Guia de Visão Geral

Sentinel 7.0.1

March 2012

NetIQ

Aviso Legal

A NetIQ Corporation (“NetIQ”) não faz representações ou garantias quanto ao conteúdo ou à utilização desta documentação e, especificamente, isenta-se de quaisquer garantias, explícitas ou implícitas, de comerciabilidade ou adequação a qualquer propósito específico. A NetIQ também reserva-se o direito de revisar esta publicação e fazer mudanças em seu conteúdo a qualquer momento, sem obrigação de notificar qualquer pessoa ou entidade sobre essas revisões ou mudanças.

A NetIQ não faz representações ou garantias quanto a qualquer software e, especificamente, isenta-se de quaisquer garantias, explícitas ou implícitas, de comerciabilidade ou adequação a qualquer propósito específico. A NetIQ também reserva-se o direito de fazer mudanças parciais ou totais no software, a qualquer momento, sem a obrigação de notificar qualquer pessoa ou entidade sobre essas mudanças.

Quaisquer informações técnicas ou sobre produtos fornecidas segundo os termos do presente Contrato estão sujeitas aos controles de exportação dos EUA e às leis comerciais de outros países. Você concorda em obedecer a todos os regulamentos de controle de exportação e em adquirir quaisquer licenças ou classificações necessárias para exportar, reexportar ou importar produtos. Você concorda em não exportar nem reexportar para entidades que constam nas listas de exclusão de exportação atual dos EUA ou para qualquer país embargado ou terrorista conforme especificado nas leis de exportação dos EUA. Você concorda em não usar produtos para fins proibidos relacionados a armas nucleares, biológicas e químicas ou mísseis. A NetIQ não assumirá qualquer responsabilidade se o usuário não obtiver as aprovações necessárias para exportação.

Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.

Para obter mais informações, entre em contato com a NetIQ em:

1233 West Loop South, Houston, Texas 77027
EUA
www.netiq.com

Índice

Sobre este guia

Este guia apresenta o Sentinel, um produto WorkloadIQ.

Público

Este guia é destinado aos profissionais de segurança da informação.

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no produto. Use o recurso User Comments (Comentários do Usuário) na parte inferior de cada página da documentação online.

Atualizações da documentação

Para obter a versão mais recente do *Guia de Visão Geral do NetIQ Sentinel 7.0.1*, visite o site de documentação do Sentinel (http://www.novell.com/documentation/sentinel70).

Documentação adicional

A documentação técnica do Sentinel está dividida em diversos volumes. São eles:

- Guia de Inicialização Rápida do Sentinel (http://www.novell.com/documentation/sentinel70/s70_quickstart/data/s70_quickstart.html)
- Guia de Instalação do Sentinel (http://www.novell.com/documentation/sentinel70/s70_install/data/bookinfo.html)
- Guia de Administração do Sentinel (http://www.novell.com/documentation/sentinel70/s70_admin/data/bookinfo.html)
- Guia do Usuário do Sentinel (http://www.novell.com/documentation/sentinel70/s70_user/data/bookinfo.html)
- Guia de Visão Geral de Vínculo do Sentinel (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Eventos de Auditoria Interna do Sentinel (http://www.novell.com/documentation/sentinel70/s70_auditevents/data/bookinfo.html)
- Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)

  O site do Sentinel SDK fornece informações sobre como você pode criar seus próprios plug-ins.

Entrando em contato com a Novell e a NetIQ

Agora o Sentinel é um produto NetIQ, mas a Novell continua administrando muitas funções de suporte.

- Site da Novell (http://www.novell.com)

- Site da NetIQ (http://www.netiq.com)
- Suporte técnico (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Suporte Pessoal (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Site para download de patches (http://download.novell.com/index.jsp)
- Fóruns de suporte da comunidade do Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)
- TIDS do Sentinel (http://support.novell.com/products/sentinel)
- Site de plug-ins do Sentinel (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **Lista de e-mails de notificação:** Inscreva-se no site de plug-ins do Sentinel

Entrando em contato com o Suporte a Vendas

Para esclarecer dúvidas sobre produtos, preços e recursos, entre em contato com seu parceiro local. Se não puder entrar em contato com seu parceiro, entre em contato com nossa equipe de Suporte a Vendas.

Mundial: Escritórios da NetIQ (http://www.netiq.com/about_netiq/officelocations.asp)

Estados Unidos e Canadá: 888-323-6768

E-mail: info@netiq.com

Site: www.netiq.com

1 Visão Geral do Sentinel

O Sentinel é uma solução de gerenciamento de segurança, informações e eventos (SIEM), além de uma solução de monitoramento de conformidade. Ele monitora automaticamente os ambientes de TI mais complexos e fornece a segurança necessária para proteger seu ambiente de TI.

1.1 Por que segurança é importante

Com o intuito de reduzir custos e fidelizar clientes, a segurança deve ser encarada com seriedade pelas empresas nos dias atuais. Cada registro vazado custa em média US $200. Bastaria uma única violação de dados e alguns milhares de registros perdidos para gerar impacto significativo em uma empresa.

No caso de um possível ataque a sua empresa, você estará sujeito às seguintes despesas:

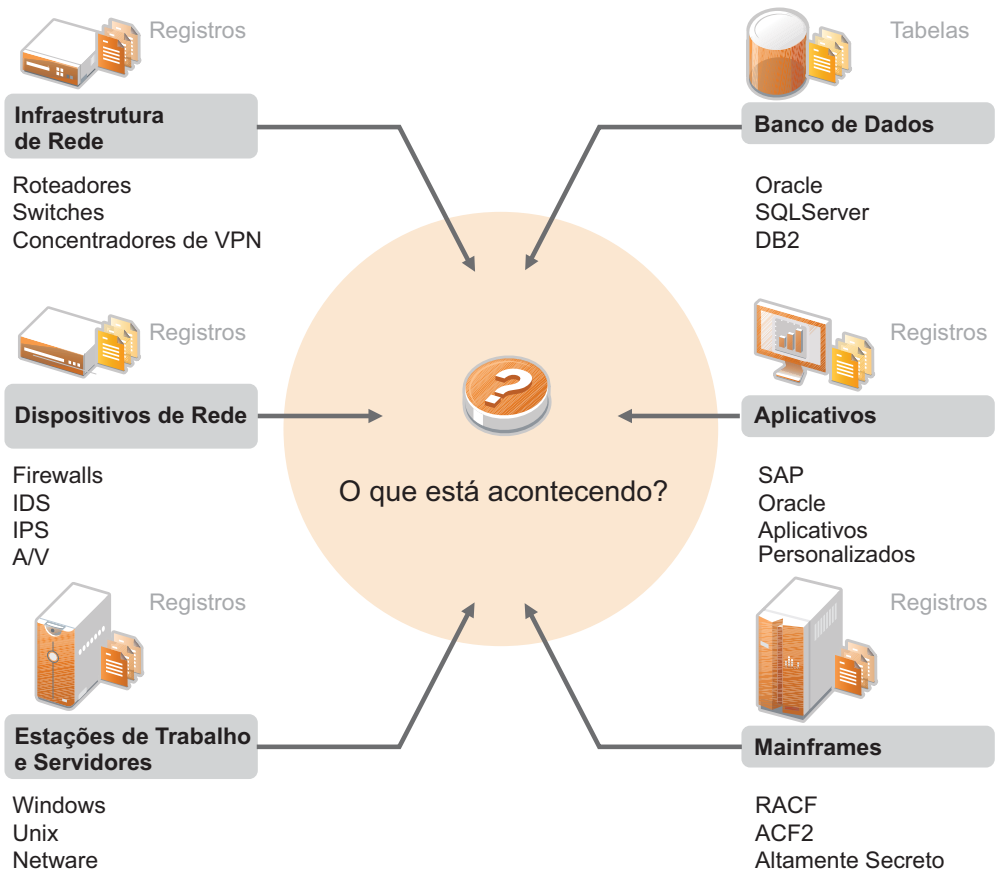
- Despesas judiciais;
- Custo com investigações e perícia forense;
- Aumento nas auditorias;
- Multas;
- Custos ocultos com perda de credibilidade por parte dos clientes
- Custos com clientes, devido à perda de credibilidade

Isso nos mostra a importância de um ambiente de TI seguro. Atualmente, a linha que separa funcionários com informações privilegiadas de pessoas não ligadas diretamente à empresa está cada vez mais tênue graças à Internet e ao crescente uso da tecnologia em nuvem.

1.2 Desafios ao proteger o ambiente de TI

A complexidade dos ambientes de TI geram grandes desafios para a segurança das informações. Existem diversos aplicativos, bancos de dados, mainframes, estações de trabalho e servidores, todos com registros de eventos. Além disso, você possui dispositivos de segurança e de infraestrutura de rede que também registram o que acontece no seu ambiente de TI.

Figura 1-1 *O que acontece no seu ambiente*



Os desafios surgem devido:

- Aos muitos dispositivos no seu ambiente de TI;
- Aos registros serem gravados em diversos formatos;
- Aos registros serem armazenados em silos;
- À quantidade de informações geradas nos registros; e
- À impossibilidade de identificar quem fez o que sem analisar manualmente todos os registros.

Para tornar as informações úteis, você deve:

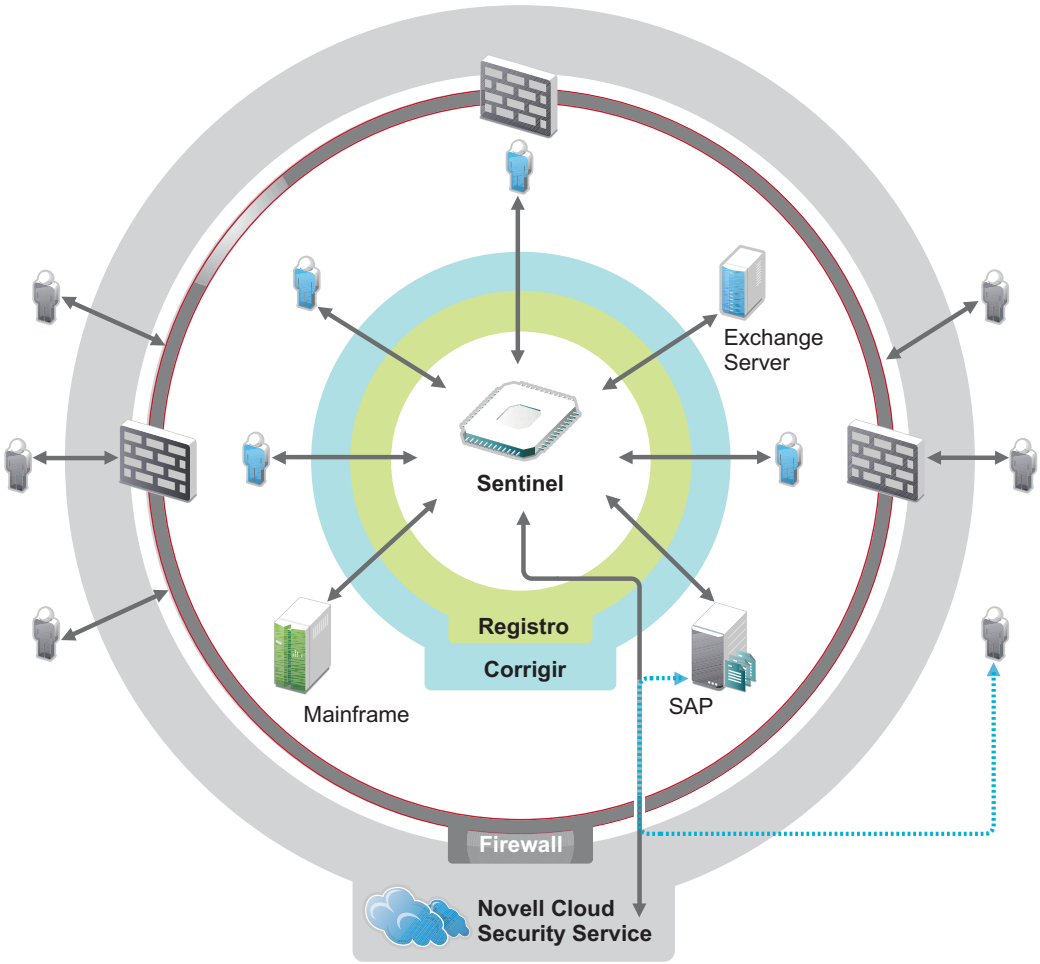
- Coletar dados;
- Consolidar esses dados;
- Normalizar dados distintos em eventos que podem ser facilmente comparados
- Mapear eventos para normas padrão
- Analisar os dados;
- Comparar eventos em diversos sistemas para determinar se há algum problema de segurança;
- Enviar notificações no caso de dados que não atendam às normas;
- Impor ações sobre as notificações para cumprir com as políticas da empresa; e
- Gerar relatórios para comprovar a conformidade.

Depois de identificar os desafios relacionados à segurança do seu ambiente de TI, é necessário determinar como proteger a empresa para e dos usuários sem tratá-los como criminosos ou sobrecarregá-los de maneira que os impeça de serem produtivos. O Sentinel é a solução.

1.3 Características do Sentinel

O Sentinel age como sistema nervoso central para a segurança empresarial. Ele retém dados de toda a infraestrutura: aplicativos, bancos de dados, servidores, armazenamento e dispositivos de segurança. Ele analise e correlaciona os dados e torna os dados processáveis, seja manual ou automaticamente.

Figura 1-2 *Características do Sentinel*



Com isso, você tem acesso ao que acontece no seu ambiente de TI a qualquer momento e consegue vincular as ações definidas para os recursos às pessoas responsáveis por aquelas ações. Isso permite determinar o comportamento dos usuários e também monitorar o controle de maneira eficiente. Independentemente de uma pessoa estar ligada diretamente ou não à empresa, é possível relacionar todas as ações tomadas por ela para que atividades verdadeiramente arriscadas sejam identificadas antes de causarem danos.

O Sentinel faz isso de maneira econômica ao:

- Fornecer uma única solução que lida com controles de TI em diversas normas;

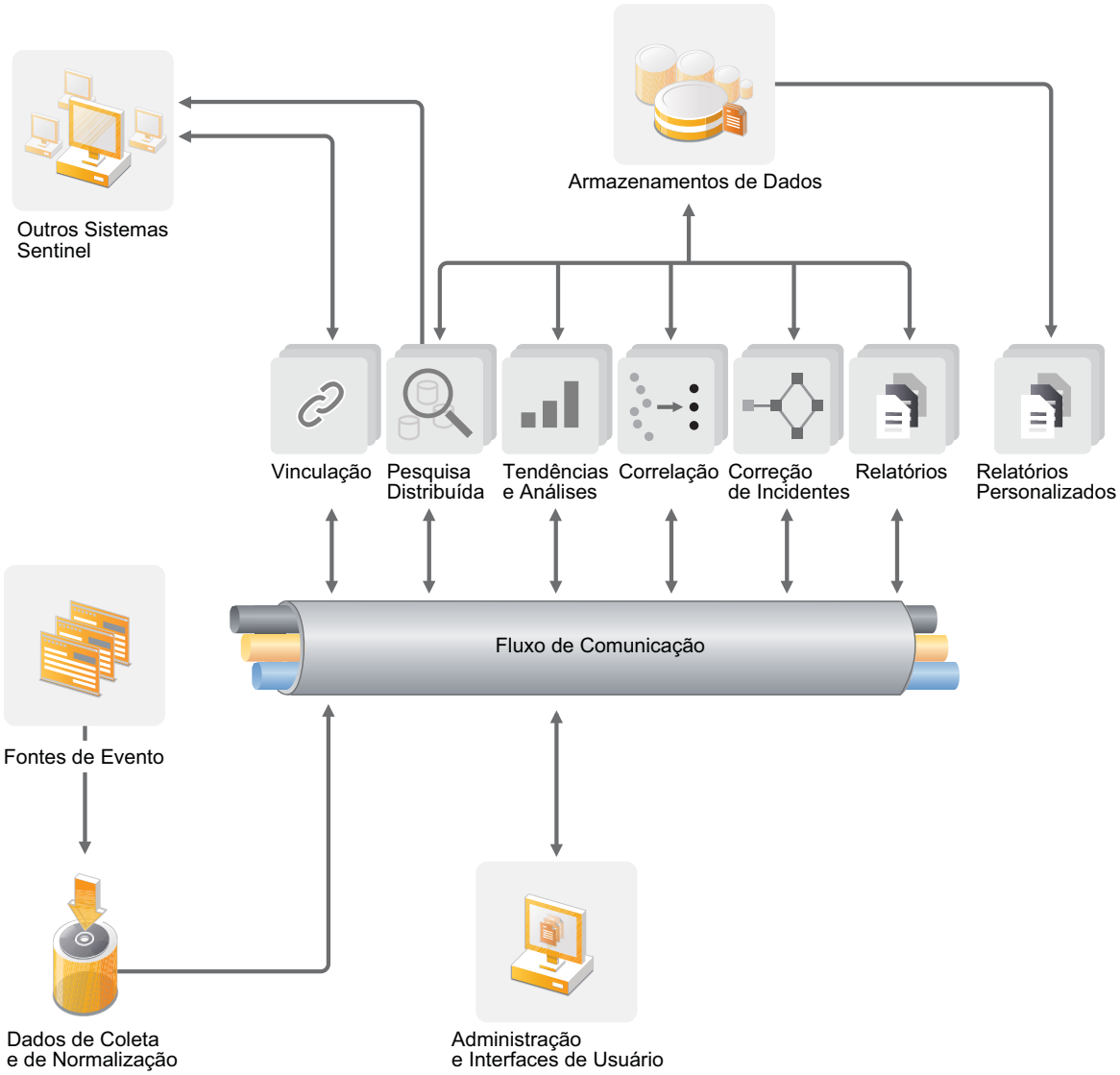
- Preencher a lacuna de conhecimento entre o que deveria acontecer e o que realmente acontece no seu ambiente em rede;
- Demonstrar aos auditores e às autoridades que sua empresa documenta, monitora e gera relatórios sobre controles de segurança;
- Fornecer monitoramento de conformidade e programas de relatórios prontos; e
- Gerar a visibilidade e o controle exigidos para avaliar continuamente o êxito dos programas de conformidade e de segurança da sua empresa.

O Sentinel automatiza os processos de geração de relatórios, análise e coleta de registros para garantir que os controles de TI sejam eficazes no suporte à detecção de ameaças e aos requisitos de auditoria. O Sentinel fornece monitoramento automatizado de eventos de segurança, eventos de conformidade e controles de TI permitindo que você tome medidas imediatas quando ocorre violação na segurança ou eventos de não conformidade. Ele também permite que você colete informações resumidas sobre o seu ambiente para comunicar a situação geral da segurança aos principais acionistas.

2 Como o Sentinel funciona

O Sentinel gerencia as informações e os eventos de segurança de forma contínua em todo o ambiente de TI para garantir uma solução de monitoramento completa. A figura a seguir mostra o funcionamento do Sentinel.

Figura 2-1 *Como o Sentinel funciona*



O Sentinel:

- Reúne informações de registros, eventos e segurança de todas as diferentes fontes de eventos no seu ambiente de TI.
- Padroniza as informações de registros, eventos e segurança coletadas em um formato comum.
- Adiciona as informações normalizadas a um barramento de mensagens com capacidade para mover milhares de pacotes de mensagem por segundo.
- Comunica-se com todos os componentes do Sentinel através do barramento de mensagens para garantir escalabilidade.

Nesse momento, os diversos componentes do Sentinel acessam o barramento de mensagens e o Sentinel faz o seguinte:

- Armazena eventos em um repositório de dados baseado em arquivo com políticas flexíveis e personalizáveis de retenção de dados.
- Permite vincular hierarquicamente diversos sistemas Sentinel, inclusive o Sentinel Log Manager, o Sentinel e o Sentinel Rapid Deployment.
- Permite pesquisar eventos não apenas no servidor Sentinel local, mas também em outros servidores Sentinel distribuídos no mundo.
- Realiza uma análise estatística que permite definir uma linha de base e, depois, compará-la ao que está acontecendo a fim de determinar se há problemas que passaram despercebidos.
- Correlaciona um conjunto de eventos semelhantes ou comparáveis em determinado período para estabelecer um padrão.
- Organiza os eventos por incidente a fim de viabilizar gerenciamento de resposta e monitoramento eficientes.
- Gerar relatórios de recursos com base em eventos em tempo real e históricos.

As seções a seguir descrevem detalhadamente os componentes do Sentinel.

2.1 Fontes de eventos

O Sentinel reúne informações de segurança e eventos de diversas fontes no seu ambiente de TI. Essas fontes são denominadas fontes de eventos. As fontes de eventos podem representar inúmeros itens distintos na sua rede.

O gráfico a seguir mostra algumas fontes de eventos distintas das quais o Sentinel pode coletar informações:

Perímetro de Segurança: dispositivos e softwares usados para criar um parâmetro de segurança em seu ambiente.

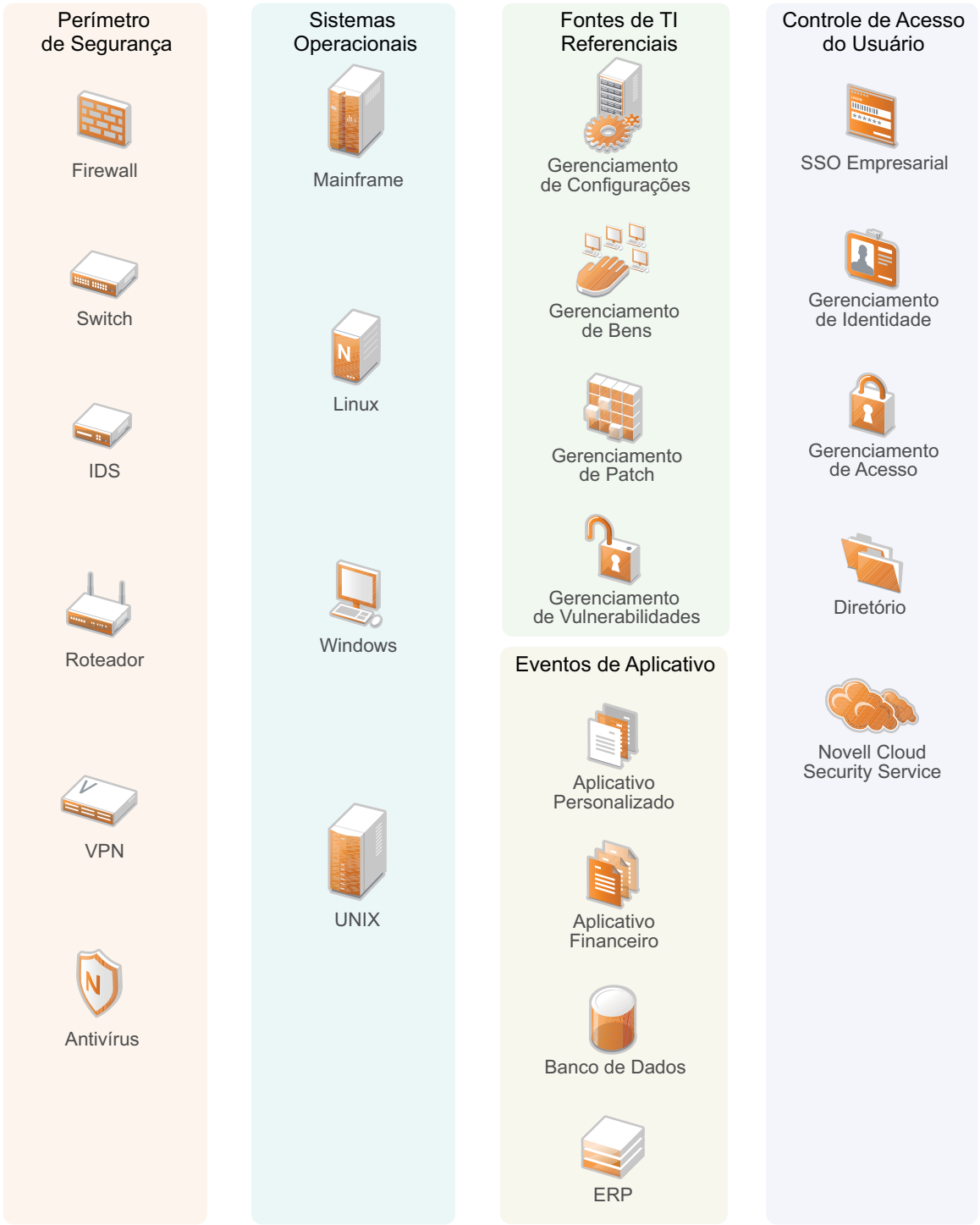
Sistemas Operacionais: eventos dos diferentes sistemas operacionais que são executados na rede.

Fontes de TI Referenciais: o software usado para manter e monitorar bens, patches, configurações e vulnerabilidade.

Eventos do Aplicativo: eventos gerados nos aplicativos instalados na rede.

Controle de Acesso de Usuário: eventos gerados nos aplicativos ou dispositivos que permitem aos usuários acessar os recursos da empresa.

Figura 2-2 *Fontes de eventos*



2.2 Evento do Sentinel

O Sentinel recebe informações de dispositivos, normaliza-as em uma estrutura chamada evento, categoriza o evento e, em seguida, envia-o para processamento. Adicionar informações de categoria (taxonomia) aos eventos facilita a comparação deles em sistemas que relatam eventos de forma diferente. Por exemplo, falhas na autenticação. Os eventos são processados pela exibição em tempo real, pelo mecanismo de correlação, por dashboards e pelo servidor back end.

Um evento consiste em mais de 200 campos. Os campos do evento têm tipos e finalidades diferentes. Alguns são predefinidos, como gravidade, importância, IP de destino e porta de destino. Há dois conjuntos de campos configuráveis: os campos reservados são de uso interno da Novell para permitir futuras expansões, enquanto que os campos de Cliente são para extensões de clientes.

Para mudar a finalidade de um campo, basta renomeá-lo. A origem de um campo pode ser referencial ou externa, a qual é definida explicitamente pelo dispositivo ou pelo Coletor correspondente. O valor de um campo referencial é computado como uma função de um ou mais campos que usam o serviço de mapeamento. Por exemplo, um campo pode ser definido como o código da construção que contém o bem mencionado como o IP de destino de um evento. Por exemplo, um campo pode ser computado pelo serviço de mapeamento por meio de um mapa definido pelo cliente usando o IP de destino do evento.

- Seção 2.2.1, “Serviço de Mapeamento” na página 15
- Seção 2.2.2, “Transmitindo mapas” na página 16
- Seção 2.2.3, “Detecção de exploração (serviço de mapeamento)” na página 16

2.2.1 Serviço de Mapeamento

O Serviço de Mapeamento permite que um mecanismo sofisticado propague dados comerciais importantes por todo o sistema. Esses dados podem aprimorar eventos com informações referenciais que fornecem contexto, permitindo que os analistas tomem melhores decisões, escrevam relatórios mais úteis e regras de correlação melhor definidas.

Você pode aprimorar os dados de evento usando mapas para adicionar informações (como detalhes do host e da identidade) aos eventos recebidos de seus dispositivos de origem. Essas informações adicionais podem ser usadas para correlação avançada e geração de relatórios. O sistema suporta vários mapas integrados e também mapas personalizados definidos pelo usuário

Os mapas definidos no Sentinel são armazenados de duas formas:

- Os mapas integrados são armazenados no banco de dados, atualizados com o APIs no código do Coletor e exportados automaticamente para o serviço de mapeamento.
- Os mapas personalizados são armazenados como arquivos CSV e podem ser atualizados no sistema de arquivos ou via IU de Configuração de Dados de Mapa e, em seguida, carregados pelo Serviço de mapeamento.

Em ambos os casos, os arquivos CSV são mantidos no servidor central do Sentinel, mas as alterações feitas nos mapas são distribuídas para cada Gerenciador de Coletor e aplicadas localmente. Esse processamento distribuído garante que a atividade de mapeamento não sobrecarregue o servidor principal.

2.2.2 Transmitindo mapas

O Serviço de Mapeamento emprega um modelo de atualização dinâmica e transmite os mapas de um ponto para outro, evitando o acúmulo de grandes mapas estáticos na memória dinâmica. A importância desse recurso de transmissão é especialmente relevante em um sistema em tempo real que seja vital para os negócios, como o Sentinel, no qual é preciso haver uma movimentação de dados constante, previsível e ágil, qualquer que seja a carga transiente no sistema.

