



Protegendo os Dados de Proprietários de Cartão de Crédito

Como o Reflection Facilita a Conformidade com PCI

CONTEÚDO

Os Doze Requisitos de PCI.	1
Como o Reflection Trata de Questões de Segurança Relacionadas ao Legado.....	2
A Abordagem do Reflection com Relação à Conformidade.....	3
Mais Funcionalidades para Maior Conformidade.....	5

Protegendo os Dados de Proprietários de Cartão de Crédito

Como o Reflection Facilita a Conformidade com PCI

Em 2004, as principais bandeiras de cartões de crédito, entre elas Visa, MasterCard e American Express, uniram forças na criação do PCI DSS (Payment Card Industry Data Security Standard). Este padrão do mercado aplica-se a todas as companhias que armazenam, processam, ou transmitem informações sobre proprietários de cartões de crédito e tem como objetivo garantir a privacidade dos dados para os clientes com rígidos controles de segurança.

Foram estabelecidos prazos para que essas companhias atendessem aos doze abrangentes requisitos do PCI DSS. Esses requisitos compreendem desde fáceis de serem implementados como garantia de software antivírus sempre atualizado, aos mais complexos como controle do acesso aos recursos da rede e dados dos proprietários de cartões de crédito.

Este white paper mostra como os emuladores de terminal, utilitários de transferência de arquivos e clientes e servidores SSH Reflection® da Attachmate® podem ajudá-lo na conformidade com PCI DSS. Quando terminar de lê-lo, você saberá como os produtos Reflection podem ajudar na conformidade com determinados requisitos PCI e como eles fazem isso. Você verá que o Reflection viabiliza a conformidade além da emulação de terminal e transferência de arquivos, até áreas que você nunca poderia imaginar.

Os Doze Requisitos de PCI

O PCI DSS compreende doze requisitos para garantir a segurança dos dados dos proprietários de cartões de crédito e a proteção da rede e do sistema que lidam com esses dados. Esses doze requisitos estão divididos entre três grupos:

Criar e manter uma rede segura
1. Instalar e manter uma configuração de firewall para proteção das informações sobre proprietários de cartões de crédito.
2. Não utilizar senhas nem parâmetros de segurança fornecidos pelos fabricantes
Proteger as Informações dos proprietários de cartões de crédito
3. Proteger as informações armazenadas dos proprietários de cartões de crédito.
4. Codificar as transmissões das informações de proprietários de cartões de crédito via redes públicas abertas.
Implantar um programa de gerenciamento de vulnerabilidades
5. Usar e atualizar regularmente software antivírus.
6. Desenvolver e manter sistemas e aplicativos seguros
Adotar medidas rígidas de controle de acesso
7. Restringir o acesso às informações sobre proprietários de cartões de crédito.
8. Atribuir um ID exclusivo a cada pessoa.
9. Restringir o acesso físico aos dados sobre os proprietários de cartões de crédito.
Monitorar e testar regularmente as redes
10. Controlar e monitorar o acesso aos recursos da rede e dados sobre os proprietários de cartões de crédito.
11. Testar regularmente os sistemas e processos
Manter uma política de segurança das informações
12. Implantar uma política que atenda à segurança das informações.

Os produtos Reflection facilitam a conformidade com os requisitos 1, 2, 4, 6, 7, 8 e 10.

Como o Reflection Trata das Questões de Segurança do Legado

Para ajudá-lo a entender como os produtos Reflection podem facilitar a conformidade com PCI, esta seção apresenta resumidamente questões referentes à segurança do legado e descreve como os produtos Reflection atendem a elas.

Segurança dos servidores

Os sistemas legados armazenam dados de proprietários de cartões de crédito e executam aplicativos que possibilitam acessar esses dados. Os sistemas legados podem ser servidores de arquivos com dados sobre os proprietários de cartões de crédito que precisam ser transferidos via redes públicas. Devido à natureza confidencial desses dados, as empresas precisam restringir o acesso a eles e codificá-los para que eles possam trafegar com segurança pela rede.

Solução Reflection: Reflection for Secure IT é uma família de clientes e servidores Secure Shell para Windows® e UNIX. Com os servidores Reflection for Secure IT você cria túneis seguros codificados para os dados em trânsito, inclusive para a comunicação de emuladores em clientes, utilitários para transferência de arquivos ou qualquer aplicativo que utilize o protocolo TCP/IP.

O Reflection for Secure IT exerce também uma outra função crítica de segurança: controle de acesso, inclusive acesso com privilégio de administrador, aos componentes do sistema. Ativando a configuração de um log de auditoria, o Reflection for Secure IT apresenta importantes informações (por exemplo, quem acessou o sistema via servidor SSH e quando) aos repositórios padrão de registro do legado.

Segurança das estações de trabalho

Os usuários e administradores de sistema frequentemente dependem de utilitários no cliente para acesso a aplicativos e arquivos armazenados no legado. Os IDs e as senhas de usuário usados para acessar o legado, assim como as informações confidenciais que trafegam entre a estação de trabalho e o legado, precisam ser protegidos contra os olhos maliciosos.

Solução Reflection: Os emuladores de terminal Reflection for Windows e Reflection for the Web suportam uma ampla variedade de tecnologias de criptografia como SSH e SSL/TLS e métodos de autenticação (como Kerberos) que operam com as funcionalidades ativas no legado. Com isso os responsáveis pela segurança podem ter a certeza que tanto as credenciais do usuário (como as senhas)

Sobre os Produtos

Reflection for Windows

Os produtos Reflection para emulação de terminal (assim como os emuladores de terminal INFOConnect® e Attachmate EXTRA!®) oferecem conexões seguras com aplicativos em sistemas IBM, HP, UNIX, Unisys, OpenVMS, Tandem e CRS/GDS. Esses comprovados e avançados produtos oferecem uma linha completa de opções de criptografia, autenticação e integridade dos dados.

Reflection Secure FTP

Parte dos produtos Reflection, EXTRA! e INFOConnect, o Reflection Secure FTP oferece um poderoso utilitário para transferência de arquivos entre as estações de trabalho e os sistemas legados.

Reflection for the Web

O Reflection for the Web é um software para emulação de terminal que conecta com segurança usuários de navegadores a aplicativos em sistemas IBM, HP, UNIX, Linux, OpenVMS, Unisys e CRS/GDS. Com rígida autenticação de usuários, registro de auditoria, funcionalidades de criptografia e controle de acesso, você oferece aplicativos do legado seguros e totalmente funcionais via Internet.

Reflection for Secure IT

Reflection for Secure IT é uma família de clientes e servidores Secure Shell para ambientes Windows e UNIX – desenvolvida para proteger os dados em trânsito. Com as funcionalidades de criptografia, autenticação, auditoria e integridade dos dados do Reflection for Secure IT, você transfere dados confidenciais, gerencia servidores remotos e acessa aplicações corporativas via conexões codificadas.

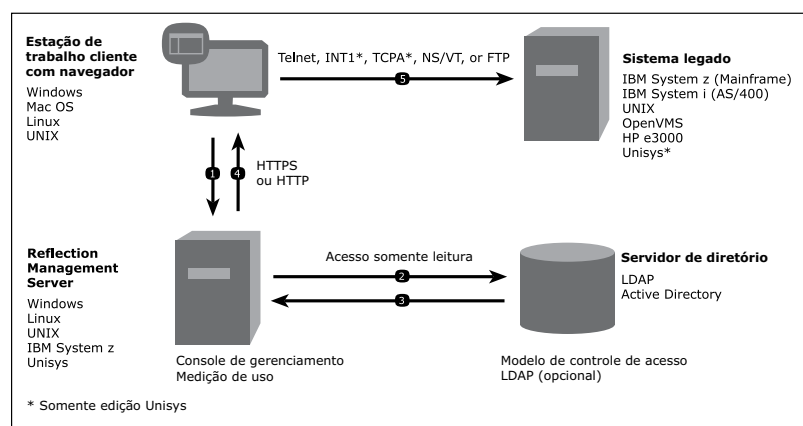
quanto as informações confidenciais (como os dados de proprietários de cartões de crédito) serão codificadas quando trafegarem do legado para a tela do emulador de terminal. Os Reflection Secure FTP clients, parte dos produtos de emulação Reflection, também suportam várias tecnologias de criptografia e métodos de autenticação. Essas tecnologias e métodos ajudam a garantir que os arquivos confidenciais não sejam acessados por usuários não-autorizados e sejam codificados antes de trafegarem pela rede.

