



# Construção de confiança em um céu nebuloso

## Visão global das organizações de serviços financeiros

99%



das organizações de serviços financeiros **executam algum tipo de serviço de nuvem**

57%



das organizações de serviços financeiros **usam soluções híbridas de nuvem pública/privada**

48%



dos entrevistados **atrasaram sua adoção da nuvem** por falta de qualificação em segurança cibernética

De acordo com nosso estudo, as empresas de serviços financeiros são mais propensas a usar serviços de nuvem do que qualquer outro setor. Enquanto 99% dessas organizações usam funções de nuvem, a média do setor como um todo é de 93%. As organizações de serviços financeiros estão entre as que mais implementaram a filosofia de “nuvem em primeiro lugar”, optando por distribuir um serviço interno somente quando não estiver disponível uma variante adequada para a nuvem. Com isso, 87% implementam essa filosofia, enquanto a média das organizações em geral é de 82%. Nós também constatamos que as arquiteturas de TI do setor de serviços financeiros estão mudando rapidamente de uma infraestrutura de data center de nuvem privada para um modelo híbrido de nuvem privada/pública. Nossos entrevistados esperam que 80% de seus orçamentos de TI sejam baseados na nuvem dentro de um prazo médio de 14 meses.

Esta análise de adoção dos serviços de nuvem pelo setor de serviços financeiros, suas preocupações e seus planos para o futuro foi extraída da **Pesquisa sobre nuvem de 2016**, da Intel Security. Foram entrevistados tomadores de decisões de TI de nível técnico sênior de diversas localidades: Alemanha, Austrália, Brasil, Canadá, Cingapura, Estados Unidos, França, Golfo Pérsico (Arábia Saudita e Emirados Árabes Unidos), Japão, México e Reino Unido.

### Principais descobertas: serviços financeiros

As organizações de serviços financeiros lideram a adoção da nuvem (99% das organizações entrevistadas), empatadas apenas com as empresas de tecnologia. A porcentagem indica a parcela do setor que usa algum tipo de serviço de nuvem. As arquiteturas de nuvem dessas empresas mudaram consideravelmente no ano passado. A quantidade de empresas com serviços de nuvem exclusivamente privados caiu de 50% em 2015 para 26% em 2016, conforme as empresas foram migrando para soluções híbridas de nuvem privada/pública. Hoje, as soluções híbridas são usadas por 57% das organizações de serviços financeiros.

Quase metade (48%) dos profissionais de serviços financeiros entrevistados afirmaram ter atrasado sua adoção da nuvem devido à falta de qualificação na área de segurança cibernética de suas equipes de TI. Ainda que diversas preocupações com a segurança e a qualificação exigida na área estejam diminuindo o ritmo de adoção, a confiança e a percepção dos serviços de nuvem pública continuam aumentando a cada ano. A maioria das organizações de serviços financeiros considera

54%



dos entrevistados de serviços financeiros rastrearam uma **infecção de malware até um aplicativo SaaS**

64%



das organizações de serviços financeiros **armazenaram alguns ou todos os dados confidenciais de clientes** em nuvens públicas

39%



dos serviços de nuvem são **contratados sem o envolvimento da TI, sendo que a TI só tem visibilidade sobre menos de 45%** deles

os serviços de nuvem pública tão seguros quanto os de nuvem privada (ou até mais seguros), com chances muito maiores de proporcionar redução dos custos de propriedade e melhor visibilidade dos dados. Estar a salvo de hackers foi a única vantagem apontada como mais provável na nuvem privada do que na pública.

Os aplicativos de nuvem continuam sendo um vetor para ataques cibernéticos e mais da metade (54%) dos entrevistados do setor de serviços financeiros indicaram ter rastreado conclusivamente uma infecção de malware até um aplicativo SaaS. Porém, essas organizações estão entre as menos propensas a passar por perdas de dados ou violações (19% em relação à média global de 22%).

**Mais de dois terços das organizações de serviços financeiros confiam nas nuvens públicas.** Esse aumento de confiança e percepção, bem como a maior compreensão dos riscos pela diretoria sênior, está incentivando mais organizações a armazenar dados confidenciais na nuvem pública. Talvez devido à natureza onipresente das transações e de diversos serviços financeiros on-line, essas organizações estão entre as mais propensas a armazenar alguns ou todos os dados confidenciais de clientes na nuvem pública (64%).

Os profissionais seniores de TI do setor de serviços financeiros afirmam ser mais propensos a usar SaaS (64%), seguido de perto por IaaS (57%). O modelo PaaS ocupa um distante terceiro lugar (38%). Porém, esses profissionais pretendem investir mais em IaaS no ano que vem: 69% têm planos de aumentar suas atividades nessa área, enquanto 60% querem investir mais em SaaS e 52% pretendem investir mais em PaaS.

Assim como acontece com outras organizações, a maior preocupação do setor de serviços financeiros com o uso de SaaS é a proteção de dados confidenciais em trânsito de/para a nuvem. Já entre as ofertas de IaaS, o que mais preocupa é a manutenção da conformidade e a possibilidade de acesso não autorizado em nuvens públicas multilocatárias. Isso difere de outras organizações, que apontaram controles de segurança consistentes como a maior preocupação em IaaS. A quantidade média de serviços de nuvem em uso pelas organizações de serviços financeiros caiu de 40 em 2015 para 29 em 2016, indicando uma possível consolidação dos provedores de nuvem.

