WHITE PAPER

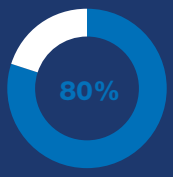
Redefinindo a nuvem e sua segurança

Por Lior Cohen, Diretor Sênior de Produtos e Soluções de Cloud Security da Fortinet.

A migração para plataformas de computação e serviços na nuvem permitiu que as organizações se adaptassem rapidamente à transição global para a economia digital. A capacidade de aplicar rapidamente os recursos, adotar novos aplicativos e responder em tempo real às demandas do usuário final e do consumidor efetivamente mantêm as organizações na concorrência no mercado digital atual. O resultado tem sido surpreendente. Em apenas alguns anos, mais de 80% das empresas adotaram dois ou mais provedores de infraestrutura de nuvem pública e quase dois terços estão usando três ou mais.

Embora as vantagens comerciais sejam significativas, essa migração rápida também traz complexidades e riscos, e poucas organizações estão preparadas adequadamente, neste momento em que é grande a falta de profissionais de cibersegurança, com os cibercriminosos cada vez mais capacitados para explorar vulnerabilidades. O que muitas organizações desconhecem ao migrar para um ambiente na nuvem é até que ponto elas são responsáveis pela proteção do seu próprio ambiente na nuvem. Os provedores de ambientes na nuvem protegem a infraestrutura, como armazenamento e recursos de computação compartilhados por todos, mas a proteção de dados, conteúdos e aplicativos é responsabilidade do cliente da nuvem.

De acordo com a Fortinet, as soluções na nuvem podem ser divididas em três categorias: modelos de implementação, modelos de entrega e provedores de serviços. *Veja o infográfico anexado.*



Em apenas alguns anos, mais de 80% das empresas adotaram dois ou mais provedores de infraestrutura de nuvem pública e quase dois terços estão usando três ou mais.

De acordo com a Fortinet, as soluções na nuvem podem ser divididas em três categorias: modelos de implementação, modelos de entrega e provedores de serviços.

Modelos de implementação

Embora a maioria das pessoas pense apenas em ambientes de nuvem pública ou privada, ou mesmo em modelos híbridos, um novo modelo está começando a surgir: a nuvem comunitária.

Nuvem pública: Neste modelo de implementação, o provedor de ambientes na nuvem é responsável pela criação e manutenção contínua da nuvem pública e de seus recursos de TI, enquanto o consumidor é responsável pela implementação e segurança de dispositivos, aplicativos e dados virtuais.

Nuvem privada: No modelo de nuvem privada, a mesma organização é tanto a provedora quanto a consumidora do ambiente na nuvem. Os ambientes na nuvem privada permitem que uma organização use a tecnologia de computação na nuvem para centralizar o acesso aos recursos de TI, geralmente em uma empresa distribuída geograficamente, e por isso exigem uma mudança na forma como são definidas e aplicadas as fronteiras organizacionais e de confiança.

Nuvem híbrida: Esse modelo de ambiente na nuvem é formado por dois ou mais modelos diferentes de implementação na nuvem. Por exemplo, uma organização pode optar por processar dados confidenciais em sua nuvem privada enquanto distribui outros serviços na nuvem com dados menos sensíveis a uma nuvem pública.

Nuvem comunitária: A nuvem comunitária fornece uma solução de computação na nuvem para um número limitado de indivíduos ou organizações que é administrado, gerenciado e protegido coletivamente por todas as organizações participantes ou por um provedor de serviços gerenciados contratado. O AWS GovCloud é um bom exemplo de nuvem comunitária.

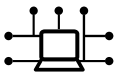
Ambientes de nuvem múltipla trazem novos riscos

Eventualmente, todas as organizações acabarão implementando uma combinação das soluções de nuvem. Porém, a adoção de ambientes de nuvem múltipla não apenas expande a superfície de ataque e dificulta a capacidade de implementar, gerenciar e orquestrar a segurança com visibilidade e controle consistentes, como também aumenta outros riscos, que incluem:

- Roubo de dados.
- Gerenciamento insuficiente de identidade, credenciais e acesso.
- Interfaces e APIs inseguras.
- Vulnerabilidades do sistema.
- Sequestro de conta.
- Mais oportunidades para o pessoal interno malicioso.
- Mais oportunidades para ameaças persistentes avançadas.
- Perda de dados e diligência insuficiente devido a um aumento exponencial na complexidade da rede.
- Sequestro e abuso de serviços na nuvem por cibercriminosos.

No entanto, a resolução desses desafios deve levar em conta outros aspectos. O desempenho não pode ser sacrificado para garantir a segurança. Em vez disso, as organizações precisam encontrar um equilíbrio entre serviços em nuvem onipresentes e sob demanda a criação de controles, políticas e processos consistentes. Isso exige buscar soluções de segurança que ajudem a organização a deixar o modelo de segurança que impede a agilidade dos negócios, migrando para um modelo em que a segurança possa ser combinada com o ambiente na nuvem e a automação para ajudar a realizar os negócios com mais rapidez e segurança.

