e apresenta widgets de visão geral que mostram status de resumo para várias atividades e itens em todos os endpoints, como ameaças não resolvidas, endpoints infectados, ameaças por mecanismo de detecção, ameaças por tipo, etc.

Esses widgets podem ser detalhados para obter mais informações.

• A exibição do painel no **EDR StandAlone** é personalizável, permitindo que os usuários usem widgets existentes, adicionem novos e criem seus próprios painéis acionáveis.

O painel é totalmente interativo com várias ações da GUI e menus suspensos disponíveis para uso.

## + Qual a importância de ter um único painel gerenciável para todas as suas atividades de RMM agora?

A capacidade de centralizar todas as atividades de RMM e EDR em uma plataforma elimina inconsistências, economiza tempo e recursos e ajuda seus técnicos a manterem o foco nas tarefas relacionadas a EDR.

• O **EDR Integrado** permite simplificar a proteção e o gerenciamento da rede a partir de um único painel, permitindo uma abordagem unificada para monitoramento e gerenciamento de dispositivos.

• Com o **EDR StandAlone**, você não se beneficiará dessa experiência unificada e do foco e eficiência que ela traz.

Então, se ter um único painel gerenciável é a sua maior prioridade no momento, o **EDR Integrado** pode ser a melhor solução pra você agora.

## + Os relatórios de EDR são essenciais para a retenção dos seus clientes?

Os relatórios de EDR ajudam a demonstrar melhor o valor da solução para os seus clientes. Alguns clientes podem até exigir relatórios do EDR para entender melhor o valor que estão obtendo ou podem ter requisitos de conformidade que exigem relatórios.

• Com o **EDR Integrado ao N-sight RMM**, você tem acesso aos relatórios nativos do N-sight RMM que cobrem a atividade de EDR, incluindo relatório de inventário de dispositivos, relatório de política de recursos, relatório de auditoria do usuário e relatório de limpeza de verificação. Você também pode exportar informações das guias *Dashboard* e *Analyze* do EDR no formato CSV e criar manualmente seus próprios relatórios.

• O **EDR integrado ao N-central** fornece relatórios de serviço de status nativos *(por exemplo, status detalhado de disponibilidade, distribuição de status de disponibilidade, dados monitorados brutos de métricas, resumo de configuração de status)*. Você também pode exportar informações das guias Dashboard e Analyze do EDR no formato CSV e criar manualmente seus próprios relatórios.

• Já o **EDR StandAlone** fornece os recursos nativos de geração de relatórios da SentinelOne. Você pode criar ou agendar relatórios dos Insights que incluem estatísticas, tendências e resumos com informações acionáveis.

Se os recursos completos de geração de relatórios forem uma prioridade importante, o **EDR StandAlone** pode ser a melhor solução para você agora.

## + Você está usando uma ferramenta SIEM?

Eventos de endpoint *(por exemplo, agente ativado/desativado, conta criada/excluída, varredura iniciada, etc.)* são registrados em mensagens Syslog. Os **sistemas de informações de segurança e gerenciamento de eventos *(SIEMs)*** coletam dados de log e eventos disponíveis em toda a empresa para serem armazenados em vários casos de uso.

Para obter uma visão centralizada de todos os eventos de rede, você pode querer enviar eventos Syslog do EDR para o seu SIEM. Atualmente, isso pode ser feito apenas com o **EDR StandAlone**.

Se você fornece serviços SOC ou usa um SOC para seu próprio negócio, o **EDR StandAlone** pode ser a melhor opção para você.

## + Você está usando um sistema de gerenciamento de tickets PSA?

Se você estiver usando um sistema de tickets PSA, precisará priorizar os tickets e encaminhá-los aos técnicos apropriados com eficiência. As notificações do EDR desempenham um papel fundamental nesse processo, pois facilitam a identificação e a priorização dos eventos que precisam de atenção imediata.

• O **EDR integrado ao N-central** vem com um serviço de status de EDR que fornece notificações sobre coisas como o EDR não ter sido instalado ou não está em execução, o recurso *anti-tamper (adulterado)* estar desativado ou um evento de ameaça maliciosa ativa que não foi mitigado; este é um subconjunto das notificações **EDR StandAlone**.

• O **EDR Integrado ao N-sight RMM** vem com um serviço de status de EDR que fornece notificações sobre coisas como um dispositivo ter sido adulterado, um evento de ameaça maliciosa ativo que ainda não foi mitigado ou se o dispositivo requer reinicialização; este é um subconjunto das notificações **EDR StandAlone**.

• Já o **EDR StandAlone** oferece um rico conjunto de notificações granulares disponíveis para configuração de e-mail e/ou syslog por meio da console da SentinelOne. As notificações incluem listas de destinatários e alertas sobre eventos administrativos, de mitigação, operações e muitos outros tipos de endpoint.

Se você fornece serviços SOC ou usa um SOC para seu próprio negócio, o **EDR StandAlone** pode ser a melhor opção para você.

## + Para quais sistemas operacionais você precisa de suporte?

• O **EDR integrado ao N-central** fornece suporte completo para Windows. Para dispositivos macOS, atualmente a implantação de EDR em dispositivos macOS pode ser feita por meio de regras, mas exige que os usuários façam login nos dispositivos macOS para concluir o processo. Além disso, o serviço de status do EDR informará aos usuários que o agente do EDR no macOS está operacional.

Para oferecer suporte a toda a gama de dispositivos, você pode querer considerar uma combinação de recursos do **EDR integrado** e do **EDR StandAlone**.

• O **EDR Integrado ao N-sight RMM** fornece suporte completo para dispositivos Windows. Para oferecer suporte a toda a gama de dispositivos, você pode querer considerar uma combinação de recursos do **EDR integrado** e do **EDR StandAlone**.

• Já o **EDR StandAlone** fornece suporte completo para dispositivos Windows, Linux e macOS. Independentemente da solução escolhida, você pode obter suporte para toda a sua gama de dispositivos.

No entanto, para o **EDR StandAlone** o suporte para Windows, macOS e Linux vem pronto para uso, enquanto para o **EDR Integrado *(N-central e RMM)***, você pode considerar uma combinação de dispositivos Windows em EDR integrado e dispositivos macOS em **EDR StandAlone**.

## + Você precisa de um recurso para caçar ameaças?

A caça a ameaças é uma abordagem proativa à segurança cibernética que ajuda a identificar vulnerabilidades de rede. Ele complementa ferramentas automatizadas com pesquisas em seu ambiente para indicadores conhecidos de comprometimento *(IOC)* e comportamento e táticas que os invasores usam.

A caça a ameaças geralmente é feita por uma equipe de segurança com conhecimento especializado sobre o que é normal em seu ambiente. Um entendimento técnico da arquitetura, sistema, aplicativo e comportamento de rede esperados é necessário para descobrir comportamentos inesperados e discrepantes:

• As táticas, técnicas e procedimentos *(TTPs)* que os invasores usam.

• Os pontos vulneráveis mais prováveis em seu ambiente.

• Fluxos confiáveis de informações para indicadores recentes e comuns de comprometimento.

A **Visibilidade Profunda** oferecida com a licença ***SentinelOne Singularity Complete*** fornece o alto nível de visibilidade em endpoints que é necessário para uma busca eficaz de ameaças.

Se você executa SOCs para seus clientes ou fornece serviços de segurança gerenciados, a busca por ameaças é um recurso valioso a ser adicionado à sua pilha de segurança. Da mesma forma, se seus clientes tiverem SOCs, os recursos de detecção de ameaças complementarão sua pilha de segurança.

As empresas que fazem a caça às ameaças normalmente têm funcionários dedicados. Se este for o seu caso, os recursos de detecção de ameaças *(Visibilidade Profunda, ou Deep Visibility, do SentinelOne)* são uma ótima opção para o seu portfólio de serviços.

## + Se eu optar por uma solução, será possível mudar para outra mais tarde?

Recomendamos que você trabalhe com seu representante **N-able** para identificar a melhor solução desde o início. Você pode experimentar ambas as soluções para ver qual atenderá melhor às suas necessidades.

É importante considerar cuidadosamente todos os aspectos acima para garantir que você tenha a solução certa para você e seus clientes.

**Observação:**

• Mover seus dispositivos do **EDR StandAlone** para o **EDR Integrado** aproveita um recurso de aquisição do **EDR StandAlone**, que permite que você mova seus dispositivos para o **EDR Integrado** sem interromper seus usuários finais.

• Mover seus dispositivos do **EDR integrado** para o **EDR StandAlone** exige que você execute as seguintes etapas: **Desinstalar > Reinicializar > Reinstalar > Reinicializar**, o que desativará a integração.

## + Como posso solicitar uma avaliação do EDR Integrado?

Se você já possui o **N-Sight RMM / N-central**, pode ativar uma avaliação de 30 dias do **EDR Integrado** a partir do aplicativo. Basta seguir estes passos:

1. Ative sua avaliação em nossa nova Visualização de gerenciamento de integração, disponível no menu de navegação à esquerda

2. Expanda o menu Integrações na navegação à esquerda

3. Selecione Gerenciamento de Integração

4. Clique em Ativar

5. Crie suas políticas de EDR

**Observação:** recomendamos testar o EDR em um ambiente que não seja de produção — configurando políticas para usar o modo de detecção durante o teste — antes de implantar amplamente.

## + Posso ativar uma avaliação integrada do EDR se estiver usando a versão StandAlone?

Sim. Você pode migrar agentes do EDR existentes implantados em endpoints já gerenciados por **N-Sight RMM / N-central** e já registrado em um console de gerenciamento de N-able EDR para **EDR Integrado**.

# Obrigado!

Ficamos felizes por você utilizar este manual :)


**Responsável:** Caio Gutierri
**Departamento:** Engenharia de Vendas
**Última alteração:** Abril/2023

**0800 761 2812**
boaspraticas@addee.com.br