



DOCUMENTO ESTRATÉGICO

Aproveite os Benefícios
de uma Rede de Autenticação
Compartilhada para Impulsionar
a Retenção de Consumidores
e Fortalecer a Diferenciação Competitiva





ÍNDICE

+ Introdução	3
+ Entenda o Compartilhamento	3
+ Este é o Momento para uma Rede de Autenticação	4
+ Aproveite a Oportunidade	4
+ Como uma Rede de Autenticação Compartilhada Funciona	5
+ Os Atraentes Benefícios de uma Rede de Autenticação Compartilhada	6
+ Vantagens Exclusivas dos Primeiros a Adotar a Rede	7
+ Conclusão	7
+ A Rede VeriSign® Identity Protection (VIP) Network	8
+ Saiba Mais	8
+ Sobre a VeriSign	8



LEI DE METCALFE: O COMPARTILHAMENTO NAS COMUNICAÇÕES

Apesar de o conceito de compartilhamento ter sido inicialmente apresentado no início dos anos 90 pela Bell Telephone, ele foi mais recentemente popularizado por Robert Metcalfe, um dos co-inventores da Ethernet. Metcalfe argumentou que o número de usuários de cartão de Ethernet precisava crescer acima de uma determinada massa crítica se os usuários quisessem colher os benefícios de suas redes.

Expressada de forma matemática, a lei de Metcalfe declara que o valor de uma rede de telecomunicações é proporcional ao quadrado do número de usuários do sistema (n^2). Essa lei foi utilizada para explicar os efeitos do compartilhamento das tecnologias de comunicação e redes como a Internet.

Aproveite os Benefícios de uma Rede de Autenticação Compartilhada para Impulsionar a Retenção de Consumidores e Fortalecer a Diferenciação Competitiva

+ Introdução

Pessoas e empresas em todo o mundo se beneficiam do “compartilhamento” todos os dias – a maioria sem nem se dar conta. Esse poderoso fenômeno é a força propulsora por trás de diversas inovações que agora consideramos necessárias. Tecnologias e serviços que eram raros, tais como telefone, caixas automáticos, aparelhos de fax, e-mail e Ethernet, tornaram-se onipresentes porque o valor de todos eles aumenta à medida que aumenta o número de participantes na rede.

E se esse conceito fosse aplicado ao problema de proteger os consumidores dos crimes cibernéticos, como roubo de identidade, phishing e fraude? O uso de uma autenticação mais forte pelos consumidores, como a autenticação de dois fatores, poderia enfim ser amplamente adotado.

Empresas visionárias estão reconhecendo que uma rede de autenticação compartilhada de dois fatores é o modelo estratégico que pode resolver as preocupações do consumidor com a segurança ao mesmo tempo em que impulsiona a adoção pelo usuário. Elas percebem que esta é a porta de entrada para aumentar a fidelidade do cliente, melhorar a diferenciação e conseguir um crescimento orgânico e lucrativo por meio de estratégias online.

As recompensas por participar de uma rede de autenticação compartilhada vão muito além do que uma única empresa poderia conseguir. Os participantes obtêm custos mais baixos, menor risco, maior proteção contra fraude e maior sucesso e aceitação das ofertas online que se tornam seguras para os consumidores por meio da autenticação forte.

Este documento estratégico apresenta o conceito de uma rede de autenticação compartilhada de dois fatores e mostra por que uma rede compartilhada para autenticação forte é um requisito essencial para a participação contínua do cliente em interações e comércio online. Ele explica ainda como o compartilhamento pode ajudar a impulsionar a ampla adoção à autenticação forte pelo consumidor e trata dos benefícios significativos disponíveis para as organizações que escolhem participar da rede.

+ Entenda o Compartilhamento

O conceito do compartilhamento já é reconhecido há pelo menos 100 anos, desde o advento do telefone. Um exemplo clássico na história mais recente é o caixa eletrônico. Inicialmente os caixas eletrônicos estavam limitados a um cartão por banco. Os usuários podiam sacar dinheiro e realizar outras transações somente nos caixas eletrônicos de seus próprios bancos. Com o aumento do uso dos caixas eletrônicos, surgiram as redes interbancárias permitindo que os clientes usassem seus cartões em qualquer banco que participasse da rede. Hoje em dia, os usuários de caixas eletrônicos podem acessar suas contas a partir de milhares de locais, e os cartões podem ser usados de diversas formas, servindo como cartão de débito, cartão de saque e outros.