A TI oculta é um problema para os departamentos de TI do setor de serviços financeiros, assim como acontece com os departamentos de TI da maioria dos setores. Os profissionais de TI de serviços financeiros relatam que serviços de nuvem contratados sem o envolvimento da TI chegam a 39% de seu uso de serviços. A TI só tem visibilidade sobre menos da metade (45%) desses aplicativos. A maioria das organizações de serviços financeiros confia principalmente nos firewalls de próxima geração para monitorar o uso de nuvem não aprovado pela TI (59%). Quando um aplicativo de TI oculta não autorizado é detectado, a resposta mais comum é bloquear completamente o acesso ao aplicativo (28%) ou recorrer ao gerenciamento de identidade e acesso (27%) para limitar o acesso. O que surpreende é que, apesar de estarem mais preocupadas do que a média com a proteção dos dados em trânsito pela nuvem pública, essas organizações estão um pouco abaixo da média na utilização de ferramentas de DLP e criptografia. De modo geral, os profissionais de TI de serviços financeiros estão entre os mais preocupados com a TI oculta: 72% deles afirmam que o fenômeno prejudica sua capacidade de manter a segurança na nuvem.

Embora as organizações de serviços financeiros estejam adotando a nuvem pública, 26% continuam usando apenas serviços totalmente privados, enquanto 57% usam uma combinação híbrida de serviços públicos e privados. Na área privada, a porcentagem atual de virtualização de servidores no data center está acima da média global (55% contra 52%) e os profissionais de serviços financeiros afirmam estar adotando os contêineres em sintonia com a média global de 80% das organizações. A maioria (73%) espera concluir a transição para um data center totalmente definido por software dentro de dois anos.

### Conclusões e recomendações

Aparentemente, o setor de serviços financeiros está entre os maiores setores em termos de amadurecimento no uso e na segurança da nuvem. Essas organizações relatam um uso maior da nuvem, porém com menos violações do que as organizações de outros setores.

As nuvens vieram para ficar, e as equipes de operações de segurança do setor de serviços financeiros trabalham para se manter um passo à frente da curva de adoção. A ampla variedade de ofertas de nuvem disponíveis permite que as organizações escolham aquela que é mais adequada, atendendo às necessidades de custo e segurança. Os fornecedores de segurança oferecem as ferramentas necessárias para lidar com questões fundamentais de segurança, como proteção dos dados em trânsito, gerenciamento dos acessos dos usuários e configuração de políticas consistentes entre múltiplos serviços.

As organizações de serviços financeiros têm registros de pagamentos valiosos e há tempos são alvo de criminosos cibernéticos. Os atacantes continuarão procurando pelos alvos mais fáceis, não importando se estão na nuvem pública, privada ou híbrida. Soluções de segurança integradas ou unificadas são uma defesa forte contra essas ameaças, proporcionando às equipes de operações de segurança visibilidade sobre todos os serviços que a organização utiliza e sobre quais conjuntos de dados podem transitar entre eles.

De acordo com o **Relatório de previsões do McAfee Labs sobre ameaças de 2017**, as credenciais de usuários, especialmente de administradores, serão a forma de ataque mais provável. Certifique-se de que sua proteção seja apropriada em todos os endpoints, incluindo tablets e smartphones. As melhores práticas de autenticação, como o uso de senhas diferentes, a autenticação por múltiplos fatores e a biometria (quando disponível), serão essenciais para a criação de estratégias preventivas que reduzam consideravelmente o risco de infecção ou comprometimento.

Apesar da percepção predominante de que a TI oculta está colocando a organização em risco, tecnologias de segurança como prevenção de perda de dados (DLP), criptografia e agentes de segurança de acesso à nuvem (CASBs) continuam subutilizadas. Integrar essas ferramentas ao sistema de segurança existente aumenta a visibilidade, permite a descoberta de serviços ocultos e proporciona opções para proteção automática de dados confidenciais estacionários e em trânsito em qualquer tipo de ambiente.

Embora seja possível terceirizar o trabalho para várias partes, não é possível terceirizar o risco. As organizações precisam evoluir rumo a uma abordagem de mitigação e gerenciamento do risco para conseguir a segurança da informação. Se ainda não tiver feito isso, considere a adoção de uma estratégia de “nuvem em primeiro lugar” para incentivar a adoção de serviços de nuvem, reduzindo os custos e aumentando a flexibilidade, e para colocar as operações de segurança em uma posição proativa em vez de reativa.

Para obter informações mais detalhadas, leia o relatório completo, **Construção de confiança em um céu nebuloso**.



**McAfee. Part of Intel Security.**

Av. das Nações Unidas, 8.501 - 16º andar  
CEP 05425-070 - São Paulo - SP - Brasil  
Telefone: +55 (11) 3711-8200  
Fax: +55 (11) 3711-8286  
www.intelsecurity.com

Intel e os logotipos da Intel e da McAfee são marcas comerciais da Intel Corporation ou da McAfee, Inc. nos EUA e/ou em outros países. Outros nomes e marcas podem ser propriedade de terceiros. Copyright © 2017 Intel Corporation. 2045\_0117  
JANEIRO DE 2017