Segurança no acesso ao sistema

Os emuladores de terminal oferecem acesso a informações confidenciais do legado, o que significa que o acesso às sessões de emulação precisa ser rigidamente controlado.

Solução Reflection: O Reflection for the Web oferece controle de autenticação e acesso que usa os diretórios de usuário existentes (como o Active Directory). Os usuários não conseguem acessar as sessões de emulação, a não ser que sejam aprovados por um administrador.

É possível atribuir configurações específicas de sessão a usuários e grupos de um domínio. Essas sessões são iniciadas por intermédio de links em uma página ou portal protegidos. Quando o usuário acessa a página ele é autenticado segundo um diretório de usuário e tem acesso concedido a sessões do legado predefinidas.



- 1) O usuário se conecta ao Reflection Management Server.
- 2) O usuário se autentica a um servidor de diretório (LDAP/Active Directory) - opcional.
- 3) O servidor de diretório oferece a identidade do usuário e do grupo.
- 4) O Reflection Management Server envia uma sessão de emulação para o cliente autenticado.
- 5) O usuário autenticado se conecta ao sistema legado.

A Abordagem do Reflection com Relação à Conformidade

Esta seção explica como o Reflection pode ajudá-lo a atender aos requisitos PCI DSS 1, 2, 4, 6, 7, 8 e 10.

Requisito 1: Instalar e manter uma configuração de firewall para proteção das informações sobre proprietários de cartões de crédito

A Seção 1.1 da documentação sobre PCI DSS especifica que determinados protocolos, como Secure Sockets Layer (SSL) e Secure Shell (SSH), podem trafegar pelo firewall sem uma documentação ou justificativa especial. Mas os protocolos como FTP, considerados arriscados, precisam de uma justificativa ou documentação para que consigam passar pelo firewall.

A Seção 1.2 especifica que os firewalls precisam ser configurados para recusar todo o tráfego, exceto o dos protocolos exigidos pelo ambiente dos dados de proprietários de cartões de crédito, de redes não confiáveis.

Veja como os produtos Reflection facilitam a conformidade com o Requisito 1:

Reflection for Windows

Todos os produtos Reflection for Windows suportam criptografia dos dados do terminal com o uso de protocolos seguros aceitáveis como SSH e SSL/TLS.

Reflection Secure FTP

O utilitário Reflection Secure FTP suporta FTP, SFTP e FTP/S cliente com protocolos seguros aceitáveis como SSH e SSL/TLS.

Reflection for the Web

O Reflection for the Web suporta criptografia dos dados do terminal com o uso de protocolos seguros aceitáveis como SSH e SSL/TLS.

Além disso o Reflection for the Web inclui o Reflection Security Proxy, que possibilita acesso seguro ao sistema legado. Os sistemas legados atrás do firewall e do e os vários sistemas legados, podem ser acessados via uma única porta aberta no firewall.

Reflection for Secure IT

Os servidores SSH do Reflection for Secure IT oferecem um mecanismo no servidor para suporte à conectividade SSH a partir de clientes Reflection de transferência de arquivo e emulação de terminal.

Requisito 2: Não utilizar senhas nem parâmetros de segurança fornecidos pelos fabricantes

A seção 2.3 exige que todos o acesso administrativo não realizado via console aos sistemas principais seja codificado. SSH e SSL/TLS são considerados protocolos aceitáveis.

Veja como os produtos Reflection facilitam a conformidade com o Requisito 2:

Reflection for Windows

Os produtos Reflection for Windows podem ser usados para acesso administrativo não via console aos sistemas legados. Todos eles suportam criptografia dos dados do terminal com o uso de protocolos seguros aceitáveis como SSH e SSL/TLS.

Reflection for the Web

O Reflection for the Web suporta criptografia dos dados do terminal com o uso de protocolos seguros aceitáveis como SSH e SSL/TLS.

O Reflection Security Proxy também oferece conexões codificadas com os sistemas legados como Unisys que não possuem suporte nativo à criptografia.

