



DOCUMENTO ESTRATÉGICO

VeriSign® Identity Protection (VIP)





ÍNDICE

+ Introdução	4
+ Habilitação da migração de comércio digital	6
Autenticação forte	6
Detecção de fraudes	7
+ VeriSign Identity Protection Services	8
VeriSign Identity Protection Authentication Service	8
VeriSign Identity Protection Fraud Detection Service	10
+ VeriSign Identity Protection Network	11
VeriSign Identity Protection Shared Authentication Network	11
VeriSign Identity Protection Fraud Intelligence Network	12
+ VeriSign: um parceiro confiável	13
+ Pesquisa e Desenvolvimento Associados	14
Serviços de autenticação mútua	14
Gerenciamento de identidades de consumidores	14
Serviços de comprovação de identidade	14
+ Saiba Mais	16
+ Sobre a VeriSign	16



VeriSign® Identity Protection

“É sempre muito importante lembrar que nosso principal negócio é atender às necessidades de nossos clientes. Isso significa que todas as tecnologias que selecionarmos devem funcionar de forma apropriada sem impactar de forma adversa o hábito de nossos clientes no Schwab.com... A equipe da VeriSign mostrou ser um grupo de pessoas com as quais poderíamos trabalhar de perto, e com as quais poderíamos manter um relacionamento produtivo a longo prazo.”

- Kostas Konstantinides
Diretor de serviços Web aos clientes
Charles Schwab & Co.

+ Introdução

Mais do que nunca, os consumidores estão efetuando compras ou utilizando serviços bancários on-line por conveniência e escolha pessoal. A “migração digital” tem levado à evolução das estratégias empresariais em diversos setores, incluindo varejo, serviços financeiros, mídia e entretenimento, assistência médica e serviços governamentais. Para as empresas, a oportunidade oferecida é o desenvolvimento de um novo canal de distribuição com a promessa de aumento nas vendas a redução nos custos operacionais. Entretanto, elas enfrentam desafios por causa da necessidade de oferecer um hábito on-line diferenciado aos clientes, combatendo ao mesmo tempo as fraudes e seus efeitos negativos.

Um esquema deficiente de autenticação dos consumidores alimentou os problemas de roubo de identidade na Internet, phishing e fraudes financeiras on-line. À medida que mais e mais consumidores utilizam computadores e dispositivos móveis para fazer compras, administrar suas finanças e acessar informações sobre seus planos de saúde, os riscos de fraudes e de roubo de identidade aumentam.

A principal causa de tantas fraudes on-line, o roubo de identidade continua a ser um problema significativo para as empresas e seus consumidores. Uma pesquisa recente da Gartner informa que no período de 12 meses, encerrado em agosto de 2006, mais de 15 milhões de americanos foram vítimas de algum tipo de fraude relacionada ao roubo de identidade, representando um aumento de 50% em relação a 2003, quando a Comissão Federal de Comércio reportou 9,9 milhões de vítimas. Os incidentes resultaram em prejuízos financeiros significativos. De acordo com a Javelin Strategy and Research, os prejuízos totais acumulados em um ano com fraudes atingiram US\$49,3 milhões em 2007. A Gartner estima que o prejuízo médio em 2006 foi de US\$3.257, mais que o dobro do valor médio de US\$1.408 em 2005.

Apesar de as perdas serem significativas por si só, o problema é agravado pelo impacto negativo na confiança dos consumidores e, logo, em seu comportamento de compra. No setor de serviços financeiros, isso pode implicar uma maior migração de contas para a concorrência, menores volumes de transações ou redução nos ativos das contas. Para outras aplicações de comércio eletrônico, como varejo, jogos ou música e entretenimento, isso pode significar oportunidades perdidas de geração de receita. Uma pesquisa nos domicílios americanos conduzida pela Forrester Research mostrou que 24% dos consumidores não efetuam compras on-line por preocupações com segurança. Outros 37% reduziram suas compras on-line pelo mesmo motivo. De acordo com um estudo recente da Gartner, as preocupações com a segurança on-line de 46% da população adulta nos EUA causaram mais de US\$2 bilhões em oportunidades de vendas perdidas em 2006. Esses dados indicam que as empresas têm uma oportunidade de se diferenciarem e começarem a gerar receitas significativas ao abordarem as preocupações com a segurança e confiança do consumidor on-line.

Antigamente, somente uma orientação em termos de regulamentação em torno da autenticação mais forte de consumidores levava ao investimento em tecnologia. Por exemplo, o U.S. Federal Financial Institutions Examination Council (FFIEC - órgão regulatório do setor financeiro americano), a Autoridade Monetária de Hong Kong e a Comissão de Regulamentação Bancária da China contam com iniciativas de regulamentação relacionadas aos serviços bancários on-line. Atualmente, no entanto, um número cada vez maior de empresas está avaliando as opções de autenticação para sua base de consumidores on-line como uma forma de habilitação de negócios.

A autenticação forte vem sendo aceita há muito tempo nas empresas como uma tecnologia capaz de proteger o acesso às redes e aplicações corporativas. Entretanto, o modelo tradicional de implantação apresenta custos e problemas de escala significativos quando aplicado ao mercado consumidor. Em vez de milhares ou dezenas de milhares de funcionários, a população de usuários pode atingir milhões de consumidores. Para tratar dos requisitos únicos desse segmento, uma abordagem inteiramente nova em relação à autenticação é necessária.



O VeriSign® Identity Protection (VIP – Proteção de Identidade da VeriSign) é um conjunto abrangente de serviços de proteção de identidade e autenticação que habilita as aplicações voltadas ao consumidor a oferecerem acesso on-line seguro aos usuários finais a um custo razoável. O VIP possibilita um meio de segurança passivo através dos serviços de detecção de fraudes VeriSign Identity Protection (VIP) Fraud Detection Services, bem como uma segurança mais ativa por meio dos serviços de autenticação VeriSign Identity Protection (VIP) Authentication Services.

Para minimizar custos e maximizar a segurança por meio do compartilhamento de inteligência e recursos, os serviços VIP são aperfeiçoados pelos efeitos da rede de proteção de identidade VeriSign Identity Protection (VIP) Network. Inspirada no mundo off-line das redes de caixas eletrônicos (ATM), a rede VIP Network tem dois valores importantes de diferenciação: o compartilhamento dos dispositivos de autenticação e da inteligência contra fraudes.

O compartilhamento de dispositivos é habilitado pela rede de autenticação compartilhada VeriSign Identity Protection (VIP) Shared Authentication Network, na qual os emissores de dispositivos e os sites que aceitam credenciais de terceiros tornam-se parte de uma rede confiável de benefícios mútuos que permite aos consumidores a utilização de um dispositivo de segundo fator em vários Websites. Este recurso oferece conveniência e uma maior segurança aos consumidores, permitindo, ao mesmo tempo, que as empresas compartilhem o custo de uma infra-estrutura de autenticação forte.

Pelo fato de as fraudes on-line serem normalmente perpetradas como um ataque em diversas propriedades on-line, a rede de inteligência contra fraudes VeriSign Identity Protection (VIP) Fraud Intelligence Network aprimora ainda mais a rede VIP Network por meio do compartilhamento de inteligência entre as empresas participantes. Essa abordagem de “vigilância da vizinhança” permite que as empresas reajam de forma rápida para mitigar o impacto das fraudes on-line.

A autenticação compartilhada VIP Shared Authentication possui algumas qualidades únicas para ajudar as empresas a possibilitarem um maior crescimento das receitas, por meio da proteção de seus consumidores:

- **Conveniente e simples.** Os usuários contam com um único dispositivo portátil (como um token em formato de chaveiro, cartão, ou telefone celular habilitado para criar uma senha dinâmica de uso único [OTP – One Time Password]), o qual serve como um segundo fator de autenticação para qualquer site da rede VIP, similar àquele utilizada nas redes de caixas eletrônicos (ATM – Automated Teller-Machine).
- **Econômica.** O VIP se baseia em um modelo de serviços compartilhados no qual a VeriSign hospeda a infra-estrutura e a integração dos serviços Web para minimizar os custos associados de implantação e manutenção. Um hábito constante do usuário também minimiza os custos de suporte dos sites membros.
- **Impulso nos negócios.** O compartilhamento dos dispositivos de autenticação pode impulsionar afiliações on-line e desenvolver canais. Por exemplo, um varejista on-line pode ser capaz de notificar a comunidade eBay / PayPal de que seu token OTP agora funciona também em seu site (em relação aos sites da concorrência).
- **Com base em padrões.** Em conformidade com os padrões abertos da arquitetura de referência da Open AuTHentication (OATH), nenhum comprometimento fixo com fornecedores precisará ser adotado na escolha dos dispositivos de autenticação. O VIP funcionará com qualquer dispositivo de autenticação compatível com os padrões OATH. Atualmente, mais de 70 fabricantes produzem soluções compatíveis com os padrões OATH.
- **Confiável.** Há muito tempo a VeriSign tem sido um provedor de serviços de segurança para mais de 900.000 servidores Web, mais de 93% das empresas listadas na Fortune 500, os 40 maiores bancos do mundo e 43 dos 50 maiores sites de comércio eletrônico. Como resultado, o selo VeriSign Secured™ Seal tem um significado muito importante para os consumidores e tem sido historicamente associado a comércio seguro.

ALGUMAS REAÇÕES DE CONSUMIDORES À IMPLANTAÇÃO DE TOKENS OTP POR UM GRANDE SERVIÇO DE LEILÕES E PROCESSAMENTO DE PAGAMENTOS ON-LINE:

“Incrivelmente fácil.”

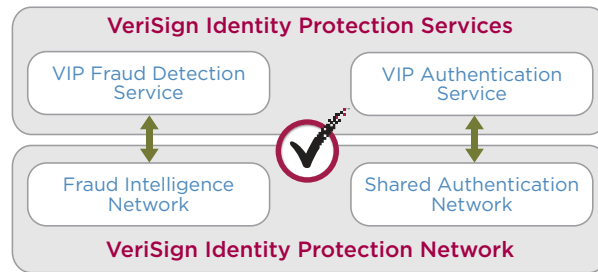
“Eu adoro! Vou tornar minha senha menos complexa porque terei minha chave de segurança sempre comigo.”

“Ele vai comigo para todos os lugares.”

“Acredito que, com a segurança adicional, eu vou aproveitar a taxa de juros de 5,03% sobre os valores depositados.”

“Um bom produto que eu gostaria que minha própria instituição financeira implementasse.”

Este documento estratégico explora como funcionam os principais componentes do VIP e como se encaixam na rede VIP Network.



+ Habilitação da migração de comércio digital

As compras on-line vêm experimentando um estrondoso crescimento na última década, tendo como principais impulsionadores a conveniência e a disponibilidade de produtos. Na temporada de compras das festas de fim de ano de 2006, mais de 66% da população on-line nos EUA efetuaram compras on-line. Os especialistas em marketing estão aperfeiçoando o hábito dos usuários on-line para oferecer sugestões de compra personalizada e impulsionar ainda mais as receitas proporcionadas pelo canal on-line.

Porém, algumas forças contrárias impedem a maximização dos canais on-line, e a segurança se encontra na linha de frente. Em uma pesquisa com mais de 5.000 adultos usuários da Internet nos EUA, aproximadamente metade afirmou que as preocupações com o roubo de informações, violações de dados ou ataques com base na Internet têm afetado seu comportamento de pagamento de compras, transações on-line ou envio/recebimento de e-mails. Se esta percepção é válida para metade de todos os adultos americanos usuários da Internet, ou mais de 155 milhões de pessoas, ela representa aproximadamente US\$2 bilhões em oportunidades de receita perdidas.

A Gartner recomenda que as empresas utilizem uma abordagem de duas frentes para recuperar essa receita perdida: tomar medidas para reduzir as fraudes, aumentando ao mesmo tempo a confiança dos consumidores; em essência, divulgar as medidas de segurança como um facilitador dos negócios.

A VeriSign acredita que a melhor forma de evitar o roubo de identidade é por meio de uma abordagem de segurança em camadas: para ajudar na prevenção do roubo de identidade por criminosos, a VeriSign recomenda a adoção da autenticação forte. Para ajudar na prevenção da utilização das identidades roubadas pelos criminosos, a VeriSign recomenda a adoção da detecção de fraudes.

Autenticação forte

A primeira linha de defesa contra o roubo de identidade é a autenticação forte. Autenticação é o processo de validação da identidade dos usuários finais. A meta é diferenciar os usuários legítimos dos impostores. O método mais simples e comum de autenticação com computadores emprega um nome de usuário e um fator único de proteção: a senha secreta. Quando os usuários efetuam seu login, os nomes de usuário identificam suas contas. As senhas provam que os usuários realmente são quem eles afirmam ser.

Problemas com senhas

Na teoria, este sistema funciona perfeitamente. De forma ideal, os usuários escolheriam senhas de difícil adivinhação por outras pessoas, senhas diferentes para cada conta e nunca compartilhariam essas senhas com outras pessoas. Infelizmente, os usuários finais raramente escolhem boas senhas, utilizam senhas diferentes para contas diferentes ou mantêm suas senhas em segredo.

As pessoas normalmente escolhem senhas simples de fácil memorização, utilizando com frequência nomes, palavras comuns e datas. Os hackers sabem disso e normalmente conseguem descobrir uma senha utilizando informações que eles sabem sobre uma pessoa (como datas de nascimento, nomes dos filhos ou outras informações), ou simplesmente chutando palavras e datas aleatórias.



A maioria dos usuários tem várias contas com diferentes serviços. Poucos usuários são capazes de lembrar uma senha diferente para cada conta e, portanto, escolhem uma única senha para ser utilizada em todos os Websites. Se a senha para qualquer um desses sites for descoberta, o acesso a todos eles estará comprometido. Os hackers podem se aproveitar disso e criar um Website “gratuito” e solicitar que os usuários se registrem para utilizar o serviço. A maioria dos usuários irá escolher o mesmo nome de usuário e senha utilizados para o acesso aos seus sites de correio eletrônico, serviços bancários e comércio eletrônico.

Finalmente, os e-mails e Websites de phishing têm sido utilizados para enganar os usuários. Muitos usuários enfrentam problemas para distinguir Websites legítimos dos falsos e podem ser enganados ao fornecer informações de contas a terceiros mal-intencionados.

Um fator adicional

A autenticação de segundo fator foi projetada para tratar desses problemas. Um bom sistema de autenticação combinará no mínimo um fator primário (algo que o usuário conhece) com um fator secundário (algo que o usuário possui ou é). Um hacker que roube somente o primeiro fator não será capaz de forjar o segundo e não conseguirá ser autenticado. De forma similar, um hacker que roube o segundo fator não conhecerá o primeiro e também não poderá ser autenticado. Os muitos tipos diferentes de fatores secundários incluem tokens, certificados digitais e dispositivos biométricos. Dependendo das necessidades específicas da empresa, um sistema de autenticação poderá requerer mais de dois fatores. Por exemplo, um sistema poderá exigir uma frase secreta, um certificado digital e um leitor biométrico, combinando, dessa forma, algo que o usuário conhece, algo que ele possui e algo que ele é.

O valor da confiança do consumidor

Além de adotar medidas para combate às fraudes, a Gartner defende o desenvolvimento da confiança dos consumidores como parte de uma estratégia para obter ou recuperar receitas perdidas por causa de preocupações com a segurança. O cliente de alto valor / alta importância representa um segmento que todos os negócios on-line cobiçam. Entretanto, ele também é um alvo especial das fraudes on-line. É compreensível o fato de que esse segmento de consumidores valoriza bastante a segurança e privacidade ao efetuar negócios on-line. Os dispositivos de autenticação forte regularmente utilizados podem associar a segurança como um atributo de marca dos comerciantes ou provedores de serviços on-line. Por sua vez, esse fato pode beneficiar as empresas ao influenciar a fidelidade dos clientes.

Detecção de fraudes

Com base na experiência em segurança de rede tradicional, e até mesmo histórico militar, todos os especialistas concordam que uma abordagem de segurança em “camadas” é a melhor solução. A detecção de fraudes oferece proteção eficaz contra o roubo de identidade, constituindo uma segunda linha de defesa quando utilizada em conjunto com a autenticação forte.

Muitos usuários on-line são receptivos às medidas adicionais de segurança, porém, essa proteção algumas vezes exige medidas adicionais durante o login e as transações comerciais. Como um primeiro estágio na implantação de uma abordagem abrangente em camadas, muitas empresas optam pela implementação de um meio passivo de detecção de fraudes, com o qual a maioria dos consumidores que utiliza o canal on-line não sofrerá nenhuma interrupção ao efetuar transações comerciais na Internet. A validação passa a ser baseada no risco, na qual somente os comportamentos fora do padrão normal dos usuários acionam a solicitação da autenticação adicional. Essas tecnologias poderosas podem oferecer uma camada inteligente e discreta para o combate às fraudes on-line.

**Detecção de transações suspeitas**

Como criaturas com hábitos, nossas ações com frequência seguem um padrão. Por exemplo, um usuário pode efetuar login em sua conta bancária e pagar contas em seu escritório no centro da cidade durante o horário de trabalho e efetuar login de sua casa fora da área central nos fins de semana. E se uma operação de login na conta fosse transmitida de um computador na Rússia na madrugada de uma quinta-feira e essa transação fosse uma transferência de todos os ativos para um banco suíço? Essa transação seria uma anomalia, ela não se encaixa no padrão normal para aquele usuário. Com a utilização de algoritmos sofisticados, os sistemas de detecção de fraudes podem “aprender” os padrões normais de utilização com o passar do tempo e detectar transações que não se enquadram nesses padrões. Essa detecção de anomalias pode ser utilizada para indicar transações potencialmente fraudulentas.

Além disso, a maior parte das empresas aprendeu com a experiência que algumas transações oferecem risco inerente. Mesmo que o sistema de aprendizagem da máquina não as classifique como anômalas, algumas transações são tão suspeitas que uma empresa pode querer efetuar dupla verificação. Por exemplo, um site de comércio eletrônico nos Estados Unidos pode querer efetuar a dupla verificação de todos os logins internacionais ou todas as compras que excederem 10.000 dólares. Uma solução completa de detecção de fraudes deverá permitir que as empresas estabeleçam regras como essas para indicar transações suspeitas.

Confirmação de identidade

Nem todas as transações suspeitas são fraudulentas. Pelo fato de um usuário final poder algumas vezes fazer algo inesperado, algumas transações aparentemente anômalas podem na realidade ser transações legítimas. Em vez de recusar a transação por completo, o sistema de detecção de fraudes de um Website deve ser complementado por um sistema de confirmação de identidade. Esse sistema é automatizado para confirmar a identidade de um usuário final. Esses sistemas deverão suportar muitos métodos automatizados diferentes de confirmação, sem o envolvimento do suporte ao cliente, inclusive solicitando a resposta a uma “pergunta secreta”; pedindo que o usuário insira um PIN enviado a ele via e-mail, via uma mensagem de texto SMS ou lida em uma chamada telefônica automática; ou que utilize um código numérico gerado por token. Isso ajuda a minimizar o custo de confirmação de identidade para o Website e também minimiza os inconvenientes para o usuário final.

+ VeriSign® Identity Protection Services

Os serviços de proteção de identidade VeriSign® Identity Protection Services são uma combinação de serviços em camadas que habilita as empresas a oferecerem transações eletrônicas de forma confiável e segura aos seus clientes, aumentando, dessa forma, a receita total e a fidelidade dos clientes. O VIP oferece mecanismos visíveis e invisíveis para proteger as transações on-line e prevenir o roubo de identidade. O serviço de detecção de fraudes VIP Fraud Detection Service oferece recursos invisíveis de monitoramento no lado do servidor e o serviço de autenticação VIP Authentication Service oferece uma solução mais visível de autenticação forte com base em padrões abertos para garantir a identidade do consumidor e proteger a integridade das transações.

VeriSign® Identity Protection Authentication Service

O serviço de autenticação VeriSign Identity Protection Authentication Service oferece uma segurança robusta e visível para aplicações comerciais on-line. O VIP Authentication Service permite que uma empresa emita e/ou aceite de forma fácil os dispositivos de autenticação de cada usuário. Ele também proporciona segurança abrangente e altamente flexível para as transações dos consumidores.

O VIP Authentication Service utiliza padrões abertos e permite que qualquer dispositivo compatível com os padrões OATH seja utilizado para autenticação. A solução oferece implementação sem servidor e suporta uma ampla gama de dispositivos de autenticação, incluindo tokens OTP, softwares de OTP, OTPs habilitados por voz, OTP em telefones celulares e OTPs via SMS.



Gerenciamento do ciclo de vida dos dispositivos

Para os clientes VIP que não desejam arcar com os encargos da emissão de dispositivos de autenticação (como a encomenda, a distribuição e o suporte técnico a tokens), a VeriSign oferece uma solução terceirizada, o Portal VIP, que emite dispositivos diretamente aos consumidores finais. O serviço também oferece suporte ao cliente de primeiro nível diretamente aos consumidores. Isso permite que as empresas terceirizem a complexidade para a VeriSign, habilitando ao mesmo tempo uma autenticação forte de vários fatores para suas aplicações on-line, de uma forma leve e de fácil integração.

Validação de dispositivos

O VIP utiliza padrões abertos e permite que qualquer iniciativa para um dispositivo compatível com os padrões OATH seja utilizada para autenticação. A OATH é uma colaboração de todo o setor para o desenvolvimento de uma arquitetura aberta de referência, utilizando os padrões abertos existentes para a adoção universal da autenticação forte. Ao oferecer suporte aos padrões abertos, a solução VIP Authentication Service pode suportar uma ampla gama de dispositivos de senha OTP, desde os tokens de hardware tradicionais até os dispositivos de fácil utilização pelos consumidores, como PDAs, flash drives USB, telefones celulares e cartões de crédito com duplo propósito.



O VIP Authentication Service inclui diversas opções para fatores suplementares, incluindo dispositivos autônomos, como tokens OTP, cartões inteligentes e tokens USB, além de dispositivos de “software”, como certificados, OTPs habilitados por voz e software para telefones celulares. O VIP facilita a oferta de qualquer uma dessas opções aos seus clientes atuais e a preparação para as futuras opções de autenticação. Os desenvolvedores de Websites poderão acessar o VIP Authentication Service através de um único conjunto de APIs, independentemente dos fatores suplementares mantidos pelo usuário final.

Integração com o VIP Authentication Service

O VIP Authentication Service é implementado como um serviço através da Internet. A integração com as aplicações de Internet é simples, utilizando uma interface baseada em serviço. O resultado é direto, os usuários não percebem uma tecnologia sofisticada por trás do login seguro.

VeriSign® Identity Protection Fraud Detection Service

A parte do VIP que é invisível ao consumidor é o serviço de detecção de fraudes VeriSign Identity Protection Fraud Detection Service. O VIP Fraud Detection Service funciona em tempo real para detectar e evitar roubo de identidade e fraude em transações. Ele inclui um sistema baseado em regras e um mecanismo heurístico comportamental exclusivo. O serviço foi projetado para ser simples e discreto para os Websites e usuários finais. Se o sistema detectar transações suspeitas, os usuários finais poderão rapidamente fornecer sua verificação adicional para confirmar suas identidades, utilizando um sistema automatizado. Por exemplo, o sistema automático do VIP Fraud Detection Service pode solicitar que o usuário se identifique mais uma vez com qualquer um dos seguintes tipos de dispositivos: um OTP, pergunta e resposta única, PIN fornecido ao usuário via e-mail, SMS ou por telefone ou chamada do atendimento ao cliente.

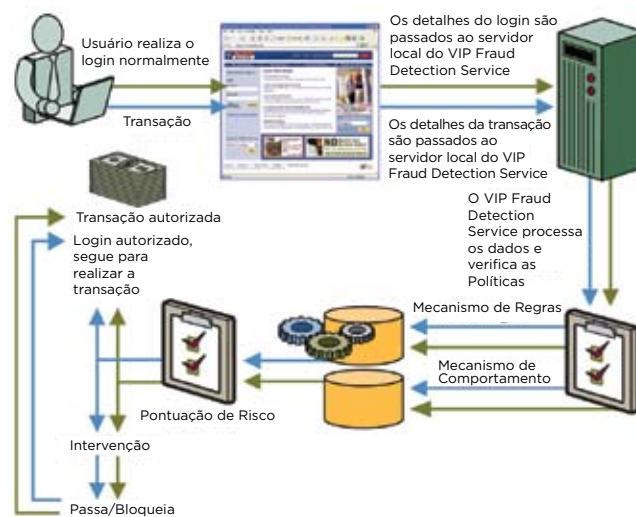
O VIP Fraud Detection Service oferece benefícios, pois ele é:

- **Invisível ao consumidor.** O VIP Fraud Detection Service não altera o hábito do usuário: Os usuários efetuam o login no Website da mesma forma com a qual estão acostumados.
- **Fácil de implantar:** Pelo fato de o VIP Fraud Detection Service ser uma solução somente no lado do servidor, ele não requer nenhuma mudança para o usuário final e requer alterações mínimas nas aplicações.
- **Inteligente:** O VIP Fraud Detection Service inclui sistemas baseados em regras e mecanismo comportamental de auto-aprendizagem para a identificação de fraudes.

Detecção de fraudes: como funciona

O VIP Fraud Detection Service utiliza uma combinação de regras de negócios e algoritmos computacionais de aprendizagem. A aplicação Web monitorada passa as informações sobre as transações ao VIP Fraud Detection Service, incluindo os cabeçalhos dos navegadores Web, o endereço IP e outros dados. O sistema VIP Fraud Detection Service poderá, então, produzir informações adicionais a partir dessas informações antes do processamento, como a determinação da localização geográfica, o tipo de conexão e o provedor de serviços de rede a partir do endereço IP. A Figura 1 abaixo mostra o fluxo lógico dos logins ou transações dos usuários monitorados pelo VIP FDS.

Figura 1: Fluxo lógico do VIP Fraud Detection Service para monitoramento de logins e transações





O primeiro componente do VIP FDS é um sistema eficiente baseado em regras. Muitas empresas vêm combatendo as fraudes on-line há anos e entendem as táticas utilizadas pelos criminosos para o roubo de dinheiro, bens e identidades. Além disso, os especialistas da VeriSign identificaram muitos padrões comuns nas transações fraudulentas. O mecanismo de regras do VIP FDS permite que as empresas combinem sua própria experiência com as informações fornecidas pela VeriSign. Os participantes podem escolher regras a partir de um conjunto de regras predefinidas desenvolvidas pela VeriSign e criar suas próprias regras, utilizando uma interface de usuário intuitiva. Adicionalmente, os serviços profissionais da VeriSign podem ajudar uma empresa a identificar padrões suspeitos e implementar regras automatizadas para a localização de padrões suspeitos específicos de seu ambiente.

O segundo componente do VIP FDS é um sistema automático de auto-aprendizagem para a detecção de anomalias. Utilizando algoritmos de agrupamento de última geração, o VIP FDS utiliza as características dos logins dos usuários, como tipo de navegador Web, endereço IP, data e hora, informações do proprietário da conta, eventuais cookies definidos pelo cliente e quaisquer outras características, para construir um perfil do comportamento normal do usuário. Quando uma tentativa de login ou outra transação não coincidir com o padrão precedente, seja porque o login foi efetuado em um computador diferente, em uma data diferente ou um país diferente, o sistema VIP FDS poderá indicar a transação como suspeita.

Uma vez que uma transação é indicada como suspeita, os clientes poderão solicitar que o sistema VIP FDS encaminhe a transação para um sistema de confirmação de identidade antes de autenticar o usuário. Esse segundo sistema irá solicitar a confirmação adicional da identidade do usuário, dependendo do grau de risco. O sistema poderá fazer perguntas adicionais ao usuário para confirmar sua identidade ou enviar uma mensagem utilizando um mecanismo externo, como uma chamada telefônica, mensagem SMS ou um e-mail. Se o usuário confirmar com sucesso sua identidade, ele será conectado como é de costume. Caso contrário, a aplicação poderá bloquear a transação ou orientar o usuário a entrar em contato serviço de atendimento ao cliente.

+ VeriSign® Identity Protection Network

O VIP Fraud Detection Service e o VIP Authentication Service oferecem uma proposta de valor atraente: uma suíte de serviços abrangentes, de fácil implementação e econômicos para a redução de fraudes e melhoria da segurança. Entretanto, o VIP oferece muito mais.

A rede VIP Network é um conjunto de serviços compartilhados que se fundamenta no VIP Fraud Detection Service e no VIP Authentication Service. A rede VIP Network consiste de dois componentes: a rede de autenticação compartilhada VIP Shared Authentication Network e a rede de inteligência contra fraudes VIP Fraud Intelligence Network. Os dois serviços VIP são aprimorados pelos efeitos de rede: o primeiro serviço ajuda as empresas a compartilharem os recursos de autenticação para reduzir custos e melhorar a interação com os usuários finais. O segundo serviço ajuda as empresas a compartilhar inteligência sobre as fraudes on-line de identidade para a melhoria da segurança.

Os clientes podem escolher a assinatura de um dos serviços separadamente ou maximizar os benefícios da afiliação à rede utilizando ambos os serviços. A rede VIP Network combina os dois serviços VIP principais em uma única estrutura de negócios que facilita o compartilhamento de custos, dados e recursos.

VeriSign Identity Protection Shared Authentication Network

A autenticação de múltiplos fatores pode ser onerosa para as empresas em termos de implantação e manutenção. Uma empresa deverá emitir tokens aos usuários finais e oferecer treinamento sobre sua utilização, alterar as aplicações para a utilização dos tokens para autenticação, auxiliar os usuários com tokens perdidos ou quebrados e esclarecer dúvidas de suporte sobre eles, e dezenas de outras tarefas.



Além disso, os clientes poderão resistir à autenticação de vários fatores pelo fato de não estarem familiarizados com ela e por consumir tempo. A rede VIP Network oferece o benefício da autenticação compartilhada para tratar esses problemas. Uma boa parte do sucesso dos cartões de crédito e dos caixas eletrônicos (ATM) se deve a sua onipresença: eles podem ser utilizados em quase todos os lugares da mesma forma. Os clientes raramente encontram caixas eletrônicos nos quais seus cartões não funcionam. Acreditamos que os usuários finais estarão mais propensos a adotar o segundo fator se puderem utilizar o mesmo dispositivo em todos os serviços e se esse dispositivo funcionar da mesma forma para todos eles.

Com o compartilhamento da infra-estrutura de autenticação entre os membros da rede, os custos da adição e manutenção do segundo fator serão drasticamente reduzidos. Ao adotarem o padrão VIP, as empresas poderão garantir uma experiência simples e consistente da parte do usuário em toda a Internet. Terceirizando o gerenciamento do ciclo de vida do token para a VeriSign, os encargos de gerenciamento dos segundos fatores e da infra-estrutura desaparecem. Para facilitar essa capacidade, a rede VIP Network se baseia em uma estrutura de compartilhamento de recursos e inteligência entre os membros da rede.