2.2.3 Detecção de exploração (serviço de mapeamento)

O Sentinel permite a referência cruzada entre as assinaturas dos dados de eventos e os dados do Vulnerability Scanner. Os usuários são notificados de forma automática e imediata em caso de tentativa de ataque para explorar um sistema vulnerável. Isso é possível graças à:

- Alimentação do Consultor;
- Detecção de intrusão;
- Verificação de vulnerabilidades; e
- Firewalls

O Consultor fornece uma referência cruzada entre as assinaturas de dados do evento e os dados do verificador de vulnerabilidades. O feed do Advisor contém informações sobre vulnerabilidades e ameaças, uma normalização de assinaturas de evento e plug-ins de vulnerabilidade. Para obter mais informações sobre o Advisor, consulte "Configurando o Advisor" no *Guia de Administração do NetIQ Sentinel 7.0.1*.

2.3 Conectores

Os Conectores fornecem a conexão entre as fontes de eventos e o sistema Sentinel. Usando protocolos padrão para obter eventos, como syslog, JBDC para ler a partir de tabelas de bancos de dados, WMI para ler a partir de registros de eventos do Windows e outros, os Conectores fornecem:

- Transporte dos dados de eventos iniciais das fontes de eventos para o Coletor.
- Filtro específico para conexão; e
- Gerenciamento de erros da conexão.

2.4 Coletores

Os Coletores normalizam e coletam informações dos Conectores. Os coletores são gravados em Javascript e definem a lógica para:

- Receber dados iniciais dos Conectores;
- Analisar e normalizar os dados;
- Aplicar lógica repetida aos dados;
- Traduzir dados específicos do dispositivo em dados específicos do Sentinel;
- Formatar os eventos;
- Passar os dados normalizados, analisados e formatados para o Gerenciador de Coletor.

2.5 Gerenciador de Coletor

O Gerenciador de Coletor do gerencia coletas de dados, monitora mensagens de status do sistema e filtra eventos, conforme necessário. As principais funções do Gerenciador de Coletor incluem:

- Transformar eventos;.
- Adicionar relevância empresarial aos eventos por meio do serviço de mapeamento.
- Realizar filtragem global do eventos;
- Rotear eventos;
- Determinar dados em tempo real, de vulnerabilidade, de bens e não tempo real; e
- Enviar mensagens de saúde ao servidor Sentinel.

2.6 Barramento de comunicação

A arquitetura do barramento de comunicação é criada a partir de uma arquitetura SOA (Service-Oriented Architecture) baseada em padrões, que combina as vantagens do processamento na memória e da computação distribuída. O barramento de comunicação é chamado de iSCALE; trata-se de um barramento de mensagens especial com capacidade para gerenciar grandes volumes de dados.

- Seção 2.6.1, “Barramento de mensagem” na página 17
- Seção 2.6.2, “Canais” na página 18

