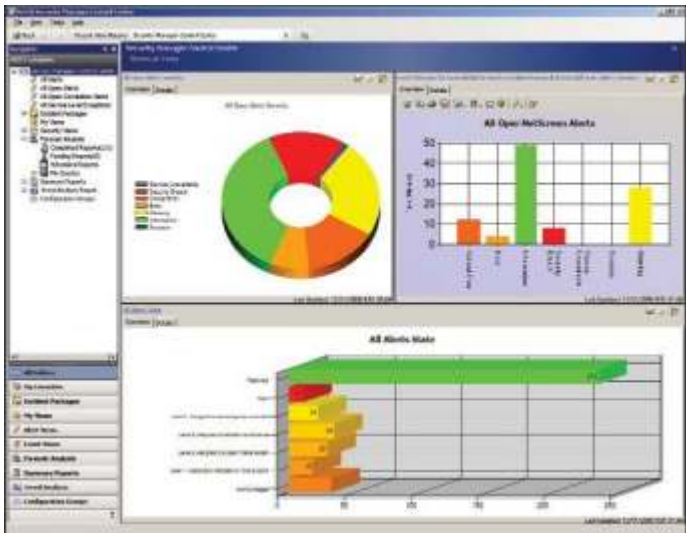
NetIQ Security Manager™

Proteja os dados críticos, automatize as tarefas de certificação de conformidade e agilize a resposta aos incidentes com gerenciamento integrado de eventos e das informações sobre segurança

Visão Geral

A solução NetIQ Security Manager oferece monitoramento em tempo real das mudanças no sistema e das atividades dos usuários, da detecção das ameaças e invasões, correlação e gerenciamento dos eventos relacionados à segurança, gerenciamento de logs e automação da resposta aos incidentes — tudo isso em uma infra-estrutura única, integrada e escalável. Atende aos exigentes requisitos de conformidade automatizando a análise da segurança, mantendo os logs, gerenciando as ameaças, as respostas aos incidentes e fazendo auditoria nas mudanças..



A solução NetIQ Security Manager apresenta uma solução prática para proteção contra invasões, gerenciando e correlacionando os eventos de segurança e executando análise forense e de tendências.

Soluções Inovadoras

Para atender as necessidades de segurança e disponibilidade, as empresas continuam investindo em uma ampla variedade de soluções pontuais de segurança como firewalls, produtos antivírus e sistemas para detecção de invasão. Essas tecnologias geram um volume enorme de dados, um tremendo desafio para a detecção de falhas na segurança em tempo real, sem contar na complexidade para a análise desses dados. A solução NetIQ Security Manager aumenta o valor da infra-estrutura de segurança existente porque consolida e arquiva dados de logs e eventos de toda a empresa. A solução oferece uma base abrangente de conhecimento para análise e correção. E ainda protege os dados nos sistemas legados como servidores, estações de trabalho, bases de dados e infra-estrutura do Active Directory.

Principais Benefícios

Menos tempo de exposição – Otimiza os tempos de reação com monitoramento em tempo real dos incidentes de segurança, funcionalidades abrangentes de notificação e informação e respostas automatizadas.

Melhor conhecimento sobre a segurança – Apresenta uma base abrangente de conhecimento que automaticamente coleta inteligência sobre a segurança e absorve informações novas e atualizadas. Isso ajuda a garantir a conhecimento disponível para entender e responder aos incidentes sempre que necessário.

Maior proteção – Integra e correlaciona dados arquivados e em tempo real de todos os sistemas e processos de segurança. Controlando os incidentes para garantir que eles sejam tratados adequadamente e em tempo, você consegue gerenciar efetivamente o ciclo de vida dos incidentes e melhorar a proteção.

Agiliza as operações – Melhora o retorno sobre o investimento consolidando as informações sobre segurança de toda a empresa em um único local, filtrando o ruído e os falsos positivos e apresentando os incidentes. Isso facilita o monitoramento direcionado e agiliza as respostas.

Garante a conformidade – Facilita a análise periódica e emissão de relatórios sobre a segurança corporativa, monitora os controles de segurança para validar a eficiência e ainda ativa as políticas e melhores práticas em tempo real, ajudando a responder aos requisitos de segurança das regulamentações.

Principais Funcionalidades

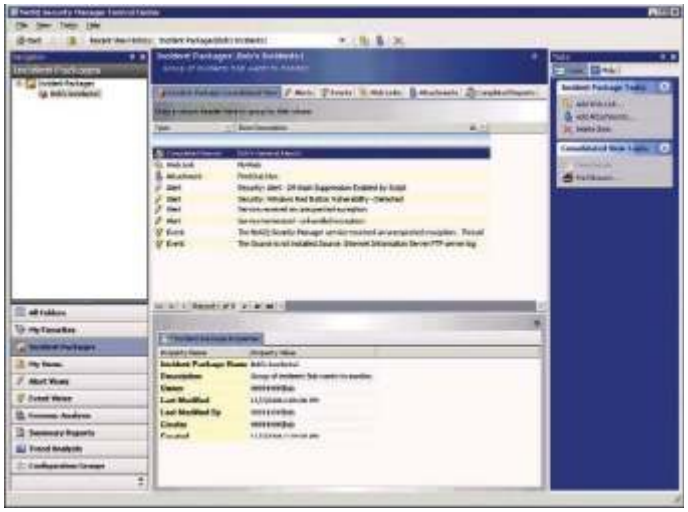
Gerenciamento de Log e Forense
Pronta identificação das ameaças ocultas, atendendo aos requisitos de auditoria e regulamentares com consolidação de eventos e log centralizado, aliados a poderosas ferramentas de análise forense e de tendências.

Ajuda a satisfazer os requisitos legais de retenção de registro – Uma solução simples e poderosa que permite que você atenda requisitos regulamentares e de auditoria com relação aos logs e informações sobre os eventos de segurança que precisam ser coletadas e mantidas por um longo período.

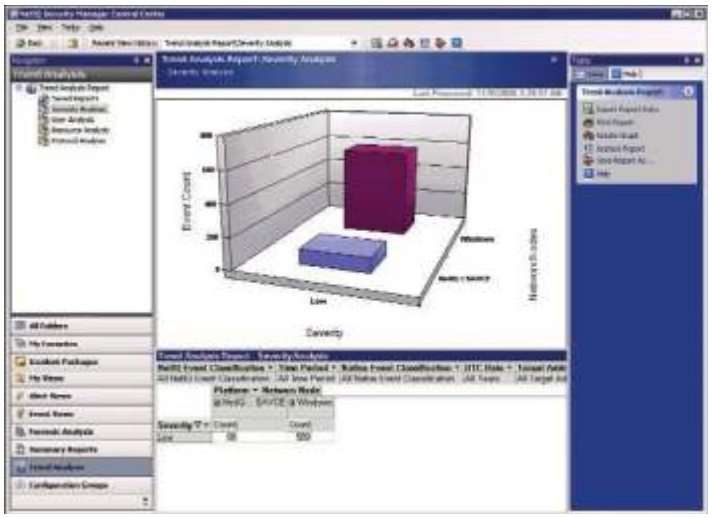
Facilita a análise periódica das informações relacionadas à segurança – Apresenta relatórios com dados resumidos sobre a segurança e informações importantes como tentativas falhas de logon). Para uma análise mais detalhada, clique no relatório. Atualizados diariamente, esses relatórios facilitam a análise das informações associadas à segurança e ajudam as atender aos requisitos de melhores práticas e regulamentares.

Análise das tendências de segurança – Apresentação das atividades associadas à segurança e rápida identificação de qualquer anomalia graças a relatórios de análise de tendência detalhados e flexíveis. Gráficos e funcionalidades de manipulação de dados apresentam diferentes representações visuais das informações sobre segurança.

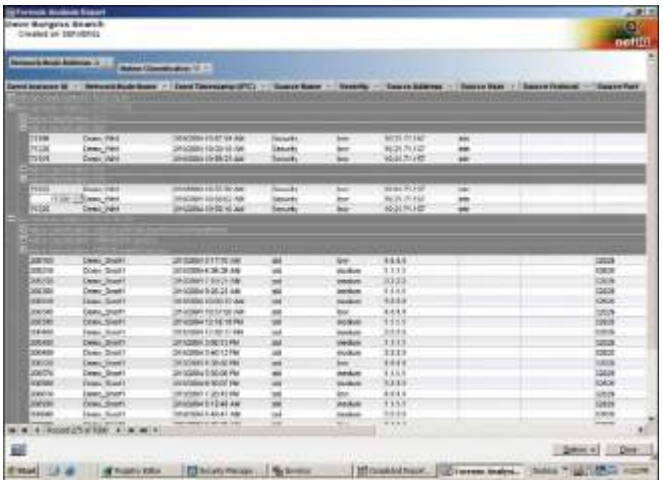
Poderosas funcionalidades para investigação forense – Reduz substancialmente o tempo necessário para detectar a causa raiz de um incidente ou anomalia, graças à poderosa análise forense. A interface de emissão de relatórios forenses permite filtrar, agrupar e classificar os alertas para melhor garimpagem dos dados.



A solução NetIQ Security Manager permite que os administradores reúnam facilmente informações sobre a segurança, de forma a ajudar na pesquisa e reduzir os tempos de resposta aos incidentes.



Poderosas ferramentas de análise apresentam diferentes quadros sobre a segurança corporativa que ajudam na identificação de tendências bem como a detectar anomalias e possíveis ameaças.



Relatórios forenses oferecem funcionalidades abrangentes de garimpagem de dados como filtragem, classificação e agrupamento dos elementos dos dados, agilizando a identificação da causa-raiz dos incidentes.

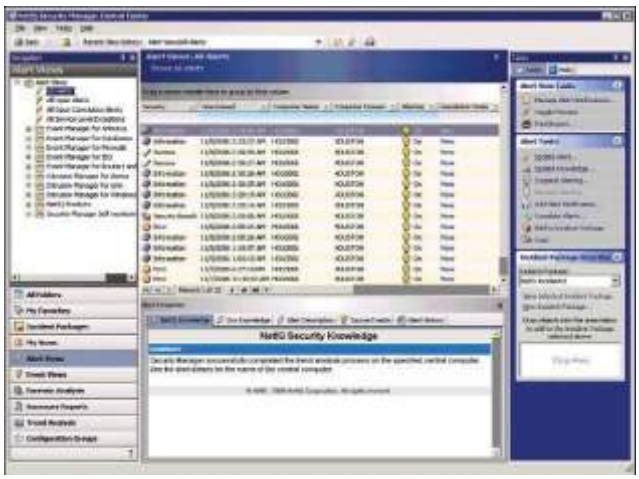
Controle de Acesso e Monitoramento de Usuários
A solução melhora a disponibilidade do sistema, a garantia dos serviços e protege a propriedade intelectual graças ao controle de acesso e monitoramento das atividades dos usuários em tempo real. Uma abrangente Base de Conhecimento ajuda na interpretação e resposta aos incidentes.

Facilita a resposta rápida aos incidentes – Oferece notificação imediata das falhas de segurança e violações de políticas com notificação e alertas em tempo real, permitindo reagir rapidamente e minimizar os riscos de qualquer dano.

Minimiza o tempo de exposição às ameaças – Responde em tempo real aos incidentes detectados, oferecendo proteção imediata porque bloqueia os ataques em andamento. A interface orientada por assistentes facilita a criação e personalização das respostas, sem necessidade de conhecimento em programação.

Protege contra alterações maliciosas e acidentais – Detecta e alerta sobre atividades autorizadas e não-autorizadas nos recursos do sistema do legado executadas por usuários finais ou administradores do sistema ou da rede. Entre as atividades podem estar logins e logoffs, mudanças de privilégio, limpeza de arquivo de log, mudanças nas permissões de auditoria e instalação de softwares.

Melhora a eficiência e o conhecimento do pessoal sobre a segurança – Contém Base de Conhecimento sobre segurança, detalhando as possíveis causas dos alertas. Esse conhecimento interno pode ser expandido com informações específicas como procedimentos para tratamento dos incidentes. Com isso o conhecimento é alimentado e reaproveitado por outras pessoas e não se perde quando algum funcionário deixa a empresa.



Uma Base de Conhecimento de segurança expansível centraliza o monitoramento e as respostas aos alertas de segurança gerados em qualquer parte da empresa.

A solução Security Manager reduz os ruídos e falsos positivos porque correlaciona os eventos de vários sensores de segurança e identifica com precisão os incidentes críticos de segurança.

Análise e Correlação de Eventos sobre Segurança
Apresenta informações valiosas e em tempo real sobre a segurança que representam a real postura da sua empresa com relação à segurança, separando os incidentes reais dos ruídos e falsos positivos, agilizando e simplificando a as respostas.

Maximiza o valor da infra-estrutura de segurança – Otimiza suas defesas via uma central de operações de segurança que coleta, correlaciona, analisa e responde com segurança aos eventos nos principais ativos, produtos pontuais de segurança e dispositivos de rede.

Reduz os ruídos e falsos positivos – Poderoso mecanismo de correlação em tempo real minimiza as informações irrelevantes, eliminando a necessidade de classificar os eventos e permitindo que as equipes de segurança visualizem e mantenham o foco em incidentes reais. Um assistente de correlação permite a rápida criação e entrada em vigor de novas regras de correlação.

Garantia de que os incidentes de segurança não serão perdidos nem esquecidos – O fluxo de trabalho de controle interno dos incidentes permite que as empresas priorizem imediatamente os incidentes e controlem o status dos mesmos, sempre que necessário. Podem ser acrescentadas informações sobre as atividades para criação de uma trilha de auditoria de como os incidentes são tratados.

Garantia de disponibilidade das atualizações mais recentes – Oferece um mecanismo prático e dinâmico para receber notificações de atualização de funcionalidades e outras informações. Também facilita a trabalhosa entrega e instalação dessas atualizações graças à tecnologia NetIQ AutoSync.

Sumário Técnico

Console Unificadas das Operações de Segurança – Uma console Win32 para os analistas da segurança e pessoal de operações que suporta alertas em tempo real, log para análise forense, coleta de informações sobre incidentes etc.

Mecanismo de Correlação Baseado em Regras – Os Computadores Centrais exercem um papel especial na correlação de eventos em tempo real. A correlação baseia-se em regras para a identificação de seqüências ou conjuntos de eventos e violações de limite em diversas tecnologias. Por exemplo, os eventos dos firewalls podem ser correlacionados com eventos dos servidores.

Coleta e Arquivamento de Log – Oferece tecnologia proprietária de gerenciamento de log para a coleta de dados de log localmente nos sites remotos e ainda apresenta análises e relatórios sobre que abrangem toda a empresa. Utiliza tecnologia OLAP para apresentar diferentes tipos de relatórios.

Monitoramento e Coleta com e sem Agente – Os agentes são responsáveis pela coleta e processamento local dos dados, oferecendo funcionalidades poderosas como monitoramento de usuários, detecção de mudanças, consultas SID e muito mais. Ajudam na flexibilidade das implementações.

Detecção de Mudanças – Os agentes detectam as mudanças no sistema como modificações nos arquivos, aumento de privilégio de usuário, alterações no registro do Windows, alterações nos objetos do iSeries e muito mais.

Monitoramento de Usuário – Os agentes suportam poderoso monitoramento dos servidores e outros dispositivos. Um sistema de controle interno de incidentes ajuda na resposta rápida aos incidentes.

Sistemas e Dispositivos Suportados

A solução NetIQ Security Manager oferece suporte a uma ampla diversidade de terminais e aplicações, inclusive suporte a:

- Servidores e estações de trabalho – como Microsoft, Linux, Unix e iSeries
- Serviços críticos – como bancos de dados, Active Directory e infra-estrutura VoIP.
- Soluções pontuais de segurança – como produtos antivírus, firewalls, sistemas de detecção e proteção contra invasão.
- Dispositivos da rede – como os roteadores e os switches.
- Soluções NetIQ – como NetIQ Secure Configuration Manager™, NetIQ AppManager®, NetIQ Change Guardian for Windows, NetIQ Change Guardian™ for Active Directory, NetIQ Group Policy Guardian™.

Graças à sua funcionalidade AutoSync, a solução NetIQ Security Manager pode ser facilmente ampliada para monitorar outros produtos, sistemas e dispositivos. Entre em contato com um representante da NetIQ para obter mais informações sobre como a NetIQ pode ajudá-lo a suportar seu ambiente e requisitos específicos.

Requisitos Mínimos do Sistema

Computador Central:
- Dois processadores dual-core AMD/Intel com 16 GB de RAM
- Windows 2003
- MS-SQL Server 2005 SP2

Servidor de Arquivo de Log:
- Dois processadores dual-core AMD/Intel com 16 GB de RAM
- Windows 2003
- 500 GB de espaço em disco (depende dos requisitos do cliente)

Servidor de Relatórios:
- Dois processadores (Recomendado quatro) dual-core AMD/Intel com 16 GB de RAM
- Windows 2003
- MS-SQL Server (Enterprise Edition) 2005 SP2, (Analysis 2005 e SRS)

Sobre a Attachmate

A Attachmate, de propriedade de um grupo de investimento liderada pela Francisco Partners, Golden Gate Capital e Thoma Cressey Equity Partners, permite que departamentos de TI expandam o alcance dos serviços de missão crítica e garantam o gerenciamento, proteção e conformidade desses serviços. Entre os principais produtos da companhia estão soluções para conectividade com o legado, gerenciamento de sistemas e da segurança e gerenciamento do ciclo de vida do PC.

Com sede em Seattle, a Attachmate atende a mais de 65 mil clientes em cerca de 60 países. Para obter mais informações, acesse **www.attachmate.com.br**