Funções na rede

As duas formas de estar na rede VIP Network são como emissor ou como parte confiável. Uma empresa que emite os dispositivos de autenticação da rede VIP Shared Authentication Network aos seus clientes é um emissor. Uma empresa que permite a autenticação de seus usuários utilizando os dispositivos de outros emissores dentro da rede VIP Shared Authentication Network é denominada parte confiável. Uma empresa pode desempenhar ambas as funções, emitir dispositivos para alguns usuários e aceitar para outros os dispositivos emitidos por terceiros. Um emissor pode incluir sua própria marca nos tokens que ele emite, mas deve também incluir o logo VIP Network. Um emissor é o primeiro ponto de contato para um cliente na rede VIP Network.

O emissor do dispositivo também é o ponto de contato para o usuário final. Os usuários finais contatam o emissor para suporte ao cliente de primeiro nível, como problemas de sincronização e reinicializações de PIN. A VeriSign pode ajudar nas dúvidas de suporte mais difíceis.

Uma empresa comprometida com autenticação forte poderá emitir seus próprios tokens que podem ser usados na rede VIP Network. Os emissores têm todos os benefícios que possuem as empresas que atuam como partes confiáveis, juntamente com as oportunidades para a promoção de suas marcas através do token e o melhor controle dos hábitos on-line de seus clientes finais. A rede VIP Network é uma forma simples de proteger o estilo de vida dos usuários na Web.

Compartilhamento de dispositivos

Para promover compatibilidade e utilização, duas regras básicas regem a rede VIP Network:

- Se uma empresa emite dispositivos de segundo fator aos seus usuários finais, ela concorda em permitir que esses dispositivos sejam utilizados para autenticação por qualquer membro da rede.
- Todos os membros da rede concordam em aceitar os dispositivos de autenticação emitidos por qualquer outro membro da rede.

Em resumo, um usuário final que receba um dispositivo de um membro da rede VIP Network sabe que ele poderá ser utilizado como um segundo fator em qualquer site dentro dessa rede.

VeriSign Identity Protection Fraud Intelligence Network

A rede de inteligência contra fraudes VIP Fraud Intelligence Network é um conjunto de serviços compartilhados na rede VIP Network que se baseia no VIP Fraud Detection Service e ajuda as empresas a acumular experiência sobre eventos de fraude on-line de identidade ocorrendo fora de suas empresas.



Os criminosos na Internet utilizam muitos mecanismos diferentes para a captura de informações pessoais, incluindo sites de phishing, key loggers, sites falsos de lojas e roubo de banco de dados. Com frequência, eles tentam utilizar as mesmas informações em vários Websites, testando as informações de login por meio de tentativa e erro, estabelecendo várias contas fraudulentas ou outras atividades nocivas. No mundo off-line, pelo fato de os bancos e as empresas de cartões de crédito saberem que os fraudadores reutilizam com frequência as informações de identidade roubadas, eles estabeleceram consórcios de compartilhamento de dados para identificar aplicações e o uso de contas fraudulentas. A mesma abordagem pode ser utilizada para impedir o roubo de identidade e a fraude de contas na Internet.

A rede VIP Fraud Intelligence Network utiliza a visibilidade única da VeriSign nas ameaças à Internet, obtida a partir da operação global de tecnologias importantes da Internet, como os serviços gerenciados de segurança VeriSign® Managed Security Services e os serviços de inteligência de segurança VeriSign® iDefense® Security Intelligence Services, bem como das informações coletadas de outros parceiros da VeriSign. A rede VIP Fraud Intelligence Network irá utilizar os padrões emergentes em desenvolvimento na OATH para o compartilhamento das informações sobre fraudes de transações (“thrauds”).

+ VeriSign: um parceiro confiável

Os Serviços VIP e a rede VIP Network fazem parte da infra-estrutura de Internet da VeriSign. Bilhões de vezes ao dia, as empresas e os consumidores confiam na infra-estrutura de Internet da VeriSign para a comunicação e condução de transações comerciais confiáveis.

Atualmente, mais de 91.000 Websites em 150 países exibem o selo VeriSign Secured™ Seal, permitindo que os clientes confirmem a identidade dos sites de comércio eletrônico. A VeriSign está entre as marcas mais confiáveis para a segurança na Internet.

As soluções SSL da VeriSign protegem mais de 40 dos maiores bancos do mundo, 43 dos maiores sites de comércio eletrônico e 93% das empresas listadas na Fortune 500.

A VeriSign opera como um provedor de serviços terceirizados confiável para um conjunto variado de aplicações, que vão desde o envio de mensagens multimídia e de texto entre operadoras até o suporte a votações de altos volumes por SMS em programas populares de TV.

A VeriSign também opera muitos dos serviços centrais para a Internet e redes de telecomunicações, incluindo os operadores de registros de domínios .com e .net, processando em torno de 30 bilhões de consultas em um único dia.

A equipe de operações da VeriSign acumula décadas de experiência na operação de infra-estrutura crítica, mantendo-a segura e disponível. A VeriSign monitora, gerencia e protege as redes das principais instituições financeiras, empresas de serviços públicos, agências governamentais e outras empresas através dos serviços gerenciados de segurança VeriSign Managed Security Services.

