ManageEngine
EventLog Analyzer

Monitoramento da integridade do arquivo com o EventLog Analyzer

Introdução

As empresas geralmente usam sistemas baseados em arquivos para organizar, armazenar e processar informações, e o monitoramento de integridade do arquivo (FIM) é uma técnica de monitoramento de mudanças que ajuda a garantir a segurança dos dados armazenados em arquivos e pastas críticos. Uma técnica abrangente de FIM monitora continuamente arquivos e pastas em busca de mudanças inesperadas ou não autorizadas e coleta instantaneamente informações contextuais importantes, incluindo quem a fez, quando e de onde.

Importância do FIM

O FIM é usado para realizar a auditoria de mudanças feitas em seus arquivos e pastas mais importantes, como:

- Arquivos binários de softwares importantes do sistema, incluindo sistemas operacionais, compiladores, montadores e drivers.
- Configurações, definições e outros arquivos importantes da aplicação.
- Arquivos essenciais aos negócios que contêm dados confidenciais, como informações de clientes.
- Arquivos de log relacionados à atividade da rede.

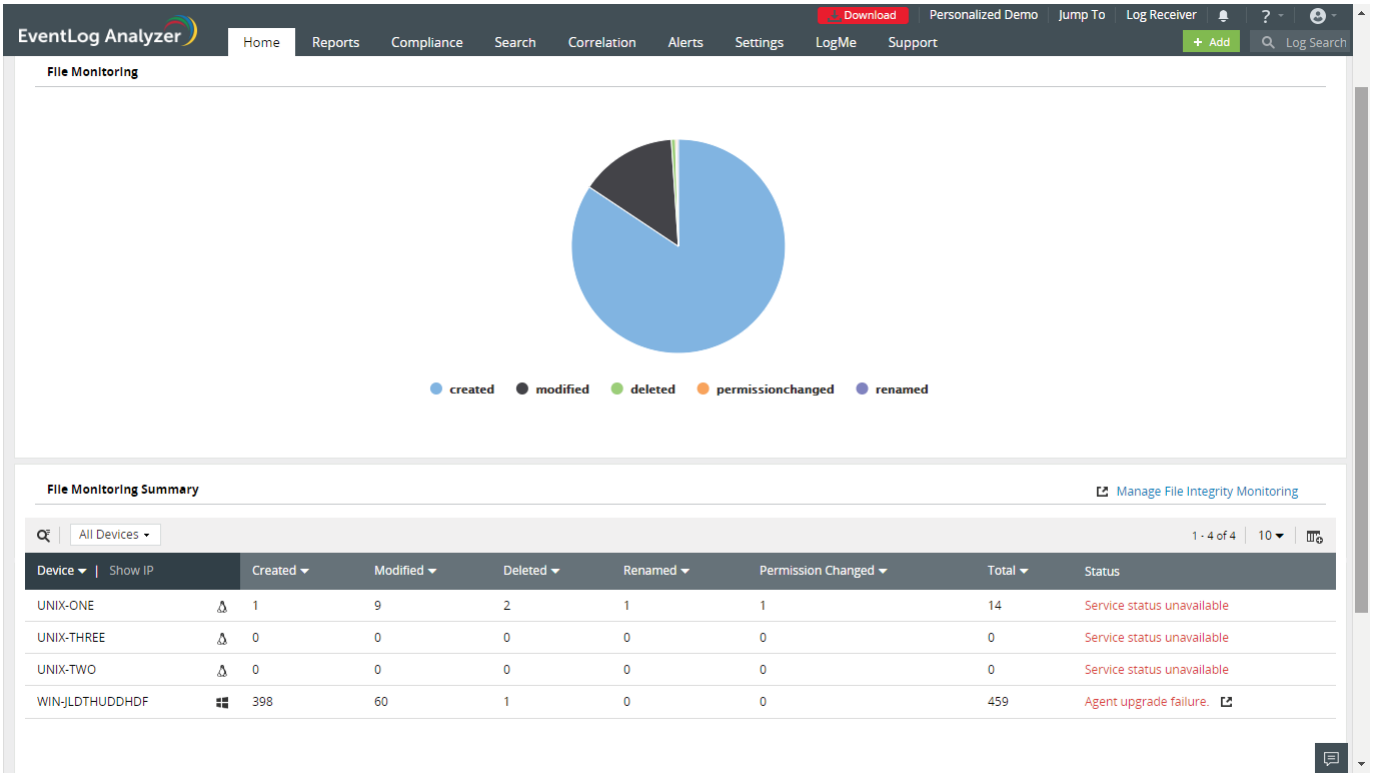
Esses arquivos são a base sobre a qual sua rede e sua empresa são executadas. Os arquivos e suas várias configurações determinam como seus sistemas operam. Eles armazenam seus dados de negócios, determinam como várias atividades de negócios são conduzidas e registram em logs toda a rede.