As organizações precisam implementar soluções de segurança que operem de maneira consistente nos ecossistemas da nuvem. Além disso, devem usar a automação em seus modelos para que a segurança possa ser aplicada de maneira consistente e simultaneamente em todos os ambientes do provedor de serviços na nuvem, principalmente ao compensar as diferenças críticas nos controles nativos. Isso inclui automatizar toda a cadeia de dados para que a segurança possa se adaptar dinamicamente à medida que as cargas de trabalho e as informações se movem dentro e entre diferentes ambientes na nuvem. A nuvem permite essas capacidades.



Modelos de entrega

As organizações têm uma variedade de opções de serviços para implementação, desde a simples adoção de aplicativos ou serviços específicos até a infraestrutura completa.

IaaS: O modelo infraestrutura como serviço fornece um ambiente de TI independente que inclui recursos de infraestrutura que podem ser acessados e gerenciados usando interfaces baseadas na nuvem. Pode incluir hardware, dispositivos de rede, ferramentas de conectividade, sistemas operacionais e outros recursos de TI “brutos”. Esses recursos de TI virtualizados permitem expansão em tempo real e personalização da infraestrutura. Porém, eles não são pré-configurados; desta forma, a equipe de TI é responsável por sua configuração, gerenciamento e segurança.

PaaS: O modelo plataforma como serviço fornece um ambiente “pronto para uso” geralmente composto de recursos de TI pré-configurados usados pelos desenvolvedores para escrever códigos, eliminando a responsabilidade do pessoal de TI de configurar e manter uma infraestrutura não virtualizada de recursos de TI. Porém, a desvantagem é que o cliente tem menos controle sobre os recursos de TI subjacentes.

Saas: O modelo software como serviço disponibiliza aplicativos e outros serviços para uma variedade de clientes na nuvem. Os principais atrativos desses serviços, como Salesforce.com ou DropBox, são a facilidade de uso e a necessidade mínima de desenvolver nada além de interfaces personalizáveis que podem ser facilmente adaptadas às necessidades organizacionais e comerciais específicas. O SaaS geralmente possui escalabilidade dinâmica e acesso onipresente. Porém, o consumidor de serviços na nuvem geralmente tem controle administrativo muito limitado sobre uma implementação no modelo SaaS.

Reformulação da segurança dos ambientes na nuvem

Tudo isso requer uma nova abordagem de segurança. As soluções de segurança legadas serão substituídas por ferramentas de segurança que possam operar de forma nativa e consistente em qualquer ambiente, seja físico ou na nuvem. As soluções que operam de forma nativa em ambientes na nuvem também precisam estar cientes dos recursos baseados na nuvem e utilizar os serviços nativos na nuvem para oferecer suporte melhor à natureza dinâmica e de escala das cargas de trabalho na nuvem. Por fim, as organizações também devem se esforçar para separar totalmente o gerenciamento de segurança da classificação de dados para classificar os recursos de qualquer infraestrutura da maneira mais natural possível, além de aplicar esses objetos ao definir a política de segurança de nuvem múltipla.

A integração nativa de soluções de segurança a serviços baseados na nuvem garante organizações mais seguras. Ao utilizar as informações sobre ameaças e as capacidades de segurança nativas de todas as nuvens e integrá-los à estrutura de segurança da nuvem múltipla, as organizações podem transformar o efeito de multiplicação de riscos em efeito de multiplicação de segurança. A capacidade de automatizar as operações de segurança com base nos aspectos de integração nativa e inteligência de ameaças permite que as organizações coordenem automaticamente suas respostas a ameaças, incluindo o isolamento de dispositivos infectados e a identificação e desativação de malware, estendendo a proteção para todo o ambiente da nuvem múltipla, reduzindo significativamente os riscos e implementando com confiança aplicativos em qualquer lugar exigido pelos negócios.

Provedores de serviços:

Uma variedade de prestadores de serviços também está disponível. Cada um inclui seus próprios controles e mercados nativos para a compra de tecnologias e serviços – próprios ou de um fornecedor contratado – e diferentes ambientes oferecem vantagens distintas aos clientes, como compatibilidade com infraestruturas existentes ou objetivos comerciais.

Principais provedores: Os principais provedores de nuvem incluem: Amazon AWS, Microsoft Azure, Google CloudPlatform, Oracle Cloud, IBM Cloud e Alibaba Cloud. O desafio de muitas organizações que usam múltiplos provedores é estabelecer políticas e controles consistentes em diferentes ambientes. O uso de fornecedores de soluções de segurança que podem operar de maneira nativa em todas as principais plataformas de nuvem oferece flexibilidade máxima em termos de adoção e controle.

Provedores menores: AAlém dos principais provedores, um número crescente de fornecedores de serviços na nuvem de menor porte, empresas de telecomunicações regionais e parceiros (para ambientes na nuvem comunitária) estão ingressando no mercado. Eles normalmente fornecem mais flexibilidade no preço e atenção mais personalizada.

479565-0-0-PT