

incidentes e intrusão - enquanto outro fornecedor oferece o painel de controle que avalia quanto a organização cumpre suas políticas de governança. O resultado pode ser uma visibilidade insatisfatória, devido à fraca integração entre produtos, lacunas de gerenciamento de cumprimento ou customização onerosa e demorada.

Com o Tivoli Security Information and Event Manager, as organizações de hoje têm uma solução SIEM de ampla cobertura, totalmente integrada, para ajudar a dar suporte e automatizar as iniciativas de cumprimento envolvendo todos os 12 padrões PCI. Combinando monitoração em tempo real com análise e relatórios históricos aprofundados, o Tivoli Security Information and Event Manager pode:

- Coletar e centralizar dados de log relevantes para o PCI DSS colhidos de fontes heterogêneas.
- Filtrar a informação coletada em relação aos requisitos PCI e à política de segurança corporativa.
- Acionar automaticamente alertas apropriados quando forem detectadas atividades suspeitas relacionadas à segurança do cartão de pagamentos.
- Arquivar dados de log relevantes ao PCI DSS para revisão.
- Oferecer visualização e relatórios consolidados via um painel de controle centralizado.

PCI Data Security Standard	
Criar e Manter uma Rede Segura	1. Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão 2. Não usar padrões dados pelo fornecedor para senhas do sistema e outros parâmetros de segurança
Proteger Dados do Titular do Cartão	3. Proteger dados armazenados do titular do cartão 4. Criptografar transmissão de dados do titular do cartão em redes públicas abertas
Manter um Programa de Gerência de Vulnerabilidade	5. Usar e atualizar regularmente software antivírus 6. Desenvolver e manter sistemas e aplicativos seguros
Implementar Fortes Medidas de Controle de Acesso	7. Restringir acesso aos dados do titular do cartão em função da necessidade do conhecimento para os negócios 8. Atribuir um ID único a cada pessoa que acesse o computador 9. Restringir acesso físico aos dados do titular do cartão
Monitorar e testar Regularmente as Redes	10. Rastrear e monitorar todo acesso a recursos da rede e dados do titular do cartão 11. Testar regularmente os processos e sistemas de segurança
Manter uma Política de Segurança de Informação	12. Manter uma política que aborde segurança de informações

O PCI DSS inclui 12 requisitos – denominados "os doze digitais" – que as organizações precisam atender todos os anos para manter cumprimento PCI

O Tivoli Security Information and Event Manager oferece às organizações sua singular metodologia W7, projetada para determinar rapidamente os sete Q's críticos de segurança: Quem fez, O quê, Quando, Onde, De Onde, Para Onde e Em Quê. Revelando quem tocou no ativo de informações e comparando aquela atividade com as políticas que definem a utilização adequada, as organizações podem automatizar requisitos de monitoração e ajudar a acelerar suas iniciativas de gerenciamento de cumprimento para PCI.

Para ambientes de mainframe, o conjunto IBM Tivoli zSecure oferece funcionalidades administrativas e de auditoria para o IBM Resource Access

Control Facility (RACF®), CA ACF2™ e CA Top Secret®. O conjunto funciona diretamente com o Tivoli Security Information and Event Manager para criar uma arquitetura em âmbito corporativo para auditoria de segurança e cumprimento. Como um elemento crítico do conjunto zSecure, o IBM Tivoli zSecure Audit oferece relatórios das configurações e exceções de política relevantes para PCI em períodos de tempo especificados pelo usuário.

Os alertas do Tivoli zSecure Audit podem ser facilmente configurados para ajudar a garantir que exceções de políticas de alta prioridade sejam tratadas imediatamente.

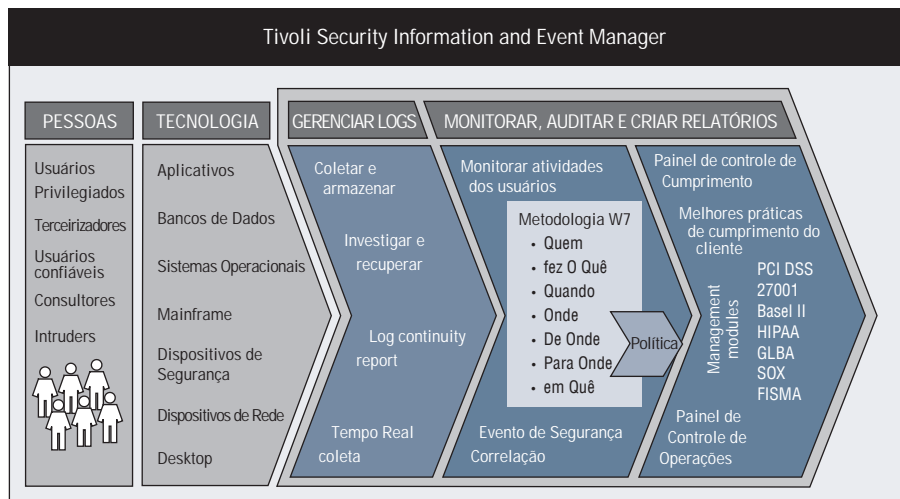
O Tivoli zSecure Audit também oferece a capacidade de identificar dados seqüenciais de log residindo tanto em fita quanto em mídia de dispositivos de acesso direto (DASD). Isso permite revisões periódicas para verificar a integridade de logs de System Management Facility (SMF) em fita e Disco.

