3. Na seção **Geral**, selecione um status para a atualização, alterando a opção **Status de aprovação da atualização**. Você pode selecionar o status *Aprovado*, *Negado*, ou *Indefinido*.

4. Clique no botão **Salvar** para salvar as alterações.

A atualização selecionada tem o status que você definiu.

Se você definir o status **Negado** para atualizações de software de terceiros, estas atualizações não serão instaladas em dispositivos para os quais elas foram planejadas, mas que ainda não foram instaladas. As atualizações permanecerão nos dispositivos nos quais elas já foram instaladas. Se você tiver de exclui-las, poderá exclui-las manualmente localmente.

Criação da tarefa Executar a sincronização do Windows Update

A tarefa *Executar a sincronização com o Windows Update* só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

A tarefa *Executar a sincronização com o Windows Update* é necessária caso deseje usar o Servidor de Administração como um servidor WSUS. Nesse caso, o Servidor de Administração baixa as atualizações do Windows para o banco de dados e fornece as atualizações para o Windows Update em dispositivos clientes no modo centralizado por meio de Agentes de Rede. Se a rede não usar um servidor WSUS, cada dispositivo cliente baixa as atualizações da Microsoft de servidores externos independentemente.

A tarefa *Executar a sincronização com o Windows Update* somente baixa metadados de servidores da Microsoft. O Kaspersky Security Center baixa as atualizações quando você executa uma tarefa de instalação de atualização e somente as atualizações selecionadas para instalação.

Ao executar a tarefa **Executar a sincronização com o Windows Update**, o aplicativo recebe uma lista das atualizações atuais de um servidor de atualização da Microsoft. A seguir, o Kaspersky Security Center compila uma lista das atualizações que se tornaram desatualizadas. Na próxima inicialização da tarefa **Encontrar as vulnerabilidades e as atualizações necessárias**, o Kaspersky Security Center sinaliza todas as atualizações desatualizadas e define a hora de exclusão para as mesmas. Na próxima inicialização da tarefa **Executar a sincronização com o Windows Update**, todas as atualizações sinalizadas para exclusão 30 dias atrás serão excluídas. O Kaspersky Security Center também verifica quanto a atualizações desatualizadas foram sinalizadas para a exclusão há mais de 180 dias, e então exclui estas atualizações mais antigas.

Quando a tarefa **Executar a sincronização com o Windows Update** for concluída e as atualizações desatualizadas são excluídas, o banco de dados ainda pode ter os códigos hash que pertencem aos arquivos de atualizações excluídas, assim como os arquivos correspondentes nos arquivos %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (se eles foram baixados anteriormente). Você pode executar a tarefa Manutenção do Servidor de Administração para excluir estes registros desatualizados do banco de dados e dos arquivos correspondentes.

Para criar uma tarefa Executar a sincronização com o Windows Update:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.

3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Executar a sincronização com o Windows Update**.

4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

5. Ative a opção **Baixar arquivos de instalação rápida** se desejar que os arquivos de atualização expressa sejam baixados ao executar a tarefa.

   Quando o Kaspersky Security Center sincroniza as atualizações com Microsoft Windows Update Servers, as informações sobre todos os arquivos são salvas no banco de dados do Servidor de Administração. Todos os arquivos necessários para uma atualização também são baixados para a unidade durante a interação com o Windows Update Agent. Em particular, o Kaspersky Security Center salva as informações sobre arquivos de atualização expressa no banco de dados e as baixa quando necessário. Baixar os arquivos de atualização expressa conduz a diminuição do espaço livre na unidade.
   Para evitar uma redução no volume de espaço em disco e reduzir o tráfego, desative a opção **Baixar arquivos de instalação rápida**.

6. Selecione os aplicativos para os quais deseja baixar atualizações.
   Se a caixa de seleção **Todos os aplicativos** estiver marcada, as atualizações serão baixadas para todos os aplicativos existentes, e para todos os aplicativos que possam ser lançados no futuro.

7. Selecione as categorias de atualizações que deseja baixar para o Servidor de Administração.

   Se a caixa de seleção **Todas as categorias** estiver marcada, as atualizações serão baixadas para todas as categorias existentes, e para todas as categorias que podem aparecer no futuro.

8. Selecione os idiomas de localização das atualizações que deseja baixar para o Servidor de Administração.
   Selecione uma das seguintes opções:

   - Baixar todos os idiomas, incluindo os novos

     Se esta opção estiver selecionada, todos os idiomas de localização disponíveis das atualizações serão baixados para o Servidor de Administração. Por padrão, esta opção está selecionada.

   - Baixar idiomas selecionados

     Se esta opção estiver selecionada, você pode selecionar na lista os idiomas de localização das atualizações que serão baixados para o Servidor de Administração.

9. Especifique qual conta usar ao executar a tarefa. Selecione uma das seguintes opções:

   - Conta padrão

     A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.
     Por padrão, esta opção está selecionada.

     Especificar conta

     Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

10. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

11. Clique no botão **Concluir**.

    A tarefa é criada e exibida na lista de tarefas.

12. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

13. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

14. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Atualizar aplicativos de terceiros automaticamente

Alguns aplicativos de terceiros podem ser atualizados automaticamente. O fornecedor do aplicativo define se o aplicativo é compatível ou não com o recurso de atualização automática. Se um aplicativo de terceiros instalado em um dispositivo gerenciado for compatível com atualização automática, você poderá especificar a configuração de atualização automática nas propriedades do aplicativo. Depois de alterar a configuração de atualização automática, os Agentes de Rede aplicam a nova configuração a cada dispositivo gerenciado no qual o aplicativo está instalado.

A configuração de atualização automática é independente dos outros objetos e configurações do recurso Gerenciamento de patches e vulnerabilidades. Por exemplo, esta configuração não depende de um status de aprovação de atualização ou das tarefas de instalação da atualização, como *Instalar as atualizações necessárias e corrigir vulnerabilidades*, *Instalar as atualizações do Windows Update* e *Corrigir vulnerabilidades*.

Para definir a configuração de atualização automática para um aplicativo de terceiros:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos**.

2. Clique no nome do aplicativo para o qual deseja alterar a configuração de atualização automática.

   Para simplificar a pesquisa, você pode filtrar a lista pela coluna **Status das atualizações automáticas**.

   A janela Propriedades do aplicativo é aberta.

3. Na seção **Geral**, selecione um valor para a seguinte configuração:

   Status das atualizações automáticas

Selecione uma das seguintes opções:

- **Indefinido**

  O recurso de atualização automática será desativado. O Kaspersky Security Center instala atualizações de aplicativos de terceiros usando as tarefas: *Instalar as atualizações necessárias e corrigir vulnerabilidades*, *Instalar as atualizações do Windows Update*, e *Corrigir vulnerabilidades*.