Reflection for Secure IT

Os clientes Reflection for Secure IT Secure Shell oferecem utilitários para tarefas de administração remota por script ou interativa via protocolo SSH.

Os servidores SSH do Reflection for Secure IT oferecem um mecanismo no servidor para suporte à conectividade SSH dos clientes de emulação de terminal Reflection.

Requisito 3: Proteger as informações armazenadas dos proprietários de cartões de crédito

A seção 3.3 estipula que os números de conta principais (PANs) precisam ser exibidos como máscara.

Veja como o Reflection® for IBM® 2007, um emulador de terminal Windows, facilita a conformidade com o Requisito 3:

Reflection for IBM 2007

O Reflection for IBM 2007 inclui uma funcionalidade de filtros de privacidade configuráveis para mascarar PANs apresentados em janelas de histórico, relatórios impressos e na área de transferência.

Observação: O software de emulação de terminal Attachmate EXTRA! oferece as mesmas funcionalidades.

Requisito 4: Codificar as transmissões das informações de proprietários de cartões de crédito via redes públicas abertas

O Requisito 4 estipula que as “informações confidenciais” precisam ser codificadas durante transmissões por rede fáceis de serem interceptadas, modificadas e desviadas por um hacker durante o trajeto. A Seção 4.1 especifica ainda que devem ser usados rígidos protocolos de segurança e criptografia para proteger dados confidenciais de proprietários de cartões de crédito em trânsito.

Veja como os produtos Reflection facilitam a conformidade com o Requisito 4:

Todos os produtos Reflection

Todas as implementações de protocolos SSH e SSL/TLS dos produtos Reflection usam rígida criptografia, inclusive os algoritmos Triple DES e AES para codificar os dados de proprietários de cartões de

crédito enviados pela rede. Na maioria dos casos essas implementações criptográficas foram validadas segundo FIPS 140-2 por um terceiro autorizado.

Requisito 6: Desenvolver e manter sistemas e aplicativos seguros

A seção 6.1 do PCI DSS exige a instalação dos patches de segurança mais atualizados no prazo de um mês após a disponibilidade pelo fabricante.

Para acompanhar o dinâmico cenário das ameaças à segurança, é necessário ter como parceiro um fabricante que monitore os principais serviços de alerta de segurança e o notifique sobre vulnerabilidades relevantes.

Os especialistas em segurança da Attachmate mantêm um banco de dados de notas técnicas no nosso suporte com as vulnerabilidades publicadas. Caso uma vulnerabilidade afete algum produto Attachmate, os clientes com contrato de Manutenção poderão fazer download dos devidos patches de segurança. A equipe de suporte técnico da Attachmate estará disponível para ajudá-lo a lidar com qualquer questão de segurança nos nossos produtos.

Requisito 7: Restringir o acesso às informações sobre proprietários de cartões de crédito

Este requisito exige que seja concedido acesso aos dados de proprietários de cartões de crédito apenas aos usuários cujo trabalho requer tal acesso e que a configuração padrão de acesso a tais dados, exceto nesses casos, seja “negar tudo”.

Veja como o Reflection for the Web facilita a conformidade com o Requisito 7:

Reflection for the Web

Todos os sistemas do legado oferecem o mesmo nível de autorização e controle de acesso. Podemos agregar uma camada extra de segurança com o Reflection for the Web para maior controle dos utilitários, como emuladores de terminal e para transferência de arquivo que acessam seus sistemas legados.

Veja como funciona: Os usuários são solicitados a acessar um site com links para as sessões de transferência de arquivo e emulação de terminal. As sessões de autenticação e acesso podem ser gerenciadas por intermédio do seu diretório de controle de acesso existente (por exemplo, o Active Directory). É possível controlar o acesso por usuário ou grupo. A configuração padrão do Reflection for the Web negará o acesso para usuários não autorizados.

Requisito 8: Atribuir um ID exclusivo para cada pessoa

De acordo com o objetivo de “implementar controle

rígido de acesso”, esse requisito especifica que os usuários precisam se identificar antes de terem acesso aos dados de proprietários de cartões de crédito. Especifica também suporte a uma ampla variedade de metodologias de autenticação e o uso de dupla autenticação para acesso remoto.