Aprimorar iniciativas de gerenciamento de cumprimento

O Tivoli Security Information and Event Manager coleta logs de um vasto leque de tipos de dispositivo, e oferece um relatório de continuidade de logs "a um olhar", que ajuda a demonstrar para os auditores que todo e qualquer log seja coletado como necessário.

Ele inclui um robusto painel corporativo de controle de auditoria que liga dados operacionais do dia a dia com a análise baseada em políticas necessária para auditoria. As funcionalidades de monitoração de atividade de usuários permite que os executivos-chefes de segurança de informações (CISOs) e auditores recebam uma visão consolidada de todas as atividades relevantes na empresa, inclusive quanta atividade foi registrada em logs e como os perfis de usuário se comparam à informação que eles estão acessando.

O Tivoli Security Information and Event Manager oferece diversos módulos de gerenciamento, inclusive um para PCI DSS. Cada módulo oferece informações detalhadas e modelos para usar ao gerenciar iniciativas de cumprimento PCI. Cada módulo inclui um modelo de



O Tivoli Security Information and Event Manager oferece um painel de controle crítico a partir do que pode ser vista a postura de segurança de uma organização. Ele também inclui um módulo de gerenciamento PCI DSS e relatórios específicos de PCI, facilitando a ligação entre a postura de segurança e a postura de cumprimento.

classificação de ativos, um modelo de política para medir os dados de eventos em relação a políticas personalizadas e uma central de relatórios que oferece relatórios direcionados aos requisitos PCI.

Além disso, o Tivoli Security Information and Event Manager oferece uma robusta plataforma unificada a partir da qual pode-se automatizar reconhecimento e resposta a incidentes, otimizar o tratamento de incidentes e viabilizar a monitoração e controle de políticas.

Como resultado, as organizações podem implementar uma comprovada metodologia automatizada de agregação e correlação de eventos de segurança para ajudar a otimizar recursos, reduzir a complexidade de gerenciar segurança, controlar a política de segurança e

ajudar a aprimorar sua postura geral de segurança.

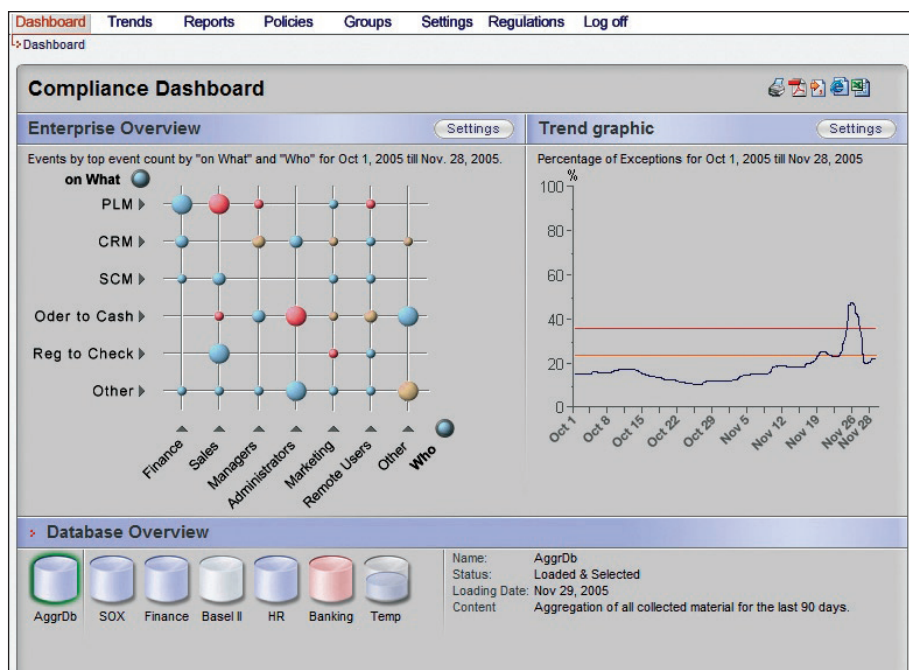
Gerenciamento contínuo de cumprimento
Nenhuma ferramenta sozinha é uma solução completa para atender a todos os requisitos PCI DSS ou para cumprir qualquer iniciativa de proteção de dados ou de privacidade. Além disso, atividades de cumprimento representam um alvo móvel. Mesmo depois que as lacunas foram cobertas, e a organização tenha passado com sucesso por uma avaliação, é necessária monitoração contínua para dar suporte a iniciativas continuadas de cumprimento. Para dar suporte a essa necessidade, o Tivoli Security and Event Manager oferece uma abordagem sistemática para monitoração confiável, ajudando a reduzir os custos de preparo e de relatórios para PCI e outras iniciativas.