- **Permitido**

  Depois que o fornecedor lança uma atualização para o aplicativo, esta atualização é instalada nos dispositivos gerenciados automaticamente. Nenhuma outra ação é necessária.

- **Bloqueado**

  As atualizações do aplicativo não são instaladas automaticamente. O Kaspersky Security Center instala atualizações de aplicativos de terceiros usando as tarefas: *Instalar as atualizações necessárias e corrigir vulnerabilidades*, *Instalar as atualizações do Windows Update*, e *Corrigir vulnerabilidades*.

4. Clique no botão **Salvar** para salvar as alterações.

A configuração de atualização automática é aplicada ao aplicativo selecionado.

Corrigindo vulnerabilidades de software de terceiros

Esta seção descreve os recursos do Kaspersky Security Center relacionados à correção de vulnerabilidades no software instalado nos dispositivos gerenciados.

Cenário: Encontrar e corrigir vulnerabilidades de software de terceiros

Esta seção fornece um cenário para localizar e corrigir vulnerabilidades nos dispositivos gerenciados que executam o Windows. Você pode encontrar e corrigir vulnerabilidades de software no sistema operacional e em software de terceiros, incluindo software da Microsoft.

Pré-requisitos

O Kaspersky Security Center está implementado em sua organização.

- Há dispositivos gerenciados executando o Windows na sua organização.
- A conexão com a Internet é necessária para que o Servidor de Administração execute as seguintes tarefas:
  - Para fazer uma lista de correções recomendadas para vulnerabilidades em softwares da Microsoft. A lista é criada e atualizada regularmente por especialistas da Kaspersky.

    Para corrigir vulnerabilidades em software de terceiros que não sejam software da Microsoft.

A localização e a correção de vulnerabilidades de software ocorre em fases:

1. **Verificar vulnerabilidades no software instalado nos dispositivos gerenciados**

   Para encontrar vulnerabilidades no software instalado nos dispositivos gerenciados, execute a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Kaspersky Security Center recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa.

   A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. Caso não tenha executado o assistente, inicie-o agora ou crie a tarefa manualmente.

   Instruções de como proceder:

   - Console de administração: Verificando aplicativos em busca de vulnerabilidades, Agendando a tarefa Encontrar as vulnerabilidades e as atualizações necessárias

     Kaspersky Security Center Web Console: Criar a tarefa Encontrar as vulnerabilidades e as atualizações necessárias, Configurações da tarefa Encontrar as vulnerabilidades e as atualizações necessárias

2. **Analisar a lista de vulnerabilidades de software detectadas**

   Visualize a lista **Vulnerabilidades de software** e decida quais vulnerabilidades devem ser corrigidas. Para visualizar informações detalhadas sobre cada vulnerabilidade, clique no nome da vulnerabilidade na lista. Para cada vulnerabilidade na lista, você também pode visualizar as estatísticas sobre a vulnerabilidade nos dispositivos gerenciados.

   Instruções de como proceder:

   Console de Administração: Visualizar informações sobre vulnerabilidades do software, Visualizar estatísticas das vulnerabilidades em dispositivos gerenciados

   - Kaspersky Security Center Web Console: Visualização das informações sobre as vulnerabilidades de software, Visualização das estatísticas de vulnerabilidades em dispositivos gerenciados

3. **Configurar a correção de vulnerabilidades**

   Quando as vulnerabilidades de software são detectadas, é possível corrigi-las nos dispositivos gerenciados usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*.

   A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa lhe permite instalar várias atualizações e corrigir várias vulnerabilidades de acordo com certas regras. Observe que esta tarefa pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades. Para corrigir vulnerabilidades de software, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* usa as atualizações de software recomendadas.

   A tarefa *Corrigir vulnerabilidades* não requer a opção de licença para o recurso Gerenciamento de patches e vulnerabilidades. Para usar esta tarefa, você deve especificar manualmente as correções para vulnerabilidades em softwares de terceiros definidas pelo usuário, listadas nas configurações da tarefa. A tarefa *Corrigir vulnerabilidades* usa as correções recomendadas para o software da Microsoft e as correções do usuário para softwares de terceiros.

   É possível iniciar o Assistente para Correção de Vulnerabilidades, que cria uma dessas tarefas automaticamente, ou criá-las manualmente.

   Instruções de como proceder:

   - Console de administração: Selecionar as correções de usuário para as vulnerabilidades de software de terceiros, Corrigir as vulnerabilidades em aplicativos

- Kaspersky Security Center Web Console: Selecionar as correções do usuário para vulnerabilidades em software de terceiros, Corrigir as vulnerabilidades de software de terceiros, Criar a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades

4 Agendar as tarefas

Para garantir que a lista de vulnerabilidades esteja sempre atualizada, agende a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para executá-la automaticamente de tempo em tempo. A frequência média recomendada é de uma vez por semana.

Se você criou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, pode agendá-la para ser executada com a mesma frequência que a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou com menor frequência. Ao agendar a tarefa *Corrigir vulnerabilidades*, é necessário selecionar correções para o software da Microsoft ou especificar correções de usuário para o software de terceiros sempre que iniciar a tarefa.

Ao agendar as tarefas, certifique-se que uma tarefa para corrigir vulnerabilidades é iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

5 Ignorar vulnerabilidades de software (opcional)

Se você desejar, poderá ignorar as vulnerabilidades de software a ser corrigidas em todos os dispositivos gerenciados ou apenas nos dispositivos gerenciados selecionados.

Instruções de como proceder:

Console de administração: Ignorar as vulnerabilidades do software

- Kaspersky Security Center Web Console: Ignorando vulnerabilidades de software

6 Executando uma tarefa de correção de vulnerabilidades

Inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*. Quando a tarefa estiver concluída, certifique-se que possui o status *Concluído com êxito* na lista de tarefas.

7 Criar o relatório sobre os resultados da correção de vulnerabilidades de software (opcional)

Para ver estatísticas detalhadas sobre a correção de vulnerabilidades, gere um Relatório de vulnerabilidades. O relatório exibe informações sobre vulnerabilidades de software que não são corrigidas. Assim, é possível ter uma ideia sobre como encontrar e corrigir vulnerabilidades em softwares de terceiros, incluindo softwares da Microsoft, em sua organização.

Instruções de como proceder:

- Console de Administração: Criando e visualizando um relatório

Kaspersky Security Center Web Console: Gerando e visualizando atualizações de software

8 Verificar a configuração para encontrar e corrigir vulnerabilidades em software de terceiros

Certifique-se de ter feito o seguinte:

Obtenção e revisão da lista de vulnerabilidades de software detectadas nos dispositivos gerenciados

- Vulnerabilidades de software ignoradas, se desejado
- A tarefa para corrigir vulnerabilidades está configurada

As tarefas para localizar e corrigir vulnerabilidades de software estão agendadas para que sejam iniciadas sequencialmente

- Verificar se a tarefa para corrigir vulnerabilidades de software foi executada

Resultados

Se você criou e configurou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, as vulnerabilidades são corrigidas nos dispositivos gerenciados automaticamente. Quando a tarefa é executada, ela correlaciona a lista de atualizações de software disponíveis às regras especificadas nas configurações da tarefa. Todas as atualizações de software que atendem aos critérios das regras serão baixadas no repositório do Servidor de Administração e instaladas para corrigir as vulnerabilidades de software.

Se você criou a tarefa *Corrigir vulnerabilidades*, apenas as vulnerabilidades de software no software da Microsoft são corrigidas.

Sobre como encontrar e corrigir vulnerabilidades de software

O Kaspersky Security Center detecta e corrige vulnerabilidades de software em dispositivos gerenciados que executam os sistemas operacionais das famílias Microsoft Windows. As vulnerabilidades são detectadas no sistema operacional e no software de terceiros, incluindo o software da Microsoft.

Localizar vulnerabilidades de software

Para encontrar vulnerabilidades de software, o Kaspersky Security Center usa características do banco de dados de vulnerabilidades conhecidas. Este banco de dados é criado por especialistas da Kaspersky. Ele contém informações sobre vulnerabilidades, como descrição da vulnerabilidade, data de detecção da vulnerabilidade, nível de gravidade da vulnerabilidade. Você pode encontrar os detalhes das vulnerabilidades de software no site da Kaspersky.

O Kaspersky Security Center usa a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para encontrar vulnerabilidades de software.

Corrigir vulnerabilidades de software

Para corrigir vulnerabilidades de software, o Kaspersky Security Center usa atualizações de software emitidas pelos fornecedores do software. Os metadados das atualizações de software são baixados no repositório do Servidor de Administração como um resultado da execução da tarefa a seguir:

Baixar atualizações no repositório do Servidor de Administração. Esta tarefa tem como objetivo fazer o download de metadados de atualizações para o Kaspersky e software de terceiros. Essa tarefa é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. Você pode criar a tarefa Baixar atualizações no repositório do Servidor de Administração manualmente.

- *Executar a sincronização com o Windows Update*. Esta tarefa tem como objetivo baixar metadados de atualizações para o software Microsoft.

As atualizações de software para corrigir vulnerabilidades podem ser representadas como pacotes ou patches de distribuição completos. As atualizações de software que corrigem vulnerabilidades de software são denominadas *correções*. As *correções recomendadas* são aquelas recomendadas para instalação pelos especialistas da Kaspersky. *Correções do usuário* são aquelas especificadas manualmente para instalação pelos usuários. Para instalar uma correção do usuário, você deve criar um pacote de instalação contendo essa correção.

Se você possui a licença do Kaspersky Security Center com o recurso Gerenciamento de patches e vulnerabilidades, para corrigir as vulnerabilidades de software, você pode usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Esta tarefa corrige automaticamente várias vulnerabilidades instalando as correções recomendadas. Para esta tarefa, você pode configurar manualmente certas regras para corrigir várias vulnerabilidades.

Se você não possui a licença do Kaspersky Security Center com o recurso Gerenciamento de patches e vulnerabilidades, para corrigir as vulnerabilidades de software, você pode usar a tarefa *Corrigir vulnerabilidades*. Por meio desta tarefa, você pode corrigir vulnerabilidades instalando as correções recomendadas para o software da Microsoft e as correções do usuário para outros softwares de terceiros.

Por motivos de segurança, todas as atualizações de softwares de terceiros instaladas usando o recurso Gerenciamento de patches e vulnerabilidades são verificadas automaticamente pelas tecnologias da Kaspersky em busca de malwares. Essas tecnologias são usadas para verificação automática de arquivos e incluem verificação de vírus, análise estática, análise dinâmica, análise de comportamento no ambiente sandbox e aprendizado de máquina.

Os especialistas da Kaspersky não realizam análises manuais de atualizações de softwares de terceiros que podem ser instaladas usando o recurso Gerenciamento de patches e vulnerabilidades. Além disso, os especialistas da Kaspersky não pesquisam vulnerabilidades (conhecidas ou desconhecidas) ou recursos não documentados nessas atualizações, nem realizam outros tipos de análise das atualizações além dos especificados no parágrafo acima.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Para corrigir algumas vulnerabilidades de software, é necessário aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software, se o aceite do EULA for solicitado. Se você recusar o EULA, a vulnerabilidade do software não será corrigida.

Corrigindo vulnerabilidades de software de terceiros

Depois de obter a lista de vulnerabilidades de software, você pode corrigir as vulnerabilidades de software nos dispositivos gerenciados que executam o Windows. É possível corrigir vulnerabilidades de software no sistema operacional e em softwares de terceiros, incluindo softwares da Microsoft, criando e executando a tarefa *Corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Como opção, é possível criar uma tarefa para corrigir vulnerabilidades de software das seguintes maneiras:

- Abrindo a lista de vulnerabilidades e especificando quais vulnerabilidades corrigir.
  Como resultado, é criada uma nova tarefa para corrigir vulnerabilidades de software. Como opção, você pode adicionar as vulnerabilidades selecionadas a uma tarefa existente.
- Executando o assistente para Correção de vulnerabilidades.

O Assistente para correção de vulnerabilidades só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

O assistente simplifica a criação e a configuração de uma tarefa de correção de vulnerabilidades e permite eliminar a criação de tarefas redundantes que contenham as mesmas atualizações para instalação.

Corrigindo vulnerabilidades de software usando a lista de vulnerabilidades

Para corrigir vulnerabilidades de software:

1. Abra uma das listas de vulnerabilidades:

   Para abrir a lista geral de vulnerabilidades, No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Vulnerabilidades de software**.

   - Para abrir a lista de vulnerabilidades de um dispositivo gerenciado, No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados** → <nome do dispositivo> → **Avançado** → **Vulnerabilidades de software**.
   - Para abrir a lista de vulnerabilidades de um aplicativo específico, No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos** → <nome do aplicativo> → **Vulnerabilidades**.

   Uma página com uma lista de vulnerabilidades em softwares de terceiros é exibida.

2. Selecione uma ou mais vulnerabilidades na lista e clique no botão **Corrigir vulnerabilidade**.

   Se a atualização de software recomendada para corrigir uma das vulnerabilidades selecionadas estiver ausente, uma mensagem informativa será exibida.

   Para corrigir algumas vulnerabilidades de software, é necessário aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software, se o aceite do EULA for solicitado. Se você recusar o EULA, a vulnerabilidade do software não será corrigida.

3. Selecione uma das seguintes opções:

   - **Nova tarefa**

     O Assistente para nova tarefa inicia. Se você tiver a licença do Gerenciamento de patches e vulnerabilidades, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* será pré-selecionada. Se você não tiver a licença, a tarefa *Corrigir vulnerabilidades* será pré-selecionada. Seguem abaixo as etapas do assistente para concluir a criação da tarefa.

   - **Corrigir vulnerabilidade (adicionar a regra à tarefa especificada)**

     Selecione uma tarefa à qual deseja adicionar as vulnerabilidades selecionadas. Se você tiver a licença de Gerenciamento de patches e vulnerabilidades, selecione a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Uma nova regra para corrigir as vulnerabilidades selecionadas será adicionada automaticamente à tarefa escolhida. Se você não tiver a licença, selecione a tarefa *Corrigir vulnerabilidades*. As vulnerabilidades selecionadas serão adicionadas às propriedades da tarefa.

     A janela de propriedades da tarefa é aberta. Clique no botão **Salvar** para salvar as alterações.

Se você escolheu criar uma nova tarefa, a tarefa será criada e exibida na lista de tarefas em **Dispositivos** → **Tarefas**. Se você optou por adicionar as vulnerabilidades a uma tarefa existente, as vulnerabilidades serão salvas nas propriedades da tarefa.

Para corrigir as vulnerabilidades de software de terceiros, inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*. Se você criou a tarefa *Corrigir vulnerabilidades*, deve especificar manualmente as atualizações de software para corrigir as vulnerabilidades de software listadas nas configurações da tarefa.

Corrigir vulnerabilidades de software usando o assistente para Correção de vulnerabilidades

O Assistente para correção de vulnerabilidades só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

Para corrigir vulnerabilidades de software usando o assistente para Correção de vulnerabilidades:

1. No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Vulnerabilidades de software**.

   Uma página com uma lista de vulnerabilidades em softwares de terceiros instalados em dispositivos gerenciados é exibida.

2. Marque a caixa de seleção ao lado da vulnerabilidade que deseja corrigir.

3. Clique no botão **Executar o assistente para correção de vulnerabilidades**.

   O assistente para Correção de vulnerabilidades é iniciado. A página **Selecionar tarefa de correção de vulnerabilidades** exibe a lista de todas as tarefas existentes dos seguintes tipos:

   - *Instalar as atualizações necessárias e corrigir vulnerabilidades*
   - *Instalar as atualizações do Windows Update*
   - *Corrigir vulnerabilidades*

   Você não pode modificar os dois últimos tipos de tarefas para instalar novas atualizações. Para instalar novas atualizações, você só pode usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

4. Se desejar que o assistente exiba apenas as tarefas que corrigem a vulnerabilidade selecionada, ative a opção **Exibir apenas tarefas que corrigem esta vulnerabilidade**.

5. Selecione o que deseja fazer:

   - Para iniciar uma tarefa, marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Iniciar**.
   - Para adicionar uma nova regra a uma tarefa existente:

     a. Marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Adicionar regra**.

     b. Na página aberta, configure a nova regra:

     Regra para corrigir vulnerabilidades deste nível de gravidade

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.
Por padrão, esta opção está desativada.

- **Regra para corrigir vulnerabilidades por meio de atualizações do mesmo tipo que a atualização definida como recomendada para a vulnerabilidade selecionada** (disponível apenas para vulnerabilidades de software da Microsoft)

  Regra para corrigir vulnerabilidades em aplicativos por fornecedor selecionado (disponível apenas para vulnerabilidades de software de terceiros)

  Regra para corrigir uma vulnerabilidade em todas as versões do aplicativo selecionado (disponível apenas para vulnerabilidades de software de terceiros)

- **Regra para corrigir a vulnerabilidade selecionada**

  Aprovar as atualizações que corrigem esta vulnerabilidade

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

c. Clique no botão **Adicionar**.

- Para criar uma tarefa:

  a. Clique no botão **Nova tarefa**.

  b. Na página aberta, configure a nova regra:

  - Regra para corrigir vulnerabilidades deste nível de gravidade

    Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.
    Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

    Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

    Por padrão, esta opção está desativada.

- **Regra para corrigir vulnerabilidades por meio de atualizações do mesmo tipo que a atualização definida como recomendada para a vulnerabilidade selecionada** (disponível apenas para vulnerabilidades de software da Microsoft)

  Regra para corrigir vulnerabilidades em aplicativos por fornecedor selecionado (disponível apenas para vulnerabilidades de software de terceiros)

- **Regra para corrigir uma vulnerabilidade em todas as versões do aplicativo selecionado** (disponível apenas para vulnerabilidades de software de terceiros)
- **Regra para corrigir a vulnerabilidade selecionada**

  Aprovar as atualizações que corrigem esta vulnerabilidade

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

c. Clique no botão **Adicionar**.

Se você optou por iniciar uma tarefa, poderá fechar o assistente. A tarefa será concluída no modo de segundo plano. Nenhuma outra ação será necessária.

Se você escolheu adicionar uma regra a uma tarefa existente, a janela de propriedades da tarefa é aberta. A nova regra já foi adicionada às propriedades da tarefa. Você pode visualizar ou modificar a regra ou outras configurações de tarefa. Clique no botão **Salvar** para salvar as alterações.

Caso tenha optado por criar uma tarefa, continue a criar a tarefa no assistente para Novas tarefas. A nova regra adicionada no assistente para Correção de vulnerabilidades é exibida no assistente para Novas tarefas. Ao concluir o assistente, a tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades* é adicionada na lista de tarefas.

Criar a tarefa Corrigir vulnerabilidades

A tarefa *Corrigir vulnerabilidades* permite corrigir vulnerabilidades de software em dispositivos gerenciados executando Windows. É possível corrigir vulnerabilidades de software em softwares de terceiros, incluindo softwares da Microsoft.

Se você não possui uma licença do Gerenciamento de patches e vulnerabilidades, não pode criar novas tarefas do tipo *Corrigir vulnerabilidades*. Para corrigir novas vulnerabilidades, adicione-as a uma tarefa *Corrigir vulnerabilidades* existente. Recomendamos usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* em vez da tarefa *Corrigir vulnerabilidades*. A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* permite instalar várias atualizações e corrigir várias vulnerabilidades automaticamente, de acordo com as regras definidas por você.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.
   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Corrigir vulnerabilidades**.
4. Especifique o nome da tarefa que está criando.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.
6. Clique no botão **Adicionar**.

   A lista de vulnerabilidades é aberta.
7. Selecione as vulnerabilidades que deseja corrigir e, a seguir, clique em **OK**.

   As vulnerabilidades de software da Microsoft geralmente têm correções recomendadas. Nenhuma ação adicional é necessária para elas. Para vulnerabilidades em softwares de outros fornecedores, primeiro é necessário especificar uma correção do usuário para cada vulnerabilidade que deseja corrigir. Depois disso, será possível adicionar essas vulnerabilidades à tarefa *Corrigir vulnerabilidades*.
8. Especifique as configurações para reiniciar o sistema operacional:

   Não reiniciar o dispositivo

   Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

   - **Reiniciar o dispositivo**

     Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

   - **Perguntar ao usuário o que fazer**

     O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.
     Por padrão, esta opção está selecionada.

   - **Repetir aviso a cada (min.)**

Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.
Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.
Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

Reiniciar após (min.)

Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

Forçar fechamento de aplicativos em sessões bloqueadas

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.
Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

9. Especificar as configurações da conta:

- **Conta padrão**

  A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.
  Por padrão, esta opção está selecionada.

  Especificar conta

  Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

- **Conta**

  Conta sob a qual a tarefa é executada.

- **Senha**

  Senha da conta sob a qual a tarefa será executada.

Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a cria**

criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

11. Clique no botão **Concluir**.

    A tarefa é criada e exibida na lista de tarefas.

12. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

13. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

14. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Criar a tarefa Instalar atualizações necessárias e corrigir vulnerabilidades

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa lhe permite instalar várias atualizações e corrigir várias vulnerabilidades de acordo com certas regras.

Para instalar atualizações ou corrigir vulnerabilidades usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, execute uma das seguintes ações:

- Execute o assistente de Instalação das atualizações ou o assistente para Correção de vulnerabilidades.

  Crie uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

- Adicione uma regra para instalação da atualização a uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.

Para criar uma tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.

3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades**.

   Se a tarefa não for exibida, verifique se sua conta tem direitos para **Ler**, **Modificar** e **Executar** na área funcional **Administração de sistema**: **Gerenciamento de Patches e Vulnerabilidades**. Você não pode criar e configurar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* sem esses direitos de acesso.

4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

5. Dispositivos aos quais a tarefa será atribuída.

6. Especifique as regras para instalação da atualização e, então, especifique as seguintes configurações:

- **Iniciar a instalação ao reiniciar ou fechar o dispositivo**

  Se esta opção estiver ativada, as atualizações serão instaladas quando o dispositivo for reiniciado ou desligado. Caso contrário, as atualizações são instaladas segundo o agendamento.

  Use esta opção caso a instalação das atualizações afete o desempenho do dispositivo.

  Por padrão, esta opção está desativada.

- **Instalar os componentes gerais do sistema necessários**

  Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional
  Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

  Por padrão, esta opção está desativada.

- **Permitir a instalação de novas versões dos aplicativos durante atualizações**

  Se esta opção estiver ativada, as atualizações serão permitidas quando resultarem na instalação de uma nova versão de um aplicativo de software.
  Se esta opção estiver desativada, o software não será atualizado. Você poderá então instalar novas versões do software manualmente ou através de outra tarefa. Por exemplo, você pode usar esta opção se a infraestrutura da sua empresa não tiver como base uma nova versão do software ou se você quiser verificar uma atualização usando uma infraestrutura de teste.

  Por padrão, esta opção está ativada.

  A atualização de um aplicativo pode causar o funcionamento incorreto de aplicativos dependentes instalados em dispositivos cliente.

- **Baixar atualizações para o dispositivo sem instalá-las**

  Se esta opção estiver ativada, o aplicativo baixa as atualizações em um dispositivo cliente, mas não as instala automaticamente. Você então poderá instalar manualmente as atualizações baixadas.
  As atualizações da Microsoft são baixadas no armazenamento de sistema do Windows. Atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencentes à Kaspersky e à Microsoft) são baixados na pasta especificada no campo **Pasta para download de atualizações**.

  Se esta opção estiver desativada, as atualizações serão instaladas no dispositivo automaticamente.
  Por padrão, esta opção está desativada.

- **Pasta para download de atualizações**

  Esta pasta é usada para baixar atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft).

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará rastreamentos, mesmo se o rastreamento estiver desativado para o Agente de Rede no Utilitário de diagnóstico remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a gravar neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.
  Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

7. Especifique as configurações para reiniciar o sistema operacional:

   Não reiniciar o dispositivo

   Os dispositivos cliente não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

   - **Reiniciar o dispositivo**

     Os dispositivos cliente sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

   - **Perguntar ao usuário o que fazer**

     O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.
     Por padrão, esta opção está selecionada.

     Repetir aviso a cada (min.)

Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.
Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

Reiniciar após (min.)

Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

Tempo de espera antes do fechamento forçado de aplicativos nas sessões bloqueadas (min)

Os aplicativos são fechados no modo forçado quando o dispositivo for bloqueado (automaticamente, após um intervalo especificado de inatividade ou manualmente).
Se esta opção estiver ativada, os aplicativos serão forçados a fechar no dispositivo bloqueado após a expiração do intervalo de tempo especificado no campo de entrada.

Se essa opção estiver ativada, os aplicativos não serão fechados no dispositivo bloqueado.
Por padrão, esta opção está desativada.

8. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.
9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.
10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.
11. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.
12. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

Se os resultados da tarefa contiverem um aviso do erro 0x80240033 "Erro de atualização do Windows Update Agent 80240033 ("Não foi possível baixar os termos da licença.")", você poderá resolver esse problema no Registro do Windows.

Adicionar regras para instalação da atualização

Esse recurso está disponível apenas sob a licença do Gerenciamento de patches e vulnerabilidades.

Ao instalar atualizações de software ou corrigir vulnerabilidades de software usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é necessário especificar regras para a instalação da atualização. Essas regras determinam as atualizações a serem instaladas e as vulnerabilidades a serem corrigidas.

