Proteja sua nuