República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) **PI 0712431-7 A2**

BRPI0712431A2

(22) Data de Depósito: 15/03/2007
(43) Data da Publicação: 10/07/2012
(RPI 2166)

(51) Int.Cl.:
G06F 12/16
G06F 21/22

(54) Título: CHECAGEM DE VÍRUS E FILTRAGEM DE REPRODUÇÃO COMBINADAS.

(30) Prioridade Unionista: 02/06/2006 US 11/421,996

(73) Titular(es): Microsoft Corporation

(72) Inventor(es): Robert M. Fries, Shiraz M. Somji

(74) Procurador(es): NELLIE ANNE DAIEL-SHORES

(86) Pedido Internacional: PCT US2007006598 de 15/03/2007

(87) Publicação Internacional: WO 2007/142715de 13/12/2007

(57) Resumo: CHECAGEM DE VÍRUS E FILTRAGEM DE REPRODUÇÃO COMBINADAS. Dados nos sistemas de cópia de proteção podem ser eficientemente protegidos contra vírus, mesmo se as definições para certos vírus são encontradas após os dados infectados terem sido copiados por proteção em um servidor de reserva. Em uma implementação, um filtro combinado que inclui componentes de filtro antivírus e de reprodução pode identificar e processar chamadas de sistema I/O (por exemplo, incluindo gravações de arquivo). Se um vírus está presente, o componente antivírus do filtro combinado pode marcar o arquivo e/ou a gravação de arquivo (e limpar a gravação de arquivo/arquivo), e passar essa informação para o componente de reprodução. Se a gravação de arquivo é associada com um arquivo a ser copiado por proteção, o componente de reprodução pode então passar, junto com os indicadores de filtro antivírus, uma cópia da gravação de arquivo, o servidor de reserva pode também identificar se as versões anteriores do arquivo armazenadas no servidor de reserva podem ter sido infectadas, e pode assim executar quaisquer ações apropriadas.

"CHECAGEM DE VÍRUS E FILTRAGEM DE REPRODUÇÃO COMBINADAS"

FUNDAMENTOS

FUNDAMENTOS E TÉCNICA RELEVANTE

Devido pelo menos em parte a ubiqüidade de arquivos eletrônicos, pessoas e organizações igualmente têm necessidade de proteger arquivos eletrônicos em uma base regular. Uma forma de proteger arquivos eletrônicos é periodicamente fazer uma cópia de proteção de arquivos para criar uma restauração confiável para os dados. Apesar de em um nível individual ou em um nível empresarial, sistemas de cópia de proteção convencionais para fazer isso podem incluir um ou mais filtros de reprodução que identificam se gravações de dados são feitas para serem copiados como proteção em um servidor de reserva. Por exemplo, um usuário pode fazer uma ou mais gravações de dados, o filtro de reprodução pode então interceptar cada uma das gravações, e então determinar se as gravações pertencem aos dados que estão previstos para serem protegidos (isto é, copiados). Se o arquivo é previsto para ser protegido, o filtro de reprodução pode então passar a gravação para um arquivo de registro contendo múltiplas de tais gravações.

O arquivo de registro (ou uma cópia correspondente do mesmo) pode então ser enviado para um ou mais servidores de reserva. Por exemplo, um usuário em um computador pessoal pode rodar um ou mais processos de cópia de proteção que reproduzem o arquivo de registro e/ou qualquer outro de tais dados identificados ao um ou mais locais ou alocações de armazenamento remoto, tal como aqueles associados com um servidor de reserva particular. De forma similar, um ou mais agentes de reprodução em um servidor de produção podem programar uma cópia de proteção de um arquivo de registro no servidor de produção e então passar as novas gravações de dados por uma ou mais das alocações de armazenamento em um servidor de reserva. Em um ponto posterior, o usuário (ou administrador do servidor de produção) pode então ser capaz de requerer os dados associados com o arquivo de registro reproduzido a partir do servidor de reserva.

Fazer uma cópia de proteção de dados dessa maneira, contudo, é somente uma forma de proteger dados. Outras formas de proteger dados incluem, por exemplo, o escaneamento de vírus. Em particular, é bem conhecido que vírus de computador podem destruir dados e causar danos em sistemas de computador, que podem levar a adicional perda de arquivos não originalmente infectados, para minimizar tais ameaças, portanto, um usuário ou administrador pode instalar um ou mais programas de antivírus em um ou mais sistemas de computador. Uma forma em que softwares convencionais antivírus podem trabalhar é através de um ou mais filtros antivírus que identificam gravações em um arquivo particular, e então escaneam a gravação para determinar se as gravações contêm um vírus conhecido. A habilidade do software antivírus de reconhecer um vírus é tipicamente baseada em um conjunto de definições antivírus, que o filtro antivírus verifica quando está

escaneando gravações de arquivo. Como tal, a possibilidade de um filtro antivírus identificar o vírus irá depender de como são feitas as atualizações das definições do antivírus. Especificamente, se o software antivírus não tiver sido recentemente atualizado, os filtros antivírus podem identificar que um arquivo particular (ou gravações de arquivo) está limpo,mesmo que o arquivo possa realmente conter um vírus recém criado.

Uma pessoa pode reconhecer, portanto, que uma entidade (pessoa ou organização, etc.) pode instalar um número de programas diferentes para proteger dados, que podem incluir um número de filtros de software diferentes operando de forma independente um do outro. Em um exemplo convencional, cada programa de software que tem um filtro irá primeiramente registrar aquele filtro (por exemplo, um filtro antivírus e/ou um filtro de reprodução) com um gerenciador de filtro operando o sistema. O gerenciador de filtro, por sua vez, passa cada uma das gravações de arquivo por cada filtro quando, ou se, apropriado. De forma geral, pode ser difícil configurar como cada filtro de software pode ser registrado junto ao gerenciador de filtro para assegurar qualquer ordenamento necessário. Como resultado, pode ser que o gerenciador de filtro envie as gravações de arquivo para um filtro de reprodução e, então, para um filtro antivírus. Em outros casos, claro, o gerenciador de filtro pode primeiramente enviar as gravações de arquivo para o filtro antivírus antes de enviar as mesmas para o filtro de reprodução.

Infelizmente, mesmo com o ordenamento específico dos filtros, pode ser difícil configurar, o ordenamento dos filtros pode ter um impacto significante em como os dados são protegidos e/ou copiados como proteção. Por exemplo, um problema particularmente sensível com organizações que programam sistemas de cópia de proteção é que a falha em encontrar certos vírus eletrônicos pode significar potencialmente maiores proliferações do vírus durante os processos de cópia de proteção. Esse problema pode ser particularmente agudo onde, por exemplo, um filtro de reprodução recebe gravações de arquivo e envia as mesmas para um arquivo de registro, antes que àquelas gravações de arquivo possam ser revisadas por um filtro antivírus. Tal ordenamento de filtros pode significar em alguns casos que um arquivo infectado pode não ser tratado ou mesmo identificado como infectado até que seja tarde, ou após o arquivo ter passado para um servidor de reserva.

Contrariamente, mesmo que tenha sido possível assegurar que o filtro antivírus recebeu as gravações de arquivo antes de um filtro de reprodução, não necessariamente isso pode resolver todos os problemas potenciais. Por exemplo, um arquivo infectado em um sistema de computador pode não ser detectado se a definição de antivírus usada pelo filtro de antivírus estiver desatualizada, tal como se uma definição não tiver sido criada para o vírus infectando o arquivo. Como tal, o arquivo pode ter sido reproduzido uma ou mais vezes por um filtro de reprodução, mesmo que tenha sido primeiramente checado por um filtro antivírus. Isso pode significar, portanto, que diversas cópias da cópia de proteção

podem existir da versão infectada do arquivo no servidor de reserva. Quando as definições do antivírus são atualizadas pelo filtro antivírus para incluir esse vírus particular, o filtro de antivírus pode, em última instância, identificar que as gravações de arquivo estão infectadas.

Na maioria dos casos, contudo, o filtro antivírus pode simplesmente apagar ou deletar as gravações de arquivo infectadas e/ou inteiramente o arquivo base correspondente no servidor de produção. Infelizmente, o filtro de reprodução geralmente não irá ter qualquer conhecimento da identificação do vírus e/ou das ações de limpeza do filtro de antivírus, e assim irá simplesmente reproduzir as gravações de arquivo limpas. O arquivo reproduzido e/ou as gravações de arquivo para o arquivo limpo podem então ser passadas para o arquivo de registro e/ou, de outra forma, reproduzidas de volta para o servidor de reserva como é normalmente feito. Como tal, o servidor de reserva pode não estar ciente de que o arquivo tenha sido infectado e pode simplesmente arquivar as atualização de cópia de proteção do arquivo (isto é, incluindo as novas gravações de arquivo) juntamente com os dados de arquivo anteriormente infectados. Assim, mesmo que o filtro de antivírus possa ser posicionando na frente do filtro de reprodução em um servidor de produção, não existe garantia de que os dados infectados no servidor de reserva tenham sido limpos.

Assim, existe um grande número de dificuldades associadas com a abordagem de informação de antivírus dentro dos sistemas de cópia de proteção.

BREVE SUMÁRIO

Implementações da presente invenção proporcionam sistema, métodos e produtos de programa de computador que efetivamente propagam informação antivírus através dos dados em um ambiente de cópia de proteção. Em pelo menos uma implementação, por exemplo, um filtro comum compreende componentes de filtro antivírus e de reprodução. O filtro comum pode receber gravações de arquivo e passar as gravações de arquivo para o componente de antivírus. O componente de antivírus escaneia cada gravação de arquivo e passa cada uma das gravações de arquivo escaneadas juntamente com qualquer informação de antivírus apropriada para a gravação de arquivo para o componente de filtro de reprodução do filtro comum. O filtro de reprodução pode assim reproduzir certas gravações de arquivo para um arquivo de registro em uma maneira que mantenha qualquer informação de vírus que possa ter sido anteriormente detectada. Como tal, tanto um servidor de produção quando um servidor de reserva pode identificar se os dados de cópia de proteção recebidos, ou os dados de cópia de proteção recebidos anteriormente podem receber atenção do antivírus.

Por exemplo, um método exemplificativo a partir da perspectiva de um servidor de produção do gerenciador de processos de filtragem de vírus e de cópia de proteção através de um filtro comum pode envolver a identificação de uma ou mais gravações de arquivos através do filtro comum. Adicionalmente, o método pode envolver o escaneamento das uma

ou mais gravações de arquivo identificadas no filtro comum de acordo com uma ou mais definições de vírus. O método pode também envolver comparação das uma ou mais gravações de arquivo escaneadas identificadas no filtro comum com uma ou mais políticas de reprodução. Adicionalmente, o método pode envolver enviar uma cópia da pelo menos uma ou mais gravações de arquivo escaneadas para o arquivo de registro, de tal modo que o pelo menos uma gravação de arquivo seja reproduzida para um servidor de reserva.

Contrariamente, um método exemplificativo da perspectiva de um servidor de reserva do gerenciamento de dados reproduzidos de acordo com um ou mais indicadores de vírus pode envolver o recebimento de um ou mais dados de cópia de proteção a partir do um ou mais servidores de produção. Adicionalmente, o método pode envolver identificar um ou mais indicadores de vírus no um ou mais dados de cópia de proteção recebidos. Em tal caso, o um ou mais indicadores de vírus pode identificar que pelo menos um das uma ou mais cópias de proteção de dados é associada com os dados infectados. O método pode também envolver a identificação de uma ou mais políticas para o servidor de reserva. Em geral, a uma ou mais políticas podem identificar uma ou mais ações de resposta que correspondem aos um ou mais indicadores de vírus. Adicionalmente, o método pode envolver executar quaisquer de uma ou mais ações de resposta de acordo com a uma ou mais políticas.

Esse Sumário é provido para introduzir uma seleção de conceitos em uma forma simplificada que serão adicionalmente descritos abaixo na Descrição Detalhada. Esse Sumário não é pretendido para identificar características chaves ou características essenciais da matéria reivindicada nem é pretendido para ser usado como um auxiliar na determinação do escopo da matéria reivindicada.

Características adicionais e vantagens da invenção serão colocadas na descrição a seguir, e em parte serão óbvias a partir da descrição ou podem ser compreendidas pela prática da invenção. Essas características e vantagens da invenção podem ser compreendidas e obtidas por meio de instrumentos e combinações particularmente apontadas nas reivindicações anexas. Essas e outras características da presente invenção se tornarão mais completamente aparentes a partir da descrição a seguir e das reivindicações anexas, ou podem ser entendidas pela prática da invenção como será colocado daqui por diante.

BREVE DESCRIÇÃO DOS DESENHOS

De modo a descrever a maneira na qual podem ser obtidas as acima mencionadas vantagens e outras vantagens e características da invenção, uma descrição mais particular da invenção brevemente descrita acima será feita com referência às modalidades específicas da mesma que são ilustradas nos desenhos anexos. Deve ser entendido que esses desenhos ilustram somente modalidades típicas da invenção e não devem, portanto,

ser considerados como sendo limitativos do seu escopo, a invenção irá ser descrita e explicada com especificidade e detalhes adicionais através do uso dos desenhos anexos, nos quais:

A Figura 1A ilustra um diagrama esquemático geral de acordo com uma implementação da presente invenção, na qual um servidor de produção escaneia gravações de arquivo através de um filtro antivírus/de reprodução comum e provê essas gravações de arquivo para um servidor de reserva;

A Figura 1B ilustra uma vista esquemática mais detalhada dos processos no servidor de produção de acordo com uma implementação da presente invenção, na qual o filtro antivírus/de reprodução comum marca a uma ou mais gravações de arquivo recebidas com um ou mais indicadores de vírus antes de enviar as gravações de arquivo para um arquivo de registro;

A Figura 1C ilustra um diagrama esquemático no qual o servidor de reserva recebe uma ou mais cópias de proteção de dados que incluem um ou mais indicadores de vírus, e executa uma ou mais ações de resposta correspondentes nas mesmas de acordo com uma implementação da presente invenção; e

A Figura 2 ilustra um fluxograma de métodos a partir das perspectivas de um servidor de produção e de um servidor de reserva para propagar as gravações de antivírus para as gravações de arquivo através de um sistema de cópia de proteção, de acordo com uma implementação da presente invenção.

DESCRIÇÃO DETALHADA

Implementações da presente invenção se estendem a sistemas, métodos e produtos de programa de computador que efetivamente propagam informação de antivírus através de dados em um ambiente de cópia de proteção. Em pelo menos uma implementação, por exemplo, um filtro comum compreende componentes de filtro antivírus e de reprodução. O filtro comum pode receber gravações de arquivo e passar as gravações de arquivo para o componente antivírus. O componente antivírus escaneia cada uma das gravações de arquivo, e passa cada uma das gravações de arquivo escaneadas junto com qualquer informação antivírus apropriada para a gravação de arquivo para os componentes de filtro de reprodução do filtro comum. O filtro de reprodução pode assim replicar certas gravações de arquivo para um arquivo de registro em uma maneira que mantenha qualquer informação de vírus que possa ter sido anteriormente detectada. Como tal, tanto um servidor de produção quando um servidor de reserva pode identificar se os dados de cópia de proteção recebidos, ou os dados de cópia de proteção recebidos anteriormente devem receber atenção antivírus.

Como será entendido mais completamente aqui, essas e outras características da presente invenção podem ser obtidas usando qualquer número de componentes, módulos e

esquemas. Por exemplo, implementações da presente invenção são descritas abaixo primariamente a partir da perspectiva de um servidor de produção e de um servidor de reserva, que comunicam dados criados e/ou modificados no servidor de produção. Tal estabelecimento, contudo, não é necessariamente requerido em todas as implementações. Em particular, o servidor de produção pode ser representativo de um sistema de computador pessoal em alguns casos em que é copiado para proteção diretamente por um outro sistema de computador, não importando se tais sistemas de computador podem ser tidos propriamente como "servidor".

Adicionalmente, implementações da presente invenção são descritas primariamente aqui em termos das ações tomadas por um filtro "comum", que proporciona uma interface comum, única, através da qual a funcionalidade dos componentes do tipo filtro antivírus e de reprodução é acessada. Esse filtro comum pode também assim ser descrito como um filtro "combinado", que é um filtro que proporciona funções combinadas de um filtro antivírus e de um filtro de reprodução. De qualquer modo, e como será apreciado aqui, devido a um filtro único poder ser construído tanto componentes de filtragem antivírus quanto de reprodução, o desenvolvedor que cria o filtro único pode projetar o ordenamento para cada componente. Isto é, o desenvolvedor pode configurar o filtro de modo que as chamadas do sistema de entrada/saída ("I/O") são cuidadas primeiro por, por exemplo, os componentes antivírus, e a seguir tratadas pelo componente de reprodução. Como tal, somente um filtro único, tal como o filtro comum, irá necessitar ser registrado com um gerenciador de filtro mediante o manejo das atividades de filtragem de antivírus e de reprodução.

Uma pessoa deve entender, contudo, que um filtro comum/combinado é simplesmente uma forma de obter uma ou mais implementações da presente invenção. Em implementações alternativas, por exemplo, um desenvolvedor pode criar filtros separados de antivírus e de reprodução que têm dispositivos apropriados para identificar e comunicar um com o outro em uma ordem particular. Em particular, os filtros antivírus e de reprodução podem ser instalados separadamente em um servidor de produção, mas em uma ordem específica, para assegurar uma ordem particular com um gerenciador de filtro. Os filtros antivírus e de reprodução podem então ser providos com um ou mais dispositivos para identificar e comunicar um com outro através, por exemplo, de um canal de comunicação fora de faixa. Como tal, uma pessoa irá apreciar, após a leitura do relatório descritivo a seguir e das reivindicações, que existe um número de formas de praticar os princípios aqui descritos.

Em todo caso, a Figura 1A ilustra um diagrama esquemático geral de um sistema de cópia de proteção 100 no qual um servidor de produção 105 recebe uma ou mais gravações de arquivo, escaneia essas gravações de arquivo com os componentes antivírus e de reprodução de um filtro comum, e passa uma ou mais dessas gravações para o

servidor de reserva 110. De uma forma geral, uma gravação de arquivo (por exemplo, 103, 107) pode ser gerada a qualquer tempo em que um usuário (ou outra entidade) cria dados, modificações ou emendas para os dados existentes ou similares. Um servidor de produção 105 pode então interceptar ou "filtrar" cada uma dessas gravações de arquivo usando qualquer número de mecanismos. Em pelo menos uma implementação da presente invenção, por exemplo, o servidor de produção 105 intercepta e recebe cada gravação de arquivo 103, 107 através de um gerenciador de filtro 115.

Geralmente, o gerenciador de filtro 115 pode ser configurado para interceptar cada chamada de sistema I/O no servidor de produção 105, e passar cada uma de tal chamada para um ou mais filtros registrados (por exemplo, filtros 125, 127, Figura 1B). Tais chamadas podem inclui qualquer número de pedidos de sistema, tal como "abrir arquivo", "fechar arquivo", bem como várias gravações, remoções, alterações em arquivos, e assim por diante. Especificamente, cada mudança em um arquivo pode gerar uma chamada de sistema I/O, e pode ter dez ou centenas de chamadas de sistema I/O em alguns casos para a qual o gerenciador de filtro 115 pode ser configurado para interceptar. Contudo, o gerenciador de filtro 115 configurado irá, no máximo, distribuir as várias chamadas que ele interceptar para qualquer número de filtros que são registrados no mesmo. Em particular, algum filtro, tal como um filtro antivírus, pode ser configurado para receber todas as chamadas interceptadas pelo gerenciador de filtro 115, enquanto outros filtros podem somente ser configurados para receber certos tipos de chamadas no sistema I/O.

Em pelo menos uma implementação da presente invenção, o gerenciador de filtro 115 pode ser configurado para passar todas as chamadas de sistema (por exemplo, gravações de arquivo) para o filtro combinado antivírus ("AV") e de reprodução 125 (ou filtro "combinado" ou "comum" 125). Por exemplo, o gerenciador de filtro 115 recebe gravações de arquivo 103, 107, e passa cada uma dessas gravações de arquivo para o filtro comum 125. Como será entendido mais completamente aqui, o filtro comum 125 pode então escanear cada gravação de arquivo recebida por vírus, e se apropriado, passar uma cópia de qualquer um ou mais dessas gravações de arquivo para o arquivo de registro 130. De uma maneira geral, um "arquivo de registro", tal como um arquivo de registro 130, geralmente compreende um ou mais arquivos eletrônicos configurados para manter cópias de todas as mudanças em dados específicos (criação, remoção, modificação, etc.) para um volume particular do servidor de produção 105. Por exemplo, um arquivo de registro 130 pode representar todas as mudanças para o volume 120 por um tempo específico.

O servidor de reserva 110 pode então fazer a cópia de proteção do arquivo de registro 130 (bem como de quaisquer arquivos de registro adicional para outros volumes no servidor de produção 105). Em geral, os processos de cópia de proteção podem ser executados sob qualquer número de circunstâncias, tal como, sob demanda, ou por um

programa de cópia de proteção específico. Em todo caso, processos de cópia de proteção que geralmente envolvem o servidor de produção 105 podem enviar os dados do arquivo de registro 130 para um ou mais agentes de gerenciamento (por exemplo, 135) no servidor de reserva 110. Tipicamente, o um ou mais agentes de gerenciamento (por exemplo, 135) irão então aplicar as mudanças nos dados recebidos para um ou mais volumes armazenados (por exemplo, 145), que podem conter outras cópias anteriores de mudanças para dados específicos.

De acordo com implementações da presente invenção, contudo, o um ou mais agentes de gerenciamento (por exemplo, 135) podem também comparar os dados de cópia de proteção recebidos a um ou mais estabelecimentos de política 140 existentes para executar uma ação de resposta 143 particular. Como será entendido mais completamente aqui, por exemplo, se o agente de gerenciamento 135 identificar que qualquer dos dados no arquivo de registro 130 tiver sido marcado como tendo vírus (isto é, inclui um ou mais indicadores de vírus), o estabelecimento de política 140 pode instruir o servidor de reserva 110 para executar qualquer número de ações de resposta correspondente 143. Por exemplo, o estabelecimento de política 140 pode instruir o servidor de reserva 110 a deletar os dados marcados com vírus, "limpar" (isto é, limpar ou remover vírus) ou deletar os dados da cópia de proteção recebidos, bem como apagar ou deletar cópias anteriores dos dados.

Desse modo, pelo menos um aspecto da presente invenção envolve não somente o escaneamento por vírus, mas também assegura que qualquer informação com relação às remoções de vírus possa ser efetivamente propagada para as entidades relevantes no sistema 100. Em pelo menos uma implementação, por exemplo, isso pode ser obtido pela indicação das gravações de arquivo com um ou mais indicadores de vírus, e assegurando que um ou mais indicadores de vírus permanecem indicados, quando apropriado. Por exemplo, a Figura 1B ilustra um diagrama esquemático detalhado de acordo com uma implementação da presente invenção na qual o servidor de produção 105 identifica um ou mais vírus através de um filtro comum 125, e usa o filtro comum 125 para indicar um ou mais indicadores de vírus para os arquivos infectados.

Em particular, a Figura 1B ilustra que o gerenciador de filtro 115 pode receber gravações de arquivo 103 e 107, tal como descrito anteriormente na Figura 1A. Adicionalmente, a Figura 1B ilustra que pelo menos uma gravação de arquivo 103 está infectada com um vírus (por exemplo, 113). O gerenciador de filtro 115 então passa as gravações de arquivo 103 e 107 para qualquer número apropriado de filtros registrados, tal como os filtros 125, 127, etc. Por exemplo, a Figura 1B ilustra que o gerenciador de filtro 115 passa a gravação de arquivo 103 (e o vírus indicado 113), bem como a gravação de arquivo 107 para o filtro de AV/de reprodução comum 125. Como anteriormente mencionado, o filtro comum 125, por sua vez, pode compreender qualquer número de

componentes adequados, incluindo pelo menos um componente antivírus 123 e um componente de reprodução 127. Em geral, o filtro 125 pode ser configurado de modo que quaisquer gravações recebidas do gerenciador de filtro 115 são passadas inicialmente para o componente antivírus 123 antes de serem passadas para o componente de reprodução 127. O ordenamento dos componentes dessa maneira, contudo, pode não ser necessariamente requerido ao tempo em que as gravações de arquivo podem ser indicadas com um ou mais indicadores de vírus, antes de serem passadas para um arquivo de registro (por exemplo, 130).

Em todo caso, a Figura 1B ilustra que o filtro comum 125 pode receber gravações de arquivo 103 e 107, e executar qualquer número de ações de escaneamento e de indicação no mesmo. Por exemplo, o componente antivírus 123 ou filtro 125 pode escanear a gravação de arquivo 103, e comparar os dados contidos no mesmo para qualquer número de definições de antivírus 150. Nesse caso, o filtro 125 identifica a presença do vírus 113 na gravação de arquivo 103. Contrariamente, os componentes antivírus 123 também recebem a gravação de arquivo 107, mas não reconhecem qualquer vírus na mesma. Desse modo, a Figura 1B ilustra que o componente antivírus 123 simplesmente passa juntamente com a gravação de arquivo 107 o componente de reprodução 127 como está, mas, com relação à gravação de arquivo 103, pode executar um número de ações adicionais.

Por exemplo, mediante a detecção do vírus 113, o componente antivírus 123 pode remover o vírus. Em outros casos, contudo, o componente antivírus 123 pode simplesmente detectar o vírus e não remover o mesmo, ou detectar o que parece ser o vírus e proporcionar uma indicação de que um vírus pode estar presente. Como tal, a Figura 1B ilustra que o componente antivírus 123 marca a gravação de arquivo 103 com um ou mais indicadores de vírus 117, que inclui a indicação com relação às ações e/ou as determinações do componente antivírus 123. Por exemplo, o um ou mais indicadores de vírus 117 pode incluir a informação de que existe um vírus 113 ainda contido dentro da gravação de arquivo 103, ou que existe somente a aparência de existir um vírus 113 presente, apesar de não estar confirmado. De forma similar, o um ou mais indicadores de vírus 117 pode indicar que o componente antivírus 123 tanto detectou quando removeu o vírus 113 da gravação de arquivo 103, mas que o vírus 113 esteve, contudo, presente em algum momento. Assim, uma pessoa deverá reconhecer que o um ou mais indicadores de vírus 117 pode incluir qualquer número de indicações que podem permitir que os componentes e os módulos seguintes tomem decisões adicionais na gravação de arquivo 103, bem como em seu arquivo fundamentado (por exemplo, 133).

Contudo, marcar ou indicar o componente de antivírus 123 pode então enviar a gravação de arquivo 103 para o componente de reprodução 127 juntamente com um ou mais indicadores de vírus 117. Por exemplo, a Figura 1B ilustra que o componente de

reprodução recebe ambas as gravações de arquivo 103 e 107. No final das contas, o componente de reprodução 127 irá comparar cada uma das gravações de arquivo 103, 107 com as políticas de reprodução 155, para determinar se os arquivos associados com essas gravações de arquivo estão programados para reprodução. Por exemplo, a Figura 1B ilustra a gravação de arquivo 107 não programada para reprodução e, como tal, o componente de reprodução 127 simplesmente passa a gravação de arquivo 107 para o volume 120, e adiciona essa gravação de arquivo para o arquivo correspondente 137. Contrariamente, a Figura 1B ilustra que o componente de reprodução 127 determina que a gravação de arquivo 103 esteja associada com o arquivo 133 que, com base nas políticas de reprodução 155, está programado para reprodução.

Claro, o agente de reprodução 127 pode alterar seus mecanismos usuais com base na presença de quaisquer indicadores de vírus (por exemplo, 117). Por exemplo, as políticas de reprodução 155 podem indicar que um arquivo, de outro modo programado para ser reproduzido, seja impedido de ser reproduzido quando um ou mais indicadores de vírus (por exemplo, 117) estão presentes. Isto é, o componente de reprodução 127 pode colocar em quarentena a gravação de arquivo 103, passar a anotar de arquivo 103 para o volume 120 sem colocar uma cópia no arquivo de registro 130, e pode também (ou alternativamente) enviar um ou mais indicadores de vírus para o arquivo de registro 130 sem os dados da gravação de arquivo correspondente. Assim, existe um número de ações para as quais o componente de reprodução 127 pode ser configurado.

Em todo caso, a Figura 1B ilustra que o componente de reprodução 127 identifica que a gravação de arquivo 103 deve ser reproduzida e, assim, cria uma cópia 103a da gravação de arquivo. Como ilustrado, a cópia da gravação de arquivo 103a também inclui uma cópia do um ou mais indicadores de vírus (isto é, 117a). Como tal, a Figura 1B ilustra que o componente de reprodução 127 passa a gravação de arquivo 103 para o volume 120, onde ele é incluído com seu arquivo de base fundamentado 133. Contrariamente, o componente de reprodução 127 passa a cópia da gravação de arquivo 103a e as cópias de indicador de vírus correspondentes 117a para o arquivo de registro 130. Como resultado, a gravação de arquivo 103, bem como o um ou mais indicadores de vírus juntado 117 podem ser incluídos nos processos de cópia de proteção (isto é, através das cópias 103a, 117a).

Como anteriormente mencionado, isso significa que o servidor de reserva 110 pode assim receber e identificar qualquer informação de vírus conhecida para (e executar ações correspondentes em) dados recebidos ou armazenados, sem necessariamente requerer o servidor de reserva 110 que execute um escaneamento adicionalmente por vírus. Como ilustrado na Figura 1C, por exemplo, um servidor de reserva 110 recebe os dados do arquivo de registro 130, que inclui a cópia de gravação de arquivo mais recente 103a e os um ou mais indicadores de vírus correspondentes 117a. Em particular, o servidor de

reserva 110 recebe e identifica os dados do arquivo de registro 130 através do um ou mais agentes de gerenciamento (por exemplo, 135). Em geral, o agente de gerenciamento compreende um grande número de instruções executáveis por computador que são implementadas por um grande número de processos, tal como iniciar processos de reprodução, executar ações em dados recebidos, e assim por diante. Especificamente, cada um dos agentes de gerenciamento 135 pode adicionalmente incluir (ou ser associado com) um ou mais agentes adicionais, tal como um agente antivírus 160.

Assim, mediante o recebimento do arquivo de registro 130, o agente de gerenciamento 135 pode identificar o um ou mias indicadores de vírus 117a. O agente de gerenciamento 135 pode então determinar quais das uma ou mais ações devem ser tomadas e, assim, adicionalmente consultar o um ou mais estabelecimento de políticas 140. Por exemplo, o um ou mais estabelecimento de políticas 140 pode incluir uma ou mais instruções para descartar uma gravação de arquivo infectada, colocar em quarentena uma gravação de arquivo infectada, e/ou executar uma ação similar em cópias anteriores dos dados. Como ilustrado na Figura 1C, por exemplo, o agente de gerenciamento 135 identifica a partir do estabelecimento de políticas 140 um conjunto de instruções para executar a ação de resposta 147. Nesse exemplo, a ação de resposta 147 inclui instruções para "limpar" todas as cópias da reprodução do arquivo de base fundamentado 133, e atualizações interativas da mesma. Especificamente, o estabelecimento de políticas 140 pode dizer ao agente de gerenciamento 135 que qualquer tempo um indicador de vírus (por exemplo, 117) pode ser recebido em uma gravação de arquivo particular (por exemplo, 103a), o arquivo de base fundamentado (por exemplo, reprodução 165) sendo presumido por conter um vírus.

Por exemplo, o servidor de reserva 110 já armazenou (por exemplo, através do volume de armazenagem 145) um número de cópias anteriores (com base em diferentes eventos de cópia de proteção) do arquivo 133. Em particular, a Figura 1C ilustra que o servidor de reserva 110 tem armazenada uma reprodução inicial 165 do arquivo 133 ao tempo "t_0", um atualizador 170 do arquivo por tempo "t_1", um atualizador 175 do arquivo por tempo "t_2", um atualizador 180 por tempo "t_3" e um atualizador 185 por tempo "t_4". Assim, a gravação de arquivo 103a pode ser, nesse caso, um atualizador para reprodução 165 (isto é, para arquivo 133) ao tempo "t_5".

Nesse exemplo particular, portanto, e em resposta às instruções da ação de resposta 147, um agente de gerenciamento 135 limpa a gravação de arquivo 103a (se já não tiver removido ou "limpo") através de um agente antivírus 160. O agente de gerenciamento 135 pode também usar o agente antivírus 160 para limpar cada uma das diferentes reproduções 165, 170, 175, 180, 185. Tendo assim limpado cada cópia, portanto, o agente de gerenciamento 135 envia instruções correspondentes 190 para repor as

reproduções de arquivo 165, 170, 175, 180, 185 com os novos dados 195. Os dados 195, por sua vez, podem incluir o arquivo de base e a seguir atualizar (isto é, "$t_0 - t_5$") sem o vírus identificado.

Conseqüentemente, as Figuras 1A – 1C proporcionam um número de esquemáticos e componentes para identificar vírus em um nível de servidor de produção, disseminando a informação para um nível de servidor de reserva, e executando qualquer número de ações correspondentes em cada nível. Em adição ao acima mencionado, implementações da presente invenção podem também ser descritas em termos dos fluxogramas dos métodos compreendendo uma ou mais seqüências de atos para obter um resultado particular. Por exemplo, a Figura 2 ilustra um fluxograma tanto da perspectiva do servidor de produção 105 quando da do servidor de reserva 110 das gravações de arquivo filtradas usando um filtro antivírus/de reprodução comum, combinado, 125. Os atos da Figura 2 são descritos abaixo com referência aos esquemáticos e aos componentes das Figuras 1A até 1C.

Por exemplo, a Figura 2 ilustra que um método a partir da perspectiva do servidor de produção 105 do gerenciamento do vírus e dos processos de filtragem de cópia de proteção através de um filtro comum pode compreender um ato 200 de identificar a uma ou mais gravações de arquivo. O ato 200 inclui identificar uma ou mais gravações de arquivo através de um filtro comum. Por exemplo, como ilustrado na Figura 1A e 1B o servidor de produção 105 recebe gravações de arquivo 103 e 107 (isto é, qualquer número de chamadas do sistema I/O) através do gerenciamento de filtro 115. O gerenciador de filtro 115 por sua vez passa essas gravações para o filtro AV/reprodução comum 125.

Adicionalmente, a Figura 2 ilustra que o método a partir da perspectiva do servidor de produção 105 pode compreender um ato 210 de escanear gravações de arquivo a procura de vírus. O ato 210 pode incluir escaneamento de uma identificada das uma ou mais gravações de arquivo no filtro comum de acordo com um ou mais definições de vírus. Como ilustrado na Figura 1B, por exemplo, um filtro AV/de reprodução comum 125 recebe as gravações de arquivo 103 e 107 e compara os dados correspondentes com uma ou mais definições de antivírus 150 através do componente antivírus 123. O filtro AV/de reprodução comum 125 assim determina através do componente antivírus 123 que a gravação de arquivo 103 inclui o vírus 113.

A Figura 2 também ilustra que o método a partir da perceptiva do servidor de produção 105 pode compreender um ato 220 de comparar os arquivos escaneados com a política de reprodução. O ato 220 inclui comparar uma identificada das uma ou mais gravações de arquivo no filtro comum com uma ou mais políticas de reprodução. Por exemplo, a Figura 1B ilustra que o filtro AV/de reprodução 125 também recebe as gravações de arquivo 103 e 107 no componente de reprodução 127 após terem sido

tratadas/escaneadas pelo componente antivírus 123. O componente de reprodução 127 então compara as gravações de arquivo 103 e 107 com as políticas de reprodução 155 para determinar se essas gravações de arquivo são designadas para serem protegidas através dos processos de cópia de proteção.

Adicionalmente, a Figura 2 ilustra que o método a partir da perspectiva do servidor de produção 105 pode compreender um ato 230 de enviar a gravação de arquivo para um arquivo de registro. O ato 230 inclui enviar uma cópia de pelo menos uma das gravações de arquivo escaneadas para um arquivo de registro, tal que a pelo menos uma gravação de arquivo é reproduzida para um servidor de reserva. Como ilustrado na Figura 1B, por exemplo, apesar do filtro AV/de reprodução comum 125 receber as gravações de arquivo 103 e 107, o filtro de reprodução identifica que somente a gravação de arquivo 103 está programada para ser reproduzida. Desse modo, o componente de reprodução 127 copia somente a gravação de arquivo 103 (isto é, como cópia 103a) para um arquivo de registro 130, mas envia ambas as gravações de arquivo 103 e 107 para armazenamento no volume 120.

Como tal, a Figura 2 ilustra que um método a partir da perspectiva do servidor de reserva 110 do gerenciamento dos dados reproduzidos de acordo com um ou mais indicadores de vírus provido por um filtro comum em um ou mais servidores de produção pode compreender um ato 240 de receber cópias de proteção de dados. O ato 240 inclui receber uma ou mais cópias de proteção de dados a partir do um ou mais servidores de produção. Por exemplo, como ilustrado na Figura 1C, o agente de gerenciamento 130 do servidor de reserva 110 recebe os dados de cópia de proteção do pelo menos um arquivo de registro 130 a partir do servidor de produção 105.

Adicionalmente, a Figura 2 ilustra que o método a partir da perspectiva do servidor de reserva 110 pode compreender um ato 250 de identificar um ou mais indicadores de vírus nos dados recebidos. O ato 250 inclui identificar um ou mais indicadores de vírus na cópia recebida das uma ou mais cópias de proteção de dados, em que o um ou mais indicadores de vírus identificam que pelo menos uma das uma ou mais cópias de proteção de dados é associada com os dados infectados. Por exemplo, a Figura 1C ilustra que o agente de gerenciamento 135 recebe dados do arquivo de registro 130, que inclui gravação de arquivo 103a e um ou mais indicadores de vírus 117a. Desse modo, o agente de gerenciamento 135 identifica a partir do um ou mais indicadores de vírus 117a que um vírus existe ou que um vírus foi removido, mas, contudo existia em uma versão anterior do arquivo.

A Figura 2 também ilustra que o método a partir da perspectiva do servidor de reserva 110 pode compreender um ato 260 de identificação de uma ou mais políticas para as ações de resposta. O ato 260 inclui identificar uma ou mais políticas para o servidor de

reserva, em que a uma ou mais políticas identificam uma ou mais ações de resposta correspondendo um ou mais indicadores de vírus. Por exemplo, a Figura 1C ilustra que o agente de gerenciamento 135 consulta os estabelecimentos de política 140 e recebe instruções para implementar ações de resposta 147, que requerem que o servidor de reserva 110 limpe todas as cópias anteriores ou cópia presentes do arquivo 133 (isto é, o arquivo fundamentado para a gravação 103a).

Adicionalmente, a Figura 2 ilustra que um método a partir da perspectiva do servidor de reserva 110 pode compreender um ato 270 de executar uma ação de resposta para os indicadores de vírus. O ato 270 inclui executar qualquer uma ou mais ações de resposta de acordo com a uma ou mais políticas. Por exemplo, a Figura 1C ilustra que o agente de gerenciamento 135 (por exemplo, através do agente antivírus 160) tome cada cópia de referência e atualize o arquivo 133 (isto é, para tempos "t_0" – "t_5") e remova qualquer infecção de vírus. O agente de gerenciamento 135 então prepara uma cópia limpa 195 desses dados, e envia as instruções correspondentes 190 para substituir as cópias originais desses dados 165, 170, 175, 180, 185 no volume armazenado 145 com os dados novos e limpos 195.

Desse modo, as Figuras 1A-2 proporcionam um número de componentes e mecanismos para assegurar que a informação de vírus identificada possa ser eficientemente propagada através do sistema de reserva 100. Como um resultado dessa e de outras características, as ameaças associadas com a reprodução inadvertida dos vírus podem ser mais efetivamente mitigadas. Em particular, a grande distribuição da informação de vírus permite um número de características adicionais de acordo com os princípios discutidos aqui. Por exemplo, o servidor de produção 105 pode receber um ou mais pedidos para dados que são ou foram infectados. O servidor de produção 105, tal como através do filtro comum 125, pode determinar que o pedido se refira a um ou mais arquivos que são associados com um ou mais indicadores de vírus, e nega ou permite o pedido com base em qualquer número de políticas do servidor de produção.

Pedidos para certos dados de cópia de proteção podem também ser tratados de uma maneira similar. Por exemplo, um usuário pode requerer um ou mais arquivos que tenham sido armazenados no servidor de reserva 110 (isto é, tiverem sido copiados para proteção). O filtro comum 125 (ou outro agente apropriado) pode identificar, a partir de um índice, que o pedido envolve um ou mais arquivo que foram anteriormente associados em um ponto com um ou mais indicadores de vírus. O servidor de produção 105 pode então prover um aviso para o usuário, ou mesmo escanear e remover quaisquer dados correspondentes mais tarde recebidos a partir do servidor de reserva 110, com base nos pedidos.

De forma similar, os pedidos passados do servidor de produção 105 para o servidor de reserva 110 para os dados de cópia de proteção podem envolver o mesmo cálculo. Isto é, o agente de gerenciamento 135 pode identificar a partir do um ou mais pedidos que os dados requeridos sejam associados com um ou mais indicadores de vírus, ou associados com um ou mais arquivos que são, por sua vez, juntados a um ou mais indicadores de vírus. O agente de gerenciamento 135 pode então remover o vírus antes de retornar os dados, negar o pedido ou similar, dependendo de qualquer número de vários estabelecimentos de política.

As modalidades da presente invenção podem compreender um computador de finalidade especial ou de finalidade geral incluindo vários hardwares de computador, como será discutido em maiores detalhes abaixo. As modalidades dentro do escopo da presente invenção também incluem meios legíveis por computador para executar ou ter instruções executáveis por computador ou estruturas de dados armazenadas no mesmo. Tais meios legíveis por computador podem ser quaisquer meios disponíveis que podem ser acessados por um computador de finalidade geral ou de finalidade especial.