Os telefones celulares são outro exemplo recente dos benefícios do compartilhamento. As operadoras compreenderam que quanto mais a rede de consumidores com telefones celulares crescia, mais pessoas viam o valor de possuir um. À medida que o número de usuários de telefone celular se aproximava de uma massa crítica, a cobertura do serviço aumentou e as taxas de roaming começaram a desaparecer. Outros exemplos lucrativos do compartilhamento incluem e-mail, mensagens instantâneas e até a Web em si.

“O conceito da rede compartilhada aborda dois impulsionadores-chave que ajudarão a difundir a adoção da autenticação do consumidor: conveniência e facilidade de uso para os consumidores. Isso fornece aos consumidores uma solução conveniente e fácil de usar para lidar com suas preocupações com roubo de identidade usando do mesmo dispositivo em diversos Web sites. Além disso, as empresas estabelecem confiança com seus usuários sem ter de carregar todo o fardo dos custos de implementação e desenvolvimento.”

- Sally Hudson, IDC

Um exemplo não-tecnológico é o modelo adotado pelas companhias aéreas, conhecido como “hub-and-spoke”. Esse modelo consiste em oferecer aos passageiros mais opções de escolha de destinos. À medida que mais pessoas escolhem estes destinos, mais rotas são disponibilizadas, aumentando ainda mais a conveniência para os passageiros, ao mesmo tempo em que oferecem maiores oportunidades de serviço para as empresas aéreas.

O mesmo conceito do compartilhamento pode ser desenvolvido e aplicado para oferecer benefícios significativos para as empresas que participam de uma rede de autenticação segura com base na autenticação forte ou de dois fatores. Com maior adoção e maior confiança dos clientes, as empresas que participam da rede obtêm novas oportunidades de branding, maior fidelidade do consumidor e menor custo e risco à segurança. Empresas visionárias estão percebendo esses benefícios e colhendo as recompensas da adoção antecipada agora.

+ Este é o Momento para uma Rede de Autenticação

Em 31 de março de 2008, havia 1,4 bilhão de usuários de Internet¹ navegando na Web em todo o mundo. Esses consumidores online trocam e-mails, participam de redes sociais, reservam viagens, baixam músicas, fazem compras e muito mais. Embora a Internet tenha transformado radicalmente a maneira como as pessoas vivem, trabalham e se divertem, o potencial para aproveitar a Internet para aplicações de negócios ainda mais inovadoras está longe de se esgotar.

Hoje, a segurança está ameaçando inibir o crescimento e a inovação online. De phishing a malware, a Internet está literalmente repleta de criminosos que utilizam um arsenal de armas para fraudar consumidores e empresas. Um relatório recente da Comissão Federal de Comércio mostrou que, pelo oitavo ano consecutivo, o roubo de identidade foi a reclamação número um dos consumidores.

As tendências mostram que o alvo dos criminosos não é mais apenas as instituições financeiras. Varejo online, saúde, transporte e muitos outros setores agora também são visados, à medida que os criminosos cibernéticos buscam maneiras de diversificar e se tornar mais sofisticados.

+ Aproveite a Oportunidade

Nenhuma solução de segurança pode ser eficiente se os consumidores não a utilizarem. Embora a autenticação de dois fatores ofereça a segurança melhorada necessária para combater os crimes cibernéticos, a adesão tem sido mais lenta do que o desejado. Os dados indicam que os consumidores estão relutantes em manter diversos dispositivos de autenticação para os diversos sites que freqüentam.

Esta aparente barreira à adoção determina o ponto central do que talvez seja a solução de segurança na Internet mais inovadora e fácil de usar: a rede de autenticação compartilhada de dois fatores. As empresas compartilham uma infra-estrutura de autenticação confiável, e os consumidores podem utilizar um único dispositivo de segurança para autenticar suas identidades em qualquer Web site membro da rede.