O Tivoli Security Information and Event Manager também pode ser usado para iniciativas de gerenciamento envolvendo vários tipos de cumprimento – uma capacitação importante hoje, pois as organizações podem estar sujeitas a múltiplos requisitos.

Explore soluções de segurança Tivoli de ponta a ponta

Além disso, outras soluções IBM estão disponíveis para ajudar a dar suporte aos requisitos PCI DSS. Para gerenciamento de identidades, o IBM Tivoli Identity Manager oferece uma solução segura, automática e baseada em políticas projetada para gerenciar privilégios de usuários ao longo de recursos heterogêneos de TI. A família de produtos IBM Tivoli Access Manager ajudar as organizações a gerenciar com segurança o acesso a aplicativos e dados críticos de negócio, ao mesmo tempo que oferece aos usuários acesso rápido e conveniente à informação que eles precisam.

O Serviço Gerenciado IBM de Firewall pode ser usado para terceirizar todos os serviços de firewall, inclusive os requisitos



Com o Tivoli Security Information and Event Manager, os usuários podem visualizar todas as atividades da empresa a partir de um painel de controle de auditoria corporativa. O tamanho de cada círculo acima indica o volume de atividade (eventos logados). Ao longo dos eixos, vemos uma comparação de pessoas (Quem) com informação (Em Quê).

de gerenciamento sobre os firewalls necessários para garantir cumprimento PCI. Para empresas que querem gerenciar seus próprios firewalls, o IBM Tivoli Application Dependency Discovery Manager pode ajudar a criar um "mapa de rede" dos componentes de TI – incluindo a localização de firewalls – conforme especificado nos requisitos PCI.

O IBM Tivoli Change and Configuration Management Database (CCMDB) pode ser aplicado para padronizar os processos de efetuar mudanças nos firewalls. O IBM Tivoli Security Compliance Manager pode ser usado para monitorar os arquivos de configuração de firewalls, garantindo que eles não tenham sido alterados fora dos processos padronizados.



Sobre o software de gerenciamento de serviços IBM Tivoli

O software Tivoli oferece uma plataforma de gerenciamento de serviços para organizações fornecerem serviços de qualidade, oferecendo visibilidade, controle e automação - visibilidade para ver e entender como funcionam seus processos de negócio; controle para gerenciar com eficácia sua empresa, minimizar riscos e proteger sua marca; e automação para otimizar seus negócios, reduzir o custo de operações e oferecer novos serviços com maior rapidez. Diferentemente da gestão de serviços centrada em TI, o software Tivoli oferece uma base comum para gerenciar, integrar e alinhar os requisitos de negócios e os tecnológicos. O software Tivoli é projetado para atender rapidamente às necessidades mais prementes de gestão de serviços de uma organização, e ajudar a responder proativamente a demandas dinâmicas de negócios. O portfólio Tivoli tem o suporte dos Serviços de classe mundial da IBM, Suporte IBM e um ecossistema ativo de Parceiros Comerciais IBM. Os clientes e Parceiros Comerciais Tivoli também podem tirar partido das melhores práticas uns dos outros, participando de Grupos de Usuários IBM Tivoli coordenados de forma independente no mundo inteiro - visite www.tivoli-ug.org.

© Copyright IBM Corporation 2008

IBM Corporation
Software Group
Route 100 Somers, NY 10589
E.U.A

Produzido nos Estados Unidos da América
Junho de 2008
Todos os direitos reservados.

IBM, o logotipo da IBM, ibm.com, RACF e Tivoli são marcas registradas da International Business Machines Corporation nos Estados Unidos, em outros países ou ambos. Se esses e outros termos de marcas registradas da IBM estiverem marcados na primeira ocorrência dessa informação com um símbolo de marca registrada (® ou ™), esses símbolos indicam marcas registradas ou de direito consuetudinário dos Estados Unidos, pertencentes à IBM no momento em que essa informação foi publicada. Essas marcas registradas também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atualizada de marcas registradas da IBM está disponível na Web em "Informações de marca registrada e direitos autorais" no endereço ibm.com/legal/copytrade.shtml.

ACF2 e Top Secret são marcas registradas da CA, Inc. ou de uma de suas subsidiárias.

Todos os demais nomes de serviços, produtos e empresas podem ser marcas registradas ou serviços de seus respectivos proprietários.

Ressalva: O cliente é responsável por garantir o cumprimento de requisitos legais. É responsabilidade exclusiva do cliente obter orientação de advogado externo competente em relação à identificação e interpretação de qualquer lei ou requisito regulatório relevante que possa afetar os negócios do cliente e qualquer ação que o cliente possa ter de tomar para cumprir essas leis. A IBM não oferece orientação jurídica, declaração ou garantia de que seus serviços ou produtos garantirão que o cliente esteja em cumprimento com qualquer lei ou regulamentação.

*Conselho de Padrões de Segurança PCI

TAKE BACK CONTROL WITH 