Como exemplo, e não de forma limitativa, tais meios legíveis por computador podem compreender RAM, ROM, EEPROM, CD-ROM ou outros meios de armazenamento óptico ou armazenamento de disco magnético ou outro dispositivo de armazenamento magnético ou quaisquer outros meios que podem ser usados para executar ou armazenar meios de código de programa desejado, na forma de instruções executáveis por computador ou de estruturas de dados e que podem ser acessadas por um computador para finalidade geral ou para finalidade especial. Quando a informação é transferida ou provida em uma rede ou outra conexão de comunicação (tanto fisicamente conectada, sem fio quanto uma combinação de fisicamente conectada quanto de sem fio) para um computador, o computador oportunamente visualiza a conexão como um meio legível por computador. Assim, qualquer tal conexão é oportunamente designada para um meio legível por computador. Combinações do acima devem também ser incluídas dentro do escopo do meio legível por computador.

Instruções executáveis por computador compreendem, por exemplo, instruções e dados que induzem um computador de finalidade geral, computador de finalidade especial ou dispositivo de processamento de finalidade especial a executar uma certa função ou um grupo de funções. Apesar de a matéria ter sido descrita em linguagem específica para as características estruturais e/ou os atos metodológicos, deve ser entendido que a matéria definida nas reivindicações anexas não está necessariamente limitada às características específicas ou aos atos acima descritos. Ao contrário, as características específicas e os atos descritos acima são descritos como forma de exemplo da implementação das reivindicações.

A presente invenção pode ser corporificada em outras formas específicas sem fugir do seu espírito ou de suas características essenciais. As modalidades descritas devem ser consideradas em todas as considerações somente como ilustrativas, e não como restritivas. O escopo da invenção é, portanto, indicado por meio das reivindicações anexas ao invés de pela descrição acima. Todas as modificações que estejam dentro do significado e da faixa de equivalência das reivindicações devem ser consideradas dentro do seu escopo.

REIVINDICAÇÕES

1. Método de gerenciamento de vírus e processo de filtragem de cópia de proteção através de um filtro comum, em um servidor de produção em um ambiente computadorizado no qual o servidor de produção é copiado para proteção por um ou mais dos servidores de reserva, **CARACTERIZADO** por compreender os atos de:

identificar uma ou mais gravações de arquivo através de um filtro comum;

escanear a identificada uma ou mais gravações de arquivo no filtro comum de acordo com uma ou mais definições de vírus;

comparar a identificada uma ou mais gravações de arquivo escaneadas no filtro comum com uma ou mais políticas de reprodução; e

enviar uma cópia da pelo menos uma ou mais gravações de arquivo escaneadas para um arquivo de registro, tal que a pelo menos uma gravação de arquivo seja reproduzida para um servidor de reserva.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de adicionalmente compreender um ato de identificar pelo menos uma ou mais das gravações de arquivo como infectada com qualquer um de um ou mais vírus.

3. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de adicionalmente compreender um ato de marcar a pelo menos uma gravação de arquivo com um ou mais indicadores de vírus antes da uma ou mais gravações de arquivo ser comparadas com a um ou mais configurações de reprodução.

4. Método, de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de que o um ou mais indicadores de vírus identificam que o vírus foi identificado, mas não removido.

5. Método, de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de adicionalmente compreender um ato de remover qualquer um dos um ou mais vírus infectando o pelo menos um arquivo, em que o um ou mais indicadores de vírus identificam que a pelo menos uma gravação de arquivo estava presente, mas agora removida.

6. Método, de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de adicionalmente compreender um ato de armazenar uma cópia da pelo menos uma gravação de arquivo no arquivo de registro com o um ou mais indicadores de vírus.

7. Método, de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de adicionalmente compreender um ato de enviar a pelo menos uma gravação de arquivo e o correspondente um ou mais indicadores de vírus para o servidor de reserva, tal que o servidor de reserva possa identificar uma associação entre a pelo menos uma gravação de arquivo e o um ou mais indicadores de vírus.

8. Método, de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de adicionalmente compreender um ato de enviar um ou mais indicadores para o servidor de

reserva antes que os dados associados com a pelo menos uma gravação de arquivo infectada sejam também infectados.

9. Método, de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de adicionalmente compreender um ato de determinar não de reproduzir a infectada da pelo menos uma gravação de arquivo.

10. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de adicionalmente compreender os atos de:

receber um ou mais pedidos para recuperar dados armazenados no servidor de reserva;

identificar que pelo menos um dos um ou mais pedidos faz referência a dados que são associados com um ou mais indicadores de vírus.

11. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de adicionalmente compreender um ato de enviar um ou mais respostas ao um ou mais pedidos com base em indicadores de vírus identificados.

12. Método, de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que a pelo menos uma das uma ou mais respostas indicam que os dados pedidos:

(i) são associados com o um ou mais vírus;

(ii) não podem ser recuperados devido ao um ou mais vírus; ou

(iii) podem somente ser recuperados se o um ou mais vírus forem primeiramente removidos.

13. Método para gerenciar dados reproduzidos de acordo com um ou mais indicadores de vírus providos por um filtro comum em um ou mais servidores de produção, em um servidor de reserva em um ambiente computadorizado, no qual o servidor de reserva efetua cópia de proteção de dados em um ou mais servidores de produção, **CARACTERIZADO** pelo fato de compreender os atos de:

receber uma ou mais cópias de proteção de dados a partir do um ou mais servidores de produção;

identificar um ou mais indicadores de vírus na uma ou mais cópias de proteção de dados recebidos, em que o um ou mais indicadores de vírus indicam que a pelo menos uma das uma ou mais cópias de proteção de dados é associada com os dados infectados;

identificar uma ou mais políticas para o serviço de cópia de proteção, em que a uma ou mais políticas identificam uma ou mais ações de resposta correspondendo a um ou mais indicadores de vírus; e

executar qualquer uma ou mais das ações de resposta de acordo com a uma ou mais políticas.

14. Método, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que a qualquer uma ou mais das ações de resposta inclui uma ação de remover um ou mais

vírus a partir de qualquer uma ou mais cópias de proteção de dados recebidos associados com o um ou mais indicadores de vírus.

15. Método, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que qualquer das uma ou mais ações de resposta inclui os atos de:

limpar pelo menos uma parte das uma ou mais cópias de proteção de dados associadas com o um ou mais indicadores de vírus; e

limpar uma cópia anterior da parte armazenada no servidor de reserva.

16. Método, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que a qualquer uma ou mais das ações de resposta inclui um ato de identificar que uma cópia de dados de referência é associada com o um ou mais vírus com base pelo menos em parte na identificação do um ou mais indicadores de vírus de qualquer da uma ou mais cópias de proteção de dados.

17. Método, de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de adicionalmente compreender os atos de:

receber um ou mais pedidos para dados associados com a cópia de dados de referência no servidor de reserva; e

enviar uma resposta que pelo menos uma parte dos dados solicitados foram associadas com o um ou mais indicadores de vírus.

18. Meio legível por computador tendo instruções executáveis por computador armazenado no mesmo que, quando executadas, induzem o um ou mais processadores a executar um método, em um servidor de produção em um ambiente computadorizado no qual o servidor de produção é copiado para proteção por um ou mais servidores de reserva, **CARACTERIZADO** pelo fato de compreender os atos de:

identificar uma ou mais gravações de arquivo através de um filtro comum;

escanear a identificada uma ou mais gravações de arquivo no filtro comum de acordo com uma ou mais definições de vírus;

comparar a identificada uma ou mais gravações de arquivo escaneadas no filtro comum com uma ou mais políticas de reprodução; e

enviar uma cópia da pelo menos uma ou mais gravações de arquivo escaneadas para um arquivo de registro, tal que a pelo menos uma gravação de arquivo seja replicada para um servidor de reserva.

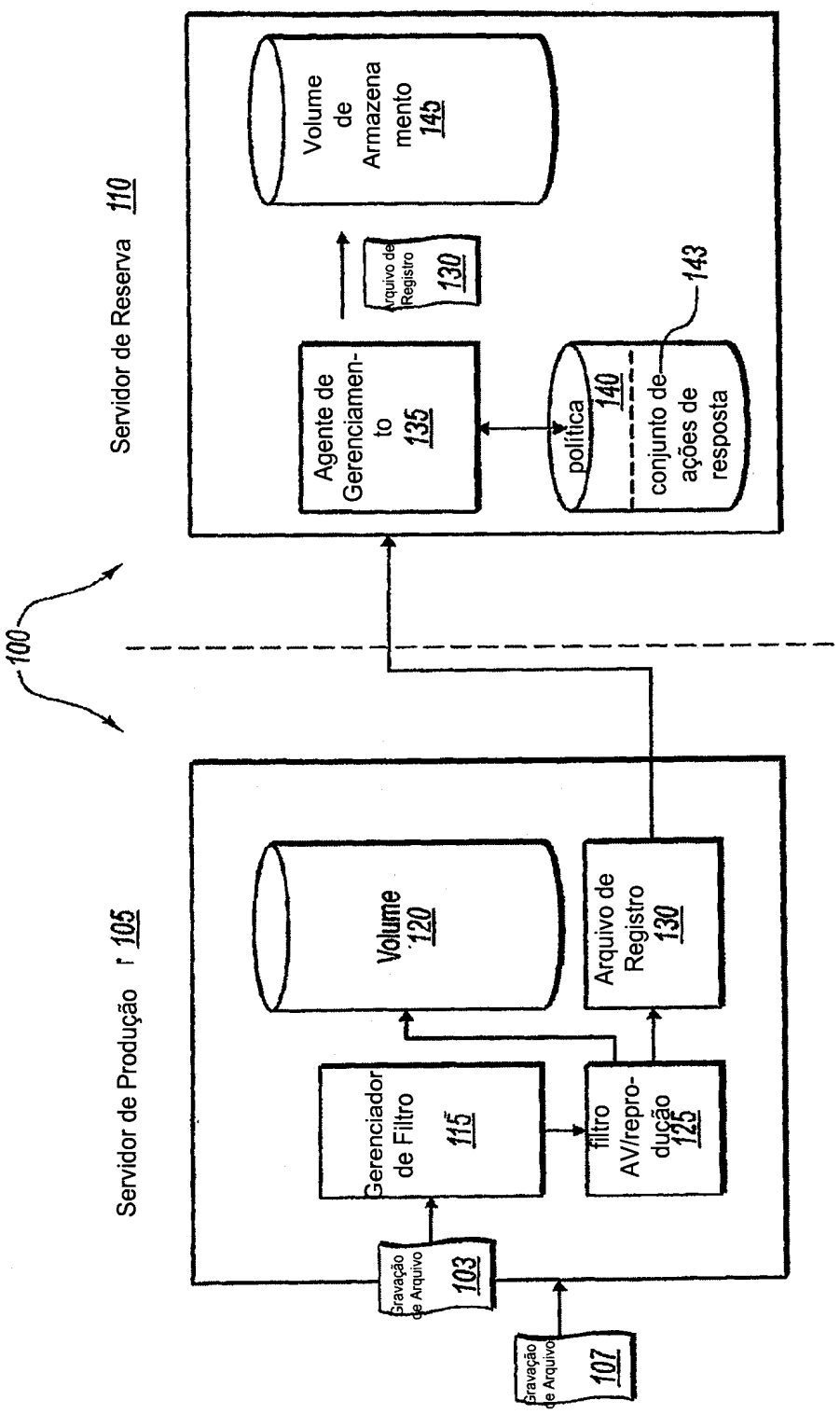
100
Servidor de Produção 105
Servidor de Reserva 110
Volume 120
Arquivo de Registro 130
Gerenciador de Filtro 115
filtro AV/reprodução 125
Gravação de Arquivo 103
Gravação de Arquivo 107
Agente de Gerenciamento 135
Arquivo de Registro 130
Volume de Armazenamento 145
política 140
conjunto de ações de resposta
143

FIG. 1A

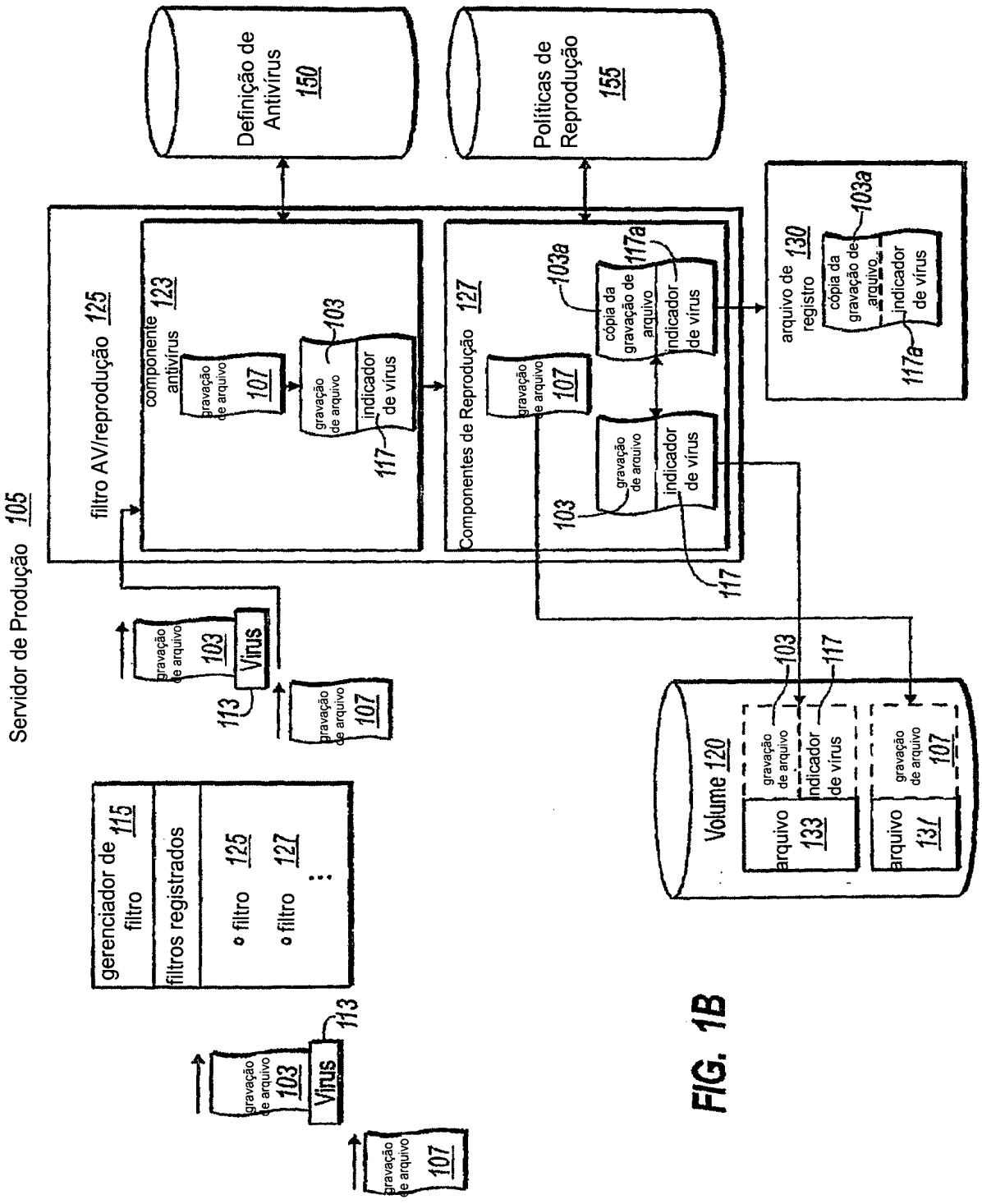
Servidor de Produção 105
filtro AV/reprodução 125
componente antivírus 123
gravação de arquivo 107
gravação de arquivo 103
indicador de vírus
117
Componentes de Reprodução 127
103a
cópia da gravação de arquivo
117a
Definição de Antivírus 150
Políticas de Reprodução 155
arquivo de registro 130
gerenciador de filtro 115
filtros registrados
filtro 125
filtro 127
Vírus
113
Volume 120
arquivo 133
arquivo 131

FIG. 1B

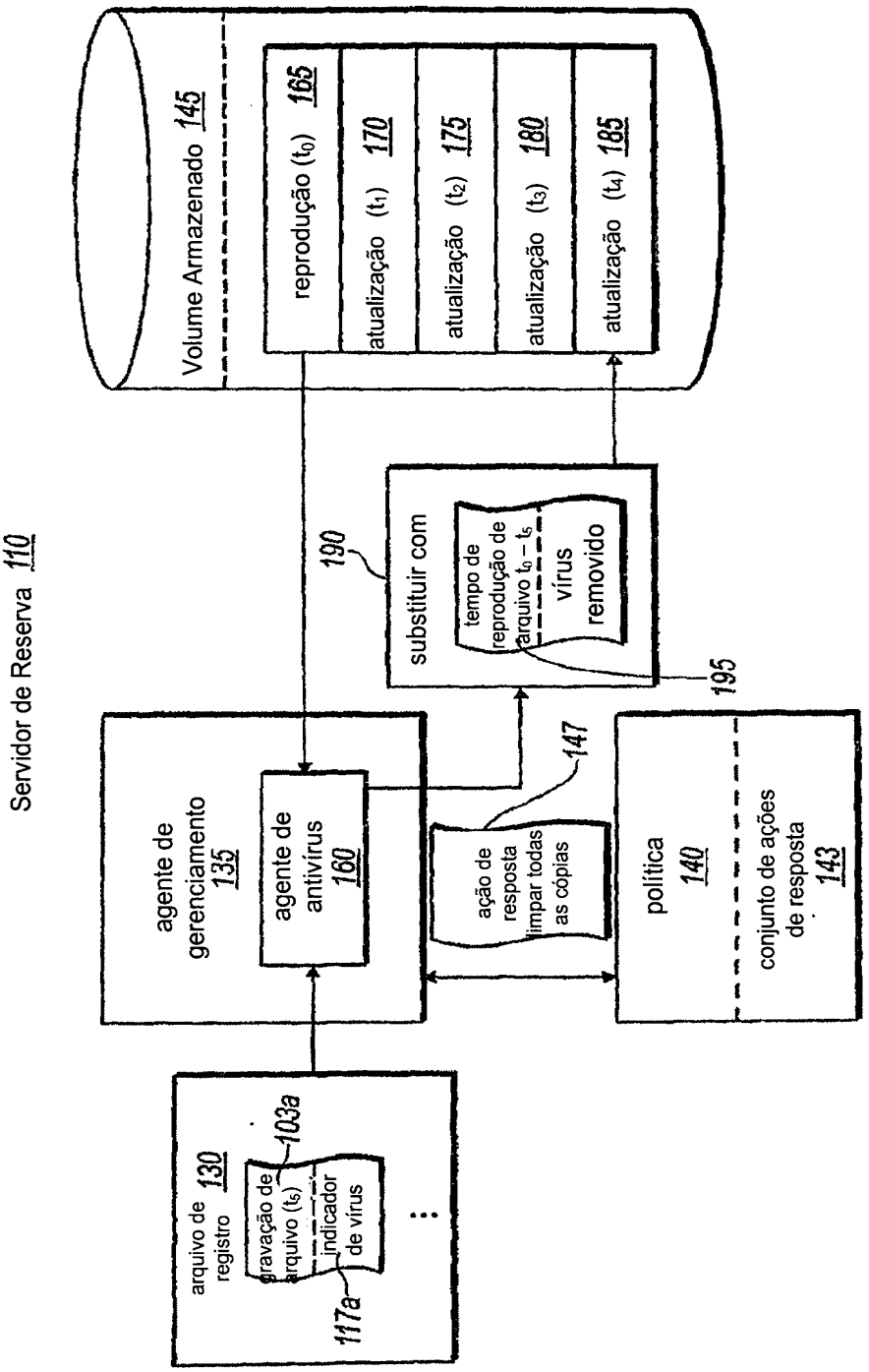
Servidor de Reserva 110
Volume Armazenado 145
reprodução (t_0) 165
atualização (t_1) 170
atualização (t_2) 175
atualização (t_3) 180
atualização (t_4) 185
190
substituir com
tempo de reprodução de arquivo $t_0 - t_5$
vírus removido
195
agente de gerenciamento 135
agente de antivírus 160
147
ação de resposta limpar todas as cópias
política 140
conjunto de ações de resposta 143
arquivo de registro 130
gravação de arquivo (t_5)
indicador de vírus
103a
117a

FIG. 1C

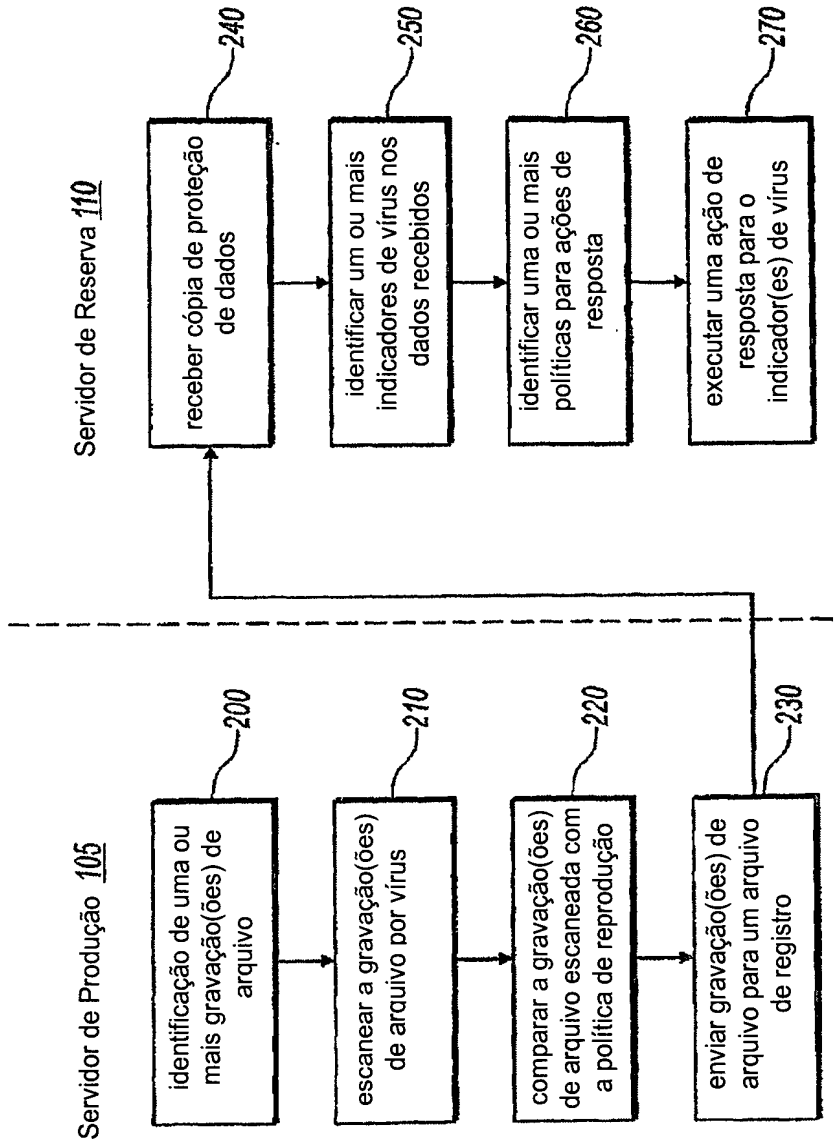
Servidor de Produção 105
identificação de uma ou mais gravação(ões) de arquivo
200
escanear a gravação(ões) de arquivo por vírus
210
comparar a gravação(ões) de arquivo escaneada com a política de reprodução
220
enviar gravação(ões) de arquivo para um arquivo de registro
230
Servidor de Reserva 110
receber cópia de proteção de dados
240
identificar um ou mais indicadores de vírus nos dados recebidos
250
identificar uma ou mais políticas para ações de resposta
260
executar uma ação de resposta para o indicador(es) de vírus
270

FIG. 2

RESUMO

"CHECAGEM DE VÍRUS E FILTRAGEM DE REPRODUÇÃO COMBINADAS"

Dados nos sistemas de cópia de proteção podem ser eficientemente protegidos contra vírus, mesmo se as definições para certos vírus são encontradas após os dados infectados terem sido copiados por proteção em um servidor de reserva. Em uma implementação, um filtro combinado que inclui componentes de filtro antivírus e de reprodução pode identificar e processar chamadas de sistema I/O (por exemplo, incluindo gravações de arquivo). Se um vírus está presente, o componente antivírus do filtro combinado pode marcar o arquivo e/ou a gravação de arquivo (e limpar a gravação de arquivo/arquivo), e passar essa informação para o componente de reprodução. Se a gravação de arquivo é associada com um arquivo a ser copiado por proteção, o componente de reprodução pode então passar, junto com os indicadores de filtro antivírus, uma cópia da gravação de arquivo, o servidor de reserva pode também identificar se as versões anteriores do arquivo armazenadas no servidor de reserva podem ter sido infectadas, e pode assim executar quaisquer ações apropriadas.