Uma rede de autenticação compartilhada oferece um método de autenticação de dois fatores eficiente e extremamente fácil de usar que incentiva e recompensa a adoção do consumidor com o uso de um único dispositivo em diversos Web sites. Ele possibilita a autenticação de dois fatores, que é fácil de usar (independentemente do nível de sofisticação da tecnologia do consumidor) e conveniente para os consumidores.

¹ www.internetworldstats.com, Miniwatts Marketing Group

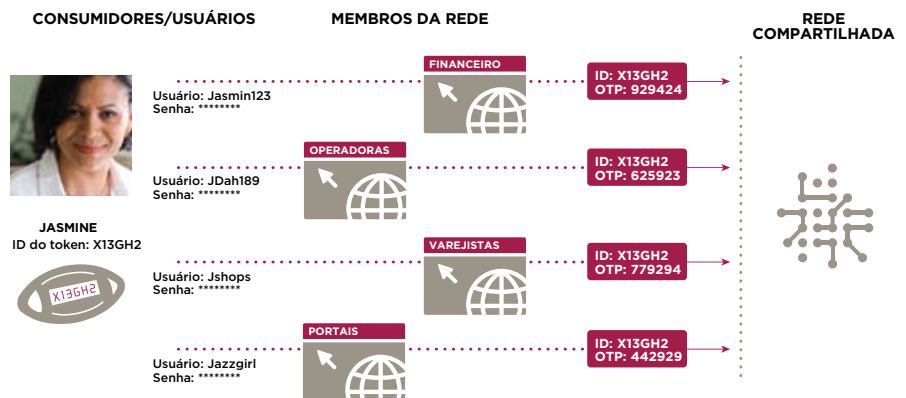
² “Consumer Fraud and Identity Theft Complaint Data” (Dados sobre as reclamações do consumidor quanto a roubo de identidade e fraude), janeiro-dezembro de 2007, Comissão Federal de Comércio, 13 de fevereiro de 2008

+ Como uma Rede de Autenticação Compartilhada Funciona

Com uma rede de autenticação compartilhada, em vez de utilizar um dispositivo de autenticação diferente para cada conta online, os consumidores elegem um de seus dispositivos para o acesso seguro a qualquer Web site que exiba o logotipo ou identificação da rede compartilhada. A identidade do consumidor e as informações da transação permanecem dentro do sistema da empresa participante; somente o código de segurança, ou a senha dinâmica de uso único (OTP – One Time Password), e a ID do dispositivo são passados anonimamente para o host compartilhado de autenticação para validação. Isso permite que as empresas continuem a controlar o hábito de seus clientes na Internet ao mesmo tempo em que aumentam a segurança com a autenticação forte.

A Figura 1 abaixo mostra como um consumidor interage com as empresas que participam da rede. O mesmo dispositivo é usado para oferecer autenticação forte para a identidade do consumidor em todos os diversos Web sites com os quais ele interage. Ao mesmo tempo, a autenticação pelo host da rede é transparente para o consumidor.

Figura 1: Hábito do Consumidor com uma Rede de Autenticação Compartilhada de Dois Fatores



Além disso, ter uma rede de empresas participantes possibilita que experiências de segurança e inteligência contra fraude sejam compartilhadas instantaneamente em toda a rede, aumentando a segurança para cada empresa e da rede como um todo.

O modelo de rede também permite variações na maneira em que as empresas participam. Os membros da rede podem simplesmente aceitar dispositivos de autenticação emitidos por outros membros ou aproveitar os diversos benefícios da participação na rede. Por outro lado, as organizações podem ter a oportunidade de emitir seus próprios dispositivos. Esses dispositivos, que podem ser tokens, mensagens de texto enviadas para um telefone celular, ou um cartão de segurança, por exemplo, podem ter a marca da empresa – fornecendo ao emissor, proprietário da marca, uma maior exposição à sua base de clientes e a outras pessoas.

Em uma pesquisa conduzida pela VeriSign na conferência eBay® Live™ em junho de 2007, as respostas mostraram que os clientes da PayPal™ estão muito interessados em utilizar um dispositivo de autenticação compartilhada de dois fatores (token, neste caso), para outros sites que visitam na Internet. Na verdade, 84% disseram que estavam interessados em utilizar o token em seu banco, 52% queriam usá-lo em sua corretora, 49% expressaram interesse em usar o token para propósitos de saúde, e 67% queriam utilizá-lo para outras transações, como compras e jogos online.