Por fim, os serviços iDefense Security Intelligence Services oferecem às empresas a melhor e mais original pesquisa sobre ameaças e vulnerabilidades emergentes. Os pesquisadores do iDefense monitoram fóruns de hackers em inglês, russo, chinês e outros idiomas. Essa pesquisa é utilizada para o aperfeiçoamento dos serviços VIP Fraud Detection Services.

Toda esta experiência e especialização são utilizadas na rede VIP Network. Os Serviços VIP são executados pela VeriSign para que você possa ter a certeza de que são seguros e confiáveis. Nenhuma empresa pode oferecer a você melhor proteção contra fraudes ou contra roubo de identidade a seus clientes.

**+ Pesquisa e desenvolvimento associados**

Atualmente, os Serviços VIP e a rede VIP Network constituem um pacote de serviços de autenticação inteligentes, de fácil utilização, abrangentes e de baixo custo. Entretanto, estamos trabalhando em outras iniciativas para estender os Serviços VIP e a rede VIP Network para oferecer uma proteção de identidade ainda melhor.

Serviços de autenticação mútua

A autenticação de vários fatores torna obsoletos os ataques planejados para a captura de senhas de usuários finais, como phishing, key logger e eavesdropping. Esses são os ataques mais comuns utilizados pelos hackers atualmente. Entretanto, ataques do tipo man-in-the-middle (como os ataques tipo “evil twin” em redes sem fio) estão se tornando mais comuns e provavelmente se tornarão um problema significativo no futuro.

A VeriSign trabalha de forma contínua com os fornecedores de navegadores para facilitar a diferenciação entre empresas legítimas e impostores pelos usuários finais. O Certificado Extended Validation SSL (EV SSL) é um resultado dessa pesquisa. O EV SSL oferece aos visitantes de Websites uma forma simples e confiável para ampliar sua confiança on-line. A partir do Microsoft® Internet Explorer 7 (e nas novas versões do Firefox e Opera), a barra de endereços assume a cor verde e exibe o nome do proprietário do Certificado EV SSL.

Além disso, a VeriSign está trabalhando com grupos de padrões como a OATH para desenvolver técnicas adicionais de autenticação de usuário. À medida que elas forem sendo disponibilizadas, a VeriSign pretende expandir a suíte de serviços VIP para ajudar a oferecer uma vivência ainda mais segura aos usuários finais.

Gerenciamento de identidades de consumidores

Além da necessidade da autenticação de usuários, as empresas e os consumidores ainda buscam uma melhor solução para o problema do gerenciamento de identidades: Como consumidor, como eu posso utilizar a mesma “identidade” em vários Websites e gerenciar as informações confidenciais compartilhadas com esses sites? É possível acessar vários Websites com um único login?

A pesquisa nessa área inclui trabalhos da Liberty Alliance (ID-WSF-2.0), Microsoft (CardSpace), Eclipse Foundation (Higgins) e OpenID. Os laboratórios VeriSign Labs são um importante contribuidor para essa pesquisa e conta com uma implementação da OpenID disponível em <https://pip.VeriSignlabs.com/>

Como essas soluções complementam a detecção de fraudes e a autenticação forte, a VeriSign continuará a determinar quais novos benefícios poderão ser obtidos por meio da expansão dos serviços da rede VIP Network.

Serviços de comprovação de identidade

Quando os usuários se registram inicialmente em um Website, sua identidade deve ser validada. Se eles não tiverem nenhum relacionamento off-line com o Website, essa validação pode ser arriscada. Os ladrões de identidades sabem disso e, com frequência, abrem contas em nome de outras pessoas. A pesquisa da FTC Clearinghouse mostrou que mais de 20% das fraudes bancárias, 60% das fraudes com cartões de crédito e 95% dos incidentes de fraudes telefônicas e com empresas de serviços públicos envolviam a criação de novas contas.

Os serviços de comprovação de identidade oferecem um meio pelo qual um terceiro confiável pode ajudar a confirmar a identidade de um usuário final ou consumidor de um Website, em benefício de ambas as partes.

Isto pode ser feito on-line, por meio de uma série de perguntas relacionadas ao usuário final, ou off-line, por meio de várias fontes e documentos de identidade. A experiência da VeriSign como uma Autoridade Certificadora é importante para essa oportunidade emergente, e ela continuará a pesquisar formas de incentivar a evolução da rede VIP Network.



+ Saiba Mais

Para obter mais informações sobre o VeriSign Identity Protection, ligue para 55 11 5853 2900 ou envie um e-mail para faleconosco@VeriSign.com.

+ Sobre a VeriSign

A VeriSign é um provedor confiável de serviços de infra-estrutura de Internet para o mundo digital. Bilhões de vezes por dia, empresas e consumidores confiam em nossa infra-estrutura de Internet para se comunicarem e realizarem transações comerciais com confiança.

Visite o nosso site em www.Verisign.com.br para obter mais informações.

©2008 VeriSign BRASIL LTDA. Todos os direitos reservados. VeriSign, o logotipo da VeriSign e o círculo com marca de verificação são marcas registradas ou marcas comerciais da VeriSign e de suas subsidiárias nos Estados Unidos e em outros países. Todas as outras marcas comerciais são de propriedade de seus respectivos donos.

00026332 15/09/08

GB 011/08