Os efeitos de ondulação causados por modificações nesses arquivos podem ser desastrosos. Um arquivo de log excluído pode fazer com que você perca completamente um incidente de segurança enquanto os invasores roubem seus dados comerciais. Isso também pode prejudicar sua investigação forense depois que você descobre o incidente e pode levar a cobranças graves contra sua empresa por falta de conformidade.

Um único arquivo de sistema corrompido pode causar uma falha em um servidor crítico, resultando em tempo de inatividade que sua empresa não pode arcar com os custos. Além disso, as mudanças feitas nas pastas onde os dados confidenciais são armazenados também podem se tornar uma causa de preocupação. Por exemplo, o malware inserido em locais críticos pode ajudar os invasores em seus esforços para assumir a rede.

As alterações desastrosas em arquivos também podem, às vezes, ser apenas o resultado de erro ou supervisão. Além de monitorar seus arquivos e pastas em busca de alterações suspeitas, o FIM ajuda a rastrear mudanças acidentais de arquivos. Ele ainda ajuda você a manter-se em conformidade com importantes políticas normativas, como o padrão PCI-DSS e a lei HIPAA.

Destaques do FIM com o EventLog Analyzer



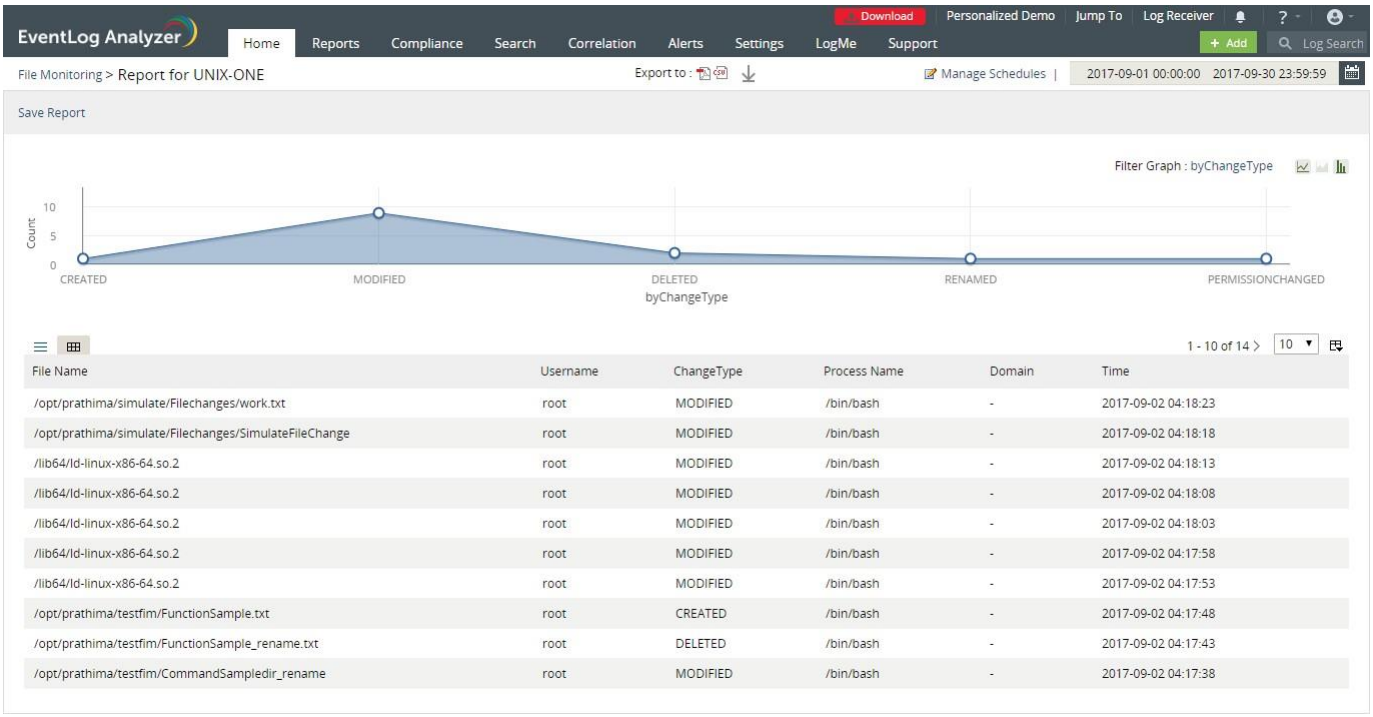
O módulo FIM do EventLog Analyzer monitora os dados críticos em seus sistemas Windows e Linux quanto mudanças. Ele é fácil de usar e permite revisar as mudanças feitas em arquivos em sua rede a partir de um console centralizado. Alguns dos destaques são:

- **Fácil configuração.** A configuração do FIM usando o EventLog Analyzer requer o mínimo de esforço do usuário. É possível configurar vários dispositivos simultaneamente e os agentes FIM necessários serão instalados automaticamente nesses dispositivos. Todas as políticas de auditoria, atualizações de agentes e configurações de SACL necessárias são atualizadas automaticamente.

- **Alto grau de controle.** Você pode exercer o controle sobre os arquivos e pastas que deseja monitorar. Os recursos a seguir fornecem controle granular:

  - **Templates.** Crie modelos para agrupar os locais de arquivos e pastas que deseja monitorar e aplicá-los a quantos dispositivos forem necessários. Ao modificar esses templates uma vez, você pode aplicar a alteração a todos os dispositivos, mesmo aqueles configurados anteriormente usando esse modelo. Os modelos predefinidos também são fornecidos para arquivos e pastas essenciais comuns.

  - **Filtros.** Você pode optar por incluir ou excluir subpastas, arquivos específicos ou tipos de arquivo.



- **Relatórios e alertas detalhados.** O painel FIM fornece uma visão geral de todas as mudanças feitas nos arquivos e pastas que você está monitorando. Relatórios e alertas também estão disponíveis para cada dispositivo independente monitorado. Esses relatórios fornecem detalhes sobre as seguintes mudanças:

  - **Criações.** Saiba quando os arquivos são criados ou copiados em pastas críticas. Isso ajuda a identificar e impedir a disseminação de malware.
  - **Modificações.** Controle as mudanças em arquivos importantes e evite que as maliciosas corrompam dados confidenciais.
  - **Exclusões.** Proteja contra a perda de dados identificando arquivos confidenciais que foram excluídos para que você possa restaurá-los imediatamente de um backup.
  - **Renomear.** Identifique os arquivos que foram movidos ou renomeados. Várias aplicações dependem de arquivos específicos e uma movimentação ou renomeação incorreta pode prejudicar as operações da empresa.
  - **Mudanças de permissão.** Controle as mudanças de permissão e garanta que ninguém obtenha acesso não autorizado a arquivos críticos.

- **Conformidade.** Gere relatórios de conformidade predefinidos para várias políticas, incluindo as leis PCI-DSS, FISMA, HIPAA e RGPD, além de fornecer detalhes sobre várias operações de arquivos conforme exigido.

Conclusão

Você pode estar lidando com informações comerciais confidenciais, definições de rede ou configurações. De qualquer forma, os arquivos armazenam muitos dados e isso é vital para o bom funcionamento da sua rede e da empresa. O FIM é um processo essencial que todas as organizações devem seguir para preservar a integridade dos dados e proteger sua rede contra ataques. Com a capacidade FIM do EventLog Analyzer, é possível monitorar arquivos em plataformas Windows e Linux com facilidade, garantindo que fiquem seguros.