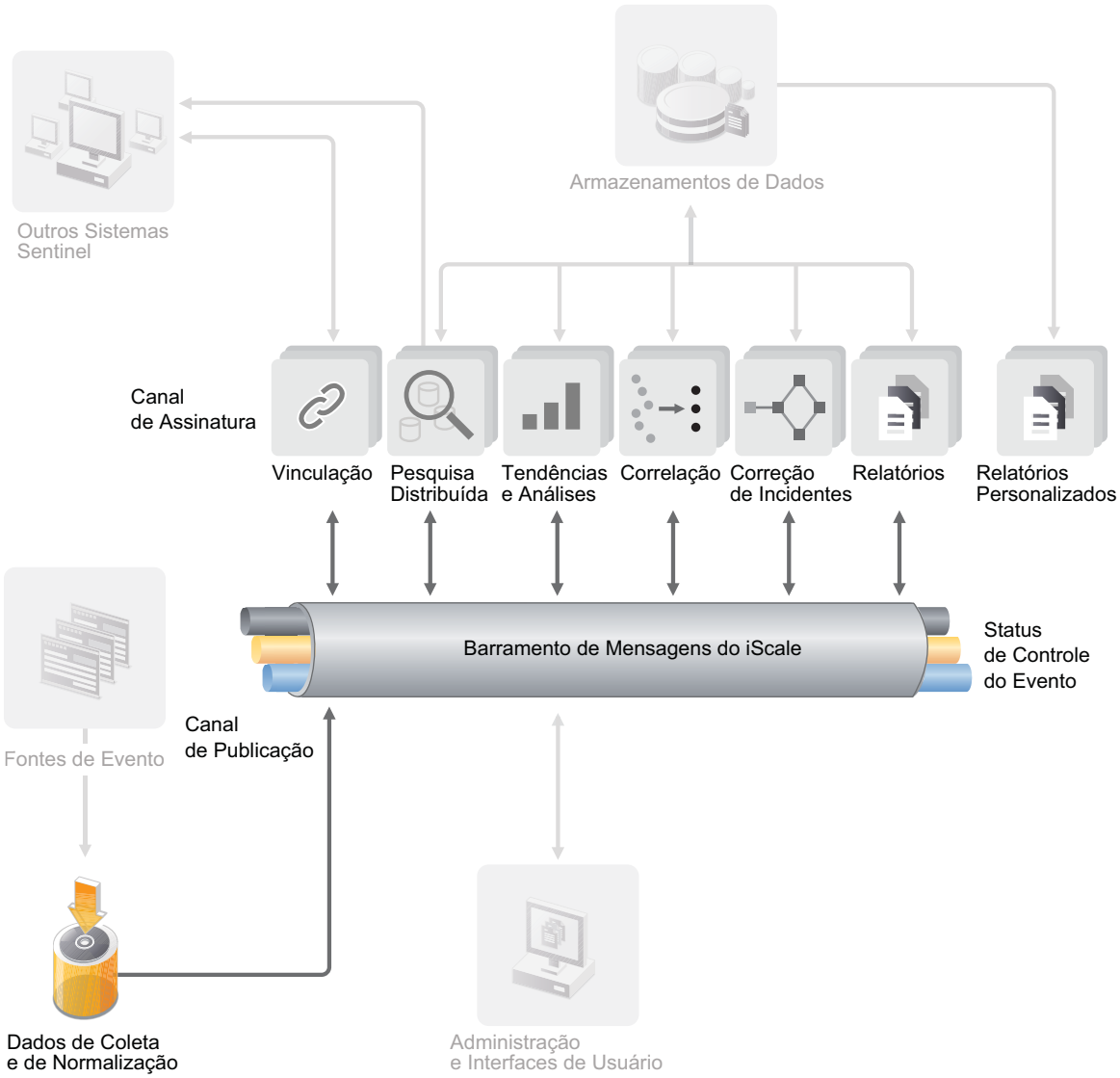
2.6.1 Barramento de mensagem

O barramento de mensagens da iSCALE permite escalar de modo independente os componentes individuais, ao mesmo tempo em que possibilita a integração baseada em padrões com aplicativos externos. O segredo da escalabilidade é o fato de que, ao contrário de outros softwares distribuídos, nenhum componente (peer) comunica-se com outro diretamente. Todos os componentes comunicam-se por meio do barramento de mensagens, capaz de mover milhares de pacotes de mensagens por segundo.

Ao tirar proveito dos exclusivos recursos do barramento de mensagem, o canal de comunicação de alto throughput pode maximizar e manter a alta taxa de throughput de dados que atravessam os componentes independentes do sistema. Os eventos são compactados e criptografados via cabo para distribuição segura e eficiente da borda da rede ou pontos de coleta para o hub do sistema, no qual são realizadas análises em tempo real.

O barramento de mensagens da iSCALE emprega uma série de serviços de enfileiramento que melhoram a confiabilidade da comunicação além dos aspectos de segurança e desempenho da plataforma. Com inúmeras filas transientes e permanentes, o sistema oferece confiabilidade e tolerância a falhas inigualáveis. Por exemplo, mensagens importantes em trânsito são gravadas (ao serem colocadas em fila) em caso de falha na via de comunicação. A mensagem em fila é enviada ao destino depois que o sistema se recupera do estado de falha.

Figura 2-3 *Barramento de Mensagens iSCALE*



2.6.2 Canais

A plataforma iSCALE emprega um modelo orientado por dados ou eventos que permite escalar os componentes de todo o sistema de maneira independente e de acordo com a carga de trabalho. Isso garante um modelo de implantação flexível, já que existem variações no ambiente de cada cliente: um site contém um grande número de dispositivos com baixo volume de eventos enquanto que outro site tem poucos dispositivos com grande volume de eventos. As densidades de evento (ou seja, o padrão de agregação e de multiplexação dos eventos no cabo a partir dos pontos de coleta) são diferentes nesses casos, e o barramento de mensagens permite escalar, de modo coerente, cargas de trabalho díspares.

A iSCALE tira proveito de um ambiente independente e com canais múltiplos que praticamente elimina a contenção e promove o processamento paralelo de eventos. Esses canais e subcanais trabalham não somente para transportar dados de eventos, como também para oferecer um controle refinado de processos a fim de escalar e equilibrar a carga do sistema em condições de carga

variáveis. Ao usar canais de serviço independentes, como os canais de controle e de status, além do canal de eventos principal, a iSCALE permite escalar de modo econômico e sofisticado a arquitetura orientada por eventos.

2.7 Armazenamento de dados no Sentinel

O Sentinel oferece diversas opções para armazenar os dados coletados. Por padrão, o Sentinel recebe dois fluxos de dados diferentes, porém muito parecidos, do Collector Managers: os dados de eventos e os dados iniciais. Esses dados são armazenados no sistema de arquivos local do servidor Sentinel.

Você pode configurar o Sentinel para armazenar dados em um local de armazenamento na rede. E também pode configurar o Sentinel para armazenar dados de eventos em um banco de dados externo usando as políticas de sincronização de dados. Para obter mais informações, consulte "Configurando o armazenamento de dados" no *Guia de Administração do NetIQ Sentinel 7.0.1*.

2.8 Filtros

No Sentinel, os filtros permitem personalizar a pesquisa de eventos e, assim, evitar a sobrecarga de dados. Esse recurso fornece um Construtor de Filtros que o ajuda a definir consultas de pesquisa das mais simples às mais complexas. Você pode salvar uma consulta de pesquisa como um filtro e reutilizá-lo sempre que necessário. Assim, você poderá realizar uma pesquisa selecionando apenas um filtro em vez de ter que especificar a consulta manualmente todas as vezes.

É possível reutilizar filtros durante a utilização ou a configuração de recursos do Sentinel, como:

- Criando painéis do Security Intelligence.

  Para obter mais informações, consulte "Criando painéis" no *Guia do Usuário do NetIQ Sentinel 7.0.1*.

- Visualização de eventos em tempo real no Active Views.

  Para obter mais informações, consulte a seção "Visualizando eventos" no *Guia do Usuário do NetIQ Sentinel 7.0.1*.

- Configurando uma política de retenção de dados.

  Para obter mais informações, consulte a seção "Configurando políticas de retenção de dados" no *Guia de Administração do NetIQ Sentinel 7.0.1*.

- Configurando a sincronização de dados.

  Para obter mais informações, consulte "Configurando a sincronização de dados" no *Guia de Administração do NetIQ Sentinel 7.0.1*.

- Testando uma regra de correlação.