+ Os Benefícios Atrativos de uma Rede de Autenticação Compartilhada

Para os consumidores, a autenticação compartilhada oferece o porto seguro de que precisam para se sentir confiantes com relação ao uso da Internet e ao comércio online. Eles obtêm maior segurança sem ter de sacrificar a conveniência. E, com o tempo, quanto mais sites participarem da rede, o valor da solução de segurança aumenta para cada consumidor, o que impulsiona maior adoção.

Com uma rede de autenticação compartilhada, a maior parte do custo, risco e esforço exigidos para assegurar níveis contínuos de autenticação forte é distribuída entre muitas empresas. Semelhante às vantagens do software como serviço (SaaS), as empresas participantes de uma rede de autenticação compartilhada não precisam do investimento de capital inicial associado a uma solução interna de autenticação. Por ser uma solução hospedada, não há software para instalar e manter, nenhum hardware adicional exigido e nenhum encargo de suporte ou manutenção. Escala e confiabilidade são facilitadas pelo host da rede compartilhada.

Os membros da rede mantêm o controle do hábito do cliente, enquanto se beneficiam das economias de custo e da maior aceitação da solução pelos clientes. O fato de não precisarem se preocupar com o desenvolvimento personalizado permite que as organizações ajudem a acelerar o prazo para lançamento de serviços e ofertas mais seguros. E esses benefícios aumentam à medida que cada vez mais organizações se associam à rede, efetivamente amortizando os custos.

Além das economias de custo e de esforços de uma rede de autenticação compartilhada, ela também oferece oportunidades únicas de branding e compartilhamento de receitas para as empresas que participam como emissoras de dispositivos de autenticação (tokens). Essas empresas podem se certificar de que suas marcas estejam na frente de seus clientes todas as vezes que eles visitarem os Web sites participantes da rede. E a exposição da marca não pára por aqui. As empresas participantes da rede obtêm maior exposição fora da sua base de clientes, já que consumidores com dispositivos de autenticação de outros emissores visitam seus sites.

Para os membros da rede que emitem dispositivos, os programas de compartilhamento de receitas, que estão atualmente sendo implementados por prestadores de serviço da rede de autenticação, podem ajudar a compensar uma parte do custo do serviço. Quando esses programas de compartilhamento de receitas estiverem disponíveis, cada vez que um dispositivo de um emissor for ativado por outros membros da rede, o emissor receberá uma parcela da taxa paga por esse usuário.

Uma Rede de Autenticação Compartilhada: do Início ao Fim

Em uma situação de teste, um site de leilões online sabe que as preocupações com segurança fizeram com que o crescimento nas transações de clientes desacelerasse. Os dados indicam que a oferta da autenticação de dois fatores é considerada aumento de valor por um segmento de seus principais usuários. No entanto, os dados também mostram que esses usuários desejam a conveniência de usar um único dispositivo de autenticação em diversos sites.

Com um investimento inicial razoável, o site de leilões se associa a uma rede de autenticação compartilhada de dois fatores, além disso, decide ser um emissor de dispositivos para aproveitar melhor as vantagens das oportunidades de exposição da marca junto a esses clientes de alto valor. Embora a adoção inicial seja rápida dentro do segmento de usuários de alto valor, a organização fica positivamente surpresa quando a adoção migra também para outros segmentos de clientes. À medida que outros sites se associam à rede, o logotipo da rede se torna mais reconhecido, com cada vez mais usuários enxergando o valor do dispositivo único de autenticação. O site também fica feliz em observar um aumento na receita, pois os dispositivos com sua marca são usados em outros sites participantes.



O número de empresas que participam da rede continua a crescer, oferecendo mais oportunidades de autenticação forte para os usuários enquanto mantém a conveniência. Os consumidores agora estão ficando relutantes em realizar transações em sites que não fazem parte da rede compartilhada, solidificando a fidelidade e criando oportunidade para mais transações com as empresas participantes. Clientes internacionais são atraídos pela maior segurança da rede e começam a fazer negócios no site de leilões, aumentando efetivamente o alcance geográfico do site. Ele começa a vender serviços adicionais para seus portadores de dispositivos de autenticação.