Veja como o Reflection for the Web facilita a conformidade com o Requisito 8:

Reflection for the Web

Colocando a camada de autenticação e autorização na frente do acesso aos utilitários de transferência de arquivo e emulação de terminal, o Reflection for the Web permite a atribuição de IDs exclusivos para cada usuário, reforçando assim o controle de acesso.

Além da autenticação por senha, o Reflection for the Web também suporta certificados digitais e chaves públicas na autenticação.

Requisito 10: Controlar e monitorar o acesso aos recursos da rede e dados sobre os proprietários de cartões de crédito

Os mecanismos de registro e a capacidade de controlar as atividades do usuário são fundamentais para a conformidade com PCI DSS. O requisito 10 refere-se ao monitoramento e registro dos eventos para auditoria e os pontos que devem ser capturados no registro.

Veja como os produtos Reflection facilitam a conformidade com o requisito 10:

Reflection for Secure IT

Como provedor de serviços Secure Shell no servidor, o Reflection for Secure IT oferece poderosas funcionalidades de registro. Os principais eventos na operação dos servidores Reflection for Secure IT, inclusive as conexões com o cliente e autenticações, são registrados em uma ampla variedade de sistemas configuráveis, inclusive nos logs de evento padrão do sistema operacional.

Reflection for the Web

Durante as sessões de transferência de arquivo e emulação de terminal, o Reflection for the Web registra os eventos de acesso e os detalhes sobre os sistemas legados aos quais os usuários se conectam.

Mais funcionalidades e maior conformidade

Não é fácil atender à ampla gama de requisitos PCI DSS. A implementação pode abranger vários departamentos, envolver várias equipes e afetar diversas plataformas de sistema. O esforço pode demandar muito tempo e dinheiro.

Infelizmente não há uma solução única que atenda a todas as necessidades de conformidade com PCI. Mas os produtos Reflection, que oferecem mais funcionalidades de conformidade com PCI que as outras soluções para emulação de terminal, oferecem uma ampla base de suporte a isso. Com ferramentas em servidores e estações de trabalho de usuário, os produtos Reflection foram desenvolvidos para reduzir o tempo para conquistar a conformidade e para o compartilhamento mais seguro de informações.

E há mais novidades: quando você estiver em conformidade com os requisitos PCI, sua empresa estará mais próxima da conformidade com outras regulamentações mais recentes.

A Conexão NetIQ

Os produtos Reflection descritos neste white paper encaixam-se perfeitamente a uma estratégia bem planejada para conformidade com PCI. Quando se trata de conformidade, gerenciamento e monitoramento com todos os requisitos PCI DSS, você pode contar com a NetIQ, uma empresa da Attachmate.

A NetIQ é líder em conformidade, monitoramento e automação de processos de TI. Considerada pelo Gartner como de altíssimo nível em soluções de segurança, a NetIQ oferece proteção e monitoramento (inclusive SIEM) para várias das maiores empresas e instituições públicas do mundo.

Abrangendo áreas críticas como segurança dos sistemas, monitoramento da rede, gerenciamento de políticas e controle de acesso, as soluções NetIQ possibilitam a rápida implementação e conformidade. Além disso os especialistas em segurança da NetIQ podem trabalhar com a sua equipe de TI e conformidade para atender os interesses específicos da sua empresa e da infra-estrutura existente.

Para obter mais informações sobre as soluções NetIQ, acesse www.netiq.com.



Sede Corporativa
1500 Dexter Avenue North
Seattle, Washington 98109
TEL 206 217 7500
FAX 206 217 7515

**Sede para a Europa,
Oriente Médio e África**
Holanda
TEL +31 172 50 55 55
FAX +31 172 50 55 51

**Sede para a América
Latina**
México
TEL +52 55 9178 4970
FAX +52 55 5540 4886

Attachmate Brasil
São Paulo - SP.
TEL +55 11 3085 0303
FAX +55 11 3085 5617

WEB www.attachmate.com.br
EMAIL Fale_conosco@atm.com.br

Para obter informações sobre os escritórios regionais, visite www.attachmate.com.br.