  Para obter mais informações, consulte a seção "Correlacionando dados de eventos" no *Guia do Usuário do NetIQ Sentinel 7.0.1*.

Por padrão, o Sentinel fornece uma lista dos filtros. Você também pode criar seus próprios filtros. Para obter mais informações, consulte "Configurando filtros" no *Guia do Usuário do NetIQ Sentinel 7.0.1*.

2.9 Correlação

Um único evento pode parecer comum, mas quando combinado com outros eventos, ele pode informar você sobre um problema potencial. O Sentinel ajuda você a correlacionar os eventos em questão usando as regras que você cria e implementa no Mecanismo de correlação e toma a medida necessária para reduzir os problemas.

A correlação agrega inteligência ao gerenciamento de eventos de segurança, automatizando a análise do fluxo de eventos de entrada para encontrar padrões relevantes. A correlação permite definir regras que identificam as ameaças importantes e padrões complexos de ataque, para que você consiga priorizar os eventos e iniciar o gerenciamento e a resposta eficazes aos incidentes. Para obter mais informações, consulte a seção "Correlacionando dados de eventos" no *Guia do Usuário do NetIQ Sentinel 7.0.1*.

2.10 Inteligência de segurança

O recurso de correlação do Sentinel fornece a capacidade de conhecer padrões de atividade, sejam eles para segurança, conformidade ou outros fins. O recurso Security Intelligence procura atividades fora do comum e que possam ser maliciosas, mas que não correspondem a nenhum padrão conhecido.

O recurso Inteligência de Segurança do Sentinel concentra-se na análise estatística dos dados de séries cronológicas para permitir que os analistas identifiquem e analisem desvios (anomalias) usando um mecanismo estatístico automático ou uma representação visual dos dados estatísticos para interpretação manual. Para obter mais informações, consulte "Analisando tendências em dados" no *Guia do Usuário do NetIQ Sentinel 7.0.1*.

2.11 iTrac

Os fluxos de dados iTRAC foram projetados para fornecer uma solução simples e flexível de automatização e monitoramento dos processos de resposta a incidentes em uma empresa. O iTRAC aproveita o sistema interno de incidentes do Sentinel para monitorar problemas de segurança ou do sistema desde a identificação (através de regras de correlação ou de identificação manual) até a solução.

Os workflows podem ser criados usando etapas manuais ou automáticas. Recursos avançados, como ramificação, escalonamento em tempo real e variáveis locais, são suportados A integração com scripts e plug-ins externos permite uma interação flexível com sistemas de terceiros. A geração de relatórios abrangente permite que os administradores compreendam e ajustem os processos de resposta a incidente. Para obter mais informações, consulte a seção "Configurando workflows do iTRAC" no *Guia do Usuário do NetIQ Sentinel 7.0.1*.

2.12 Relatórios

O Sentinel fornece um recurso para executar relatórios nos dados coletados. O Sentinel vem com diversos relatórios personalizáveis, sendo que alguns são de uso geral e outros destinados a dispositivos específicos (como o SUSE Linux). Alguns desses relatórios apresentam flexibilidade para permitir que os usuários especifiquem as colunas que devem ser exibidas nos resultados.

Os usuários podem executar, programar e enviar relatórios em PDF por e-mail. Eles também podem executar qualquer relatório como uma pesquisa e, depois, interagir com os resultados como em uma pesquisa (refinando a pesquisa ou executando ações com os resultados). Você também pode executar relatórios nos servidores Sentinel localizados em diferentes locais. Para obter mais informações, consulte "Geração de relatórios" no *Guia do Usuário do NetIQ Sentinel 7.0.1*.

2.13 Análise de eventos

O Sentinel fornece um conjunto de ferramentas avançadas para ajudar você a encontrar e analisar mais facilmente dados críticos de eventos. O sistema é ajustado e otimizado para obter a máxima eficiência em qualquer tipo de análise específica, e os métodos para executar facilmente transições de um tipo de análise para outro são fornecidos a fim de obter transições contínuas.

A investigação de eventos do Sentinel geralmente começa com as Telas Ativas em tempo real. Embora ferramentas mais avançadas estejam disponíveis, as Telas ativas exibem fluxos de evento filtrados juntamente com gráficos resumidos que podem ser usados para análises simples e gerais de tendências de evento, dados de evento e identificação de eventos específicos. Ao longo do tempo, você cria filtros ajustados para classes de dados específicas, como os resultados da correlação. Você pode usar as Telas ativas como um painel mostrando um comportamento geral operacional e de segurança.

Em seguida, você pode usar a pesquisa interativa para executar análises mais detalhadas de eventos. Isso permite que você pesquise e encontre de forma mais rápida e fácil dados relacionados a uma consulta específica, como a atividade de um usuário específico ou em sistema específico. Clicar nos dados do evento ou usar o painel de refinamento do lado esquerdo permite focar eventos de interesse específicos.

Ao analisar centenas de eventos, os recursos de relatório do Sentinel fornecem controle personalizado sobre o layout do evento o podem exibir volumes de dados maiores. O Sentinel facilita essa transição permitindo transferir as pesquisas interativas criadas na Interface de pesquisa para um modelo de relatório, o qual cria instantaneamente um relatório que exibe os mesmos dados em um formato que se adequa melhor a uma quantidade maior de eventos.

O Sentinel inclui vários modelos para esse fim. Alguns modelos são ajustados para exibir tipos específicos de informações, como dados de autenticação ou criação de usuários, e outros modelos são para fins gerais que permitem personalizar grupos e colunas de forma interativa no relatório.

Ao longo do tempo, você desenvolverá filtros e relatórios usados com frequência que facilitarão seus fluxos de trabalho. O Sentinel suporta totalmente o armazenamento e a distribuição dessas informações para as pessoas da sua empresa. Para obter mais informações, consulte o *Guia do Usuário do NetIQ Sentinel 7.0.1*.