Quando a massa crítica da rede é atingida, quase todos os usuários do site de leilões agora querem a autenticação de dois fatores. A empresa é vista como líder em segurança do consumidor e em proteção contra fraude de ponta. Ela aumentou sua presença entre outros sites membros da rede e recebe da provedora da rede uma parcela da receita por seus dispositivos estarem sendo utilizados em outros sites. Os dispositivos com a marca do site de leilão são usados em milhares de sites participantes todos os dias. A fidelidade do cliente e as transações aumentaram, e o relacionamento com o dispositivo de autenticação oferece um valioso canal para oportunidades futuras de branding, vendas e serviços. A satisfação é alta, e o número de incidentes e o custo relacionado à fraude foram reduzidos. O benefício total do compartilhamento foi percebido.

+ Vantagens Exclusivas dos Primeiros a Adotar a Rede

Por que ser o primeiro em uma rede de autenticação compartilhada? Há benefícios diferenciados esperando pelas primeiras empresas a adotar a rede. Essas vantagens vão além da solução de segurança efetiva, escalonável, confiável e forte que a rede possibilita. Participar de uma rede de autenticação compartilhada logo no início de seu ciclo de vida estabelece uma diferenciação competitiva, ajuda a posicionar a empresa como líder e visionária no setor e obtém cobertura positiva de mídia por introduzir soluções inovadoras de segurança. Para empresas que buscam uma fatia do mercado internacional, a rede atrai clientes potenciais de países em que a autenticação compartilhada de dois fatores do consumidor já é uma solução conhecida e respeitada.

+ Conclusão

Uma rede de autenticação compartilhada eleva a condição da autenticação de dois fatores de uma simples medida de segurança para uma oportunidade estratégica de negócios. Os benefícios criados por uma rede de autenticação compartilhada vão além de tranquilizar os receios quanto à segurança e proteger os resultados – a participação pode ser uma base de lançamento para ofertas online diferenciadas e inovadoras.

Qualquer empresa com uma aplicação de gestão de conta online hoje em dia, ou que esteja considerando a possibilidade de ter uma, deve buscar mais informações sobre a autenticação compartilhada de dois fatores e sobre as vantagens do compartilhamento. Então elas devem usar esse conhecimento para desenvolver um modelo de estratégia que ajude a moldar o futuro uso da Internet e a estabelecer liderança competitiva no fornecimento de um hábito online seguro.

**+ A Rede VeriSign® Identity Protection (VIP) Network**

Os serviços de proteção de identidade VeriSign® Identity Protection (VIP) Services ajudam os consumidores a fazerem o login em suas contas de forma conveniente e segura para utilizarem os serviços online da sua empresa. A autenticação de dois fatores, a detecção de fraudes com base em auto-aprendizagem e uma poderosa infra-estrutura de validação ajudam a fornecer uma solução de ponta a ponta segura e a um custo razoável, da marca de segurança mais reconhecida da Internet.

Empresas que são membros da rede VIP Network se beneficiam do compartilhamento de uma infra-estrutura de validação única e externa com inteligência global. Os consumidores que utilizam convenientemente um dispositivo único para fazer o login em diversos Web sites têm a proteção adicional da autenticação de dois fatores. A rede de inteligência contra fraudes VeriSign® Fraud Intelligence Network oferece notificação antecipada de ataques e listas abrangentes de suspeitos para bloquear fontes de fraude potenciais.

+ Saiba Mais

Para obter mais informações sobre a proteção de identidade VeriSign Identity Protection, ligue para 55 11 5853 2900 ou envie e-mail para: faleconosco@verisign.com.

+ Sobre a VeriSign

A VeriSign é a fornecedora confiável de serviços de infra-estrutura de Internet para o mundo digital. Bilhões de vezes por dia, a VeriSign ajuda empresas e consumidores de todas as partes do mundo a se comunicar e realizar transações com segurança.

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 propriedades de seus respectivos titulares.

00026465 17/09/08

GB 013/08