As configurações exatas dependem de você ter adicionado uma regra para todas as atualizações, para atualizações do Windows Update ou para atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software que não sejam a Kaspersky ou a Microsoft). Ao adicionar uma regra para atualizações do Windows Update ou atualizações de aplicativos de terceiros, é possível selecionar aplicativos e versões de aplicativo específicos para os quais deseja instalar atualizações. Ao adicionar uma regra para todas as atualizações, é possível selecionar atualizações específicas que deseja instalar e vulnerabilidades que deseja corrigir com a instalação das atualizações.

É possível adicionar uma regra para a instalação da atualização das seguintes maneiras:

Adicionando uma regra ao criar uma nova tarefa do tipo Instalar as atualizações necessárias e corrigir vulnerabilidades.

Adicionando uma regra na guia **Configurações do aplicativo** na janela de propriedades de uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.

- Por meio do assistente de Instalação das atualizações ou do assistente para Correção de vulnerabilidades.

Para adicionar uma nova regra para todas as atualizações:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para todas as atualizações**.

3. Na página **Critérios gerais**, use as listas suspensas para especificar as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     Instale apenas atualizações aprovadas. Isso instala apenas as atualizações aprovadas.

     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software.
Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.
Por padrão, esta opção está desativada.

4. Na página **Atualizações**, selecione as atualizações a serem instaladas:

- **Instalar todas as atualizações adequadas**

  Instale todas as atualizações de software que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Instalar apenas as atualizações da lista**

  Instale somente as atualizações de software que você seleciona manualmente da lista. Essa lista contém todas as atualizações de software disponíveis.

  Por exemplo, pode ser necessário selecionar atualizações específicas nos seguintes casos: para verificar a instalação em um ambiente de teste, para atualizar somente aplicativos críticos ou para atualizar somente aplicativos específicos.

  - **Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas**

    Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

    Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

    Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

    Por padrão, esta opção está ativada.

5. Na página **Vulnerabilidades**, selecione as vulnerabilidades que serão corrigidas instalando as atualizações selecionadas:

- **Corrigir todas as vulnerabilidades que correspondem a outros critérios**

  Corrija todas as vulnerabilidades que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **C**

Corrija somente as vulnerabilidades que você seleciona manualmente da lista. Essa lista contém todas as vulnerabilidades detectadas.

Por exemplo, pode ser necessário selecionar vulnerabilidades específicas nos seguintes casos: para verificar a correção em um ambiente de teste, para corrigir vulnerabilidades somente em aplicativos críticos ou para corrigir vulnerabilidades somente em aplicativos específicos.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Para adicionar uma nova regra para atualizações do Windows Update:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para o Windows Update**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

   Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

   Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.
   Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

   Por padrão, esta opção está desativada.

   - Corrigir vulnerabilidades com um nível de gravidade do MSRC igual ou maior do que

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.
Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.
5. Na página **Categorias de atualizações**, selecione as categorias das atualizações a serem instaladas. Essas categorias são iguais às no Catálogo do Microsoft Update. Por padrão, todas as categorias estão selecionadas.
6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Para adicionar uma nova regra para as atualizações de aplicativos de terceiros:

1. Clique no botão **Adicionar**.
   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
2. Na página **Tipo de regra**, selecione **Regra para atualizações de terceiros**.
3. Na página **Critérios gerais**, especifique as seguintes configurações:

- Conjunto de atualizações a instalar

  Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

  - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.

    Instalar todas as atualizações (exceto as recusadas). Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.

    Instalar todas as atualizações (incluindo as recusadas). Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

- Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção Configurações da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Selecionar as correções do usuário para vulnerabilidades em software de terceiros

Para usar a tarefa *Corrigir vulnerabilidades*, você deve especificar manualmente as atualizações de software para corrigir as vulnerabilidades em softwares de terceiros listadas nas configurações da tarefa. A tarefa *Corrigir vulnerabilidades* usa as correções recomendadas para o software da Microsoft e as correções do usuário para outros softwares de terceiros. *Correções do usuário* são atualizações de software para corrigir as vulnerabilidade que o administrador especifica manualmente para instalação.

Para selecionar correções do usuário para vulnerabilidades em software de terceiros:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   A página exibe a lista de vulnerabilidades de software detectadas nos dispositivos cliente.

2. Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade de software para o qual você deseja especificar uma correção do usuário.

   A janela Propriedades da vulnerabilidade é aberta.

3. No painel esquerdo, selecione a seção **Correções do usuário e outras correções**.

   A lista de correções do usuário para a vulnerabilidade de software selecionada é exibida.

4. Clique em **Adicionar**.
   A lista de pacotes de instalação disponíveis é exibida. A lista de pacotes de instalação exibidos corresponde à lista **Operações → Repositórios → Pacotes de instalação**. Se você não criou um pacote de instalação contendo a correção do usuário para a vulnerabilidade selecionada, poderá criar o pacote agora iniciando o Assistente de novo pacote.

5. Selecione um pacote de instalação (ou pacotes) que contenha uma correção (ou correções) do usuário para a vulnerabilidade no software de terceiros.

6. Clique em **Salvar**.

Os pacotes de instalação que contenham correções do usuário para a vulnerabilidade de software são especificados. Quando a tarefa *Corrigir vulnerabilidades* for iniciada, o pacote de instalação será instalado e a vulnerabilidade de software será corrigida.

Visualizar informações sobre vulnerabilidades de software detectadas em todos os dispositivos gerenciados

Depois de verificar o software em dispositivos gerenciados quanto a vulnerabilidades, você pode visualizar a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados.

Para exibir a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados,

No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Vulnerabilidades de software**.

A página exibe a lista de vulnerabilidades de software detectadas nos dispositivos cliente.

Você também pode gerar e visualizar o Relatório de vulnerabilidades.

Você pode especificar um filtro para visualizar a lista de vulnerabilidades de software. Clique no ícone **Filtro** ( ) no canto superior direito da lista de vulnerabilidades de software para gerenciar o filtro. Você também pode selecionar um dos filtros predefinidos na lista suspensa **Filtros predefinidos** acima da lista de vulnerabilidades de software.

Você pode obter informações detalhadas sobre qualquer vulnerabilidade na lista.

Para obter informações sobre uma vulnerabilidade de software:

Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade.

A janela de propriedades da vulnerabilidade de software é aberta.

Visualizar informações sobre vulnerabilidades de software detectadas no dispositivo gerenciado selecionado

Você pode visualizar informações sobre vulnerabilidades de software detectadas no dispositivo gerenciado selecionado que executa o Windows.

Para visualizar uma lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo para o qual você deseja visualizar as vulnerabilidades de software detectadas.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Na janela de propriedades do dispositivo selecionado selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Vulnerabilidades de software**.
   Se deseja visualizar ver somente as vulnerabilidades de software que podem ser corrigidas, marque a caixa **Exibir somente vulnerabilidades que podem ser corrigidas.**

A lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado é exibida.

Para visualizar as propriedades da vulnerabilidade de software selecionada,

Clique no link com o nome da vulnerabilidade de software na lista de vulnerabilidades de software.

A janela de propriedades de vulnerabilidade de software selecionada é exibida.

Visualizar as estatísticas de vulnerabilidades em dispositivos gerenciados

Você pode visualizar estatísticas para cada vulnerabilidade de software em dispositivos gerenciados. Estatísticas são representadas como um diagrama. O diagrama exibe o número de dispositivos com os seguintes status:

- *Ignorado em: <número de dispositivos>*. O status será atribuído se, nas propriedades da vulnerabilidade, você tiver definido manualmente a opção para ignorá-la.
- *Corrigido em: <número de dispositivos>*. O status será atribuído se a tarefa para corrigir a vulnerabilidade for concluída com êxito.
- *Correção agendada em: <número de dispositivos>*. O status será atribuído se você tiver criado a tarefa para corrigir a vulnerabilidade, mas a tarefa ainda não foi executada.
- *Correção aplicada em: <número de dispositivos>*. O status será atribuído se você tiver selecionado manualmente uma atualização de software para corrigir a vulnerabilidade, mas essa atualização de software não tiver corrigido a vulnerabilidade.
- *Correção necessária em: <número de dispositivos>*. O status será atribuído caso a vulnerabilidade seja corrigida apenas na parte dos dispositivos gerenciados, e é necessário que ela seja corrigida no restante dos dispositivos gerenciados.

Para exibir as estatísticas de uma vulnerabilidade nos dispositivos gerenciados:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.
   A página exibe uma lista de vulnerabilidades nos aplicativos detectados nos dispositivos gerenciados.

2. Selecione a caixa de seleção ao lado da vulnerabilidade necessária.

3. Clique no botão **Estatísticas de vulnerabilidades em dispositivos**.

O diagrama dos status de vulnerabilidade é exibido. Clicar em um status abre uma lista de dispositivos nos quais a vulnerabilidade tem o status selecionado.

Exportar a lista de vulnerabilidades de software para um arquivo

Você pode exportar a lista de vulnerabilidades exibidas para os arquivos CSV ou TXT. Você pode usar esses arquivos, por exemplo, para enviá-los ao seu gerente de segurança de informações ou para armazená-los para fins de estatística.

Para exportar a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados para um arquivo de texto:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   A página exibe uma lista de vulnerabilidades nos aplicativos detectados nos dispositivos gerenciados.

2. Clique no botão **Exportar linhas para arquivo TXT** ou **Exportar linhas para arquivo CSV**, dependendo do formato de exportação preferido.

O arquivo que contém a lista de vulnerabilidades de software é baixado no dispositivo que você está usando no momento.

Para exportar a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado para um arquivo de texto:

1. Abra a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado.

2. Selecione as vulnerabilidades de software que você deseja exportar.
   Pule esta etapa se desejar exportar uma lista completa de vulnerabilidades de software detectadas no dispositivo gerenciado.

   Se você deseja exportar a lista completa de vulnerabilidades de software detectadas no dispositivo gerenciado, apenas as vulnerabilidades exibidas na página atual serão exportadas.

3. Clique no botão **Exportar linhas para arquivo TXT** ou **Exportar linhas para arquivo CSV**, dependendo do formato de exportação preferido.

O arquivo que contém a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado é baixado no dispositivo que você está usando no momento.

Ignorar as vulnerabilidades de software

Você pode ignorar as vulnerabilidades do software a ser corrigidas. Os motivos para ignorar vulnerabilidades de software, por exemplo, os seguintes:

A vulnerabilidade de software não é considerada crítica para sua organização.

- Você entende que a correção de vulnerabilidade do software pode danificar os dados relacionados ao software que exigia a correção da vulnerabilidade.
- Você tem certeza de que a vulnerabilidade do software não é perigosa para a rede da sua organização porque usa outras medidas para proteger seus dispositivos gerenciados.

Você pode ignorar uma vulnerabilidade de software em todos os dispositivos gerenciados ou apenas nos dispositivos gerenciados selecionados.

Para ignorar uma vulnerabilidade de software em todos os dispositivos gerenciados:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

A página exibe a lista de vulnerabilidades de software detectadas nos dispositivos gerenciados.

2. Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade de software que você deseja ignorar.

   A janela Propriedades de vulnerabilidade do software é aberta.

3. Na guia **Geral**, ative a opção **Ignorar vulnerabilidade**.

4. Clique no botão **Salvar**.

   A janela de propriedades de vulnerabilidade do software é fechada.

A vulnerabilidade de software é ignorada em todos os dispositivos gerenciados.

Para ignorar uma vulnerabilidade de software no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo no qual você deseja ignorar uma vulnerabilidade de software.
   A janela Propriedades do dispositivo é aberta.

3. Na janela Propriedades do dispositivo, selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Vulnerabilidades de software**.

   A lista de vulnerabilidades de software detectadas no dispositivo é exibida.

5. Na lista de vulnerabilidades de software, selecione a vulnerabilidade que você deseja ignorar no dispositivo selecionado.

   A janela Propriedades de vulnerabilidade do software é aberta.

6. Na janela de propriedades da vulnerabilidade de software, na guia **Geral**, ative a opção **Ignorar vulnerabilidade**.

7. Clique no botão **Salvar**.

   A janela de propriedades de vulnerabilidade do software é fechada.

8. Feche a janela Propriedades do dispositivo.

A vulnerabilidade de software é ignorada no dispositivo selecionado.

A vulnerabilidade de software ignorada não será corrigida após a conclusão das tarefas *Corrigir vulnerabilidades* ou *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Você pode excluir vulnerabilidades de software ignoradas da lista de vulnerabilidades por meio do filtro.

Gerenciando a execução de aplicativos em dispositivos cliente

Esta seção descreve os recursos do Kaspersky Security Center relacionados ao gerenciamento de aplicativos executados nos dispositivos cliente.

Cenário: Gerenciamento de Aplicativos

Você pode gerenciar a inicialização de aplicativos nos dispositivos do usuário. Você pode permitir ou bloquear a execução de aplicativos em dispositivos gerenciados. Essa funcionalidade é realizada pelo componente Controle de Aplicativos. Você pode gerenciar aplicativos instalados em dispositivos Windows ou Linux.

Para sistemas operacionais baseados em Linux, o componente Controle de Aplicativos está disponível a partir do Kaspersky Endpoint Security 11.2 for Linux.

Pré-requisitos

- O Kaspersky Security Center está implementado em sua organização.
- A política do Kaspersky Endpoint Security for Windows ou do Kaspersky Endpoint Security for Linux está criada e ativa.

Fases

O cenário de uso do Controle de Aplicativos prossegue em fases:

1. **Formar e visualizar a lista de aplicativos em dispositivos cliente**

   Esta etapa ajuda a descobrir quais aplicativos estão instalados nos dispositivos gerenciados. Você pode exibir a lista de aplicativos e decidir quais aplicativos deseja permitir e quais deseja proibir, de acordo com as políticas de segurança de sua organização. As restrições podem estar relacionadas às políticas de segurança da informação em sua organização. Você pode pular esta fase se souber exatamente quais aplicativos estão instalados nos dispositivos gerenciados.

   Instruções de como proceder:

   - Console de Administração: Exibir o registro dos aplicativos
   - Kaspersky Security Center Web Console: Obter e visualizar uma lista de aplicativos instalados nos dispositivos cliente

2. **Formar e visualizar a lista de arquivos executáveis em dispositivos cliente**

   Esta etapa ajuda a descobrir quais arquivos executáveis são encontrados nos dispositivos gerenciados. Exiba a lista de arquivos executáveis e compare-a com a lista de arquivos executáveis permitidos e proibidos. As restrições sobre a utilização de arquivos executáveis podem estar relacionadas às políticas de segurança da informação em sua organização. Você pode pular esta fase se souber exatamente quais arquivos executáveis estão instalados nos dispositivos gerenciados.

   Instruções de como proceder:

   - Console de administração: Inventário de arquivos executáveis
   - Kaspersky Security Center Web Console: Obtendo e visualizando uma lista de arquivos executáveis armazenados nos dispositivos cliente

3. **Criar categorias de aplicativo para os aplicativos usados na sua organização**

Analise a lista de aplicativos e arquivos executáveis armazenados nos dispositivos gerenciados. Baseando-se na análise, crie categorias de aplicativo. É recomendável criar uma categoria "Aplicativos de trabalho" que cubra o conjunto padrão de aplicativos usados na sua organização. Se diferentes grupos de segurança usarem conjuntos diferentes de aplicativos em seu trabalho, uma categoria de aplicativo poderá ser criada para cada grupo de segurança.

Dependendo do conjunto de critérios para criar uma categoria de aplicativo, você pode criar categorias de aplicativo de três tipos.

Instruções de como proceder:

- Console de Administração: Criação de uma categoria de aplicativo com conteúdo adicionado manualmente, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir de dispositivos selecionados, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir da pasta selecionada.
- Kaspersky Security Center Web Console: Criação de uma categoria de aplicativo com conteúdo adicionado manualmente, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir de dispositivos selecionados, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir da pasta específica.

4 Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security

Configure o componente Controle de Aplicativos na política do Kaspersky Endpoint Security usando as categorias de aplicativos criadas na etapa anterior.

Instruções de como proceder:

- Console de Administração: Configurar o gerenciamento da inicialização do aplicativo em dispositivos cliente
- Kaspersky Security Center Web Console: Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows

5 Ativar o componente Controle de Aplicativos no modo de teste

Para garantir que as regras do Controle de Aplicativos não bloqueiem os aplicativos necessários para o trabalho do usuário, é recomendável ativar o teste das regras do Controle de Aplicativos e analisar a sua operação após a criação de novas regras. Quando o teste está ativado, o Kaspersky Endpoint Security for Windows não bloqueia os aplicativos cuja inicialização é proibida pelas regras do Controle de Aplicativos, mas envia notificações sobre a inicialização ao Servidor de Administração.

Ao testar as regras do Controle de Aplicativos, é recomendável realizar as seguintes ações:

- Determine o período de teste. O período de teste pode variar de vários dias a dois meses.
- Examine os eventos resultantes do teste da operação do Controle de Aplicativos.

Instruções para o Kaspersky Security Center Web Console: Configurar o componente Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows. Siga estas instruções e ative a opção **Modo de teste** no processo de configuração.

6 Alterar as configurações das categorias de aplicativos do componente Controle de Aplicativos

Se necessário, faça alterações nas configurações do Controle de Aplicativos. Com base nos resultados do teste, você pode adicionar arquivos executáveis relativos a eventos do componente Controle de Aplicativos a uma categoria de aplicativo com conteúdo adicionado manualmente.

Instruções de como proceder:

- Console de Administração: Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos
- Kaspersky Security Center Web Console: Adicionar arquivos executáveis relacionados a eventos à categoria de aplicativo

Aplicar as regras do Controle de Aplicativos no modo de operação

Após as regras de Controle de Aplicativos terem sido testadas e a configuração das categorias de aplicativo estar concluída, você pode aplicar as regras do Controle de Aplicativos no modo de operação.

Instruções para o Kaspersky Security Center Web Console: Configurar o componente Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows. Siga estas instruções e desative a opção **Modo de teste** no processo de configuração.

Verificar a configuração do Controle de Aplicativos

Certifique-se de ter feito o seguinte:

- Categorias de aplicativos criadas.
- Configurado o Controle de Aplicativos usando as categorias de aplicativos.
- Aplicado as regras do Controle de Aplicativos no modo de operação.

Resultados

Quando o cenário estiver concluído, a inicialização dos aplicativos nos dispositivos gerenciados será controlada. Os usuários podem iniciar apenas aqueles aplicativos permitidos na sua organização e não podem iniciar aplicativos proibidos na sua organização.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows

  Ajuda on-line do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Sobre o Controle de Aplicativos

O componente Controle de Aplicativos monitora as tentativas do usuário para iniciar aplicativos e regula a inicialização de aplicativos usando as regras do Controle de Aplicativos.

> O componente Controle de Aplicativos está disponível para o Kaspersky Endpoint Security for Windows e para o Kaspersky Security for Virtualization Light Agent. Todas as instruções nesta seção descrevem a configuração do Controle de Aplicativos para o Kaspersky Endpoint Security for Windows.

A inicialização de aplicativos cujas configurações não correspondem a nenhuma das regras do Controle de Aplicativos é regulada pelo modo de operação selecionado do componente:

- *Lista de bloqueio*. O modo é usado se você deseja permitir a inicialização de todos os aplicativos, exceto os aplicativos especificados nas regras de bloqueio. Este modo é selecionado por padrão.

  Lista de permissão. O modo é usado se você deseja bloquear a inicialização de todos os aplicativos, exceto os aplicativos especificados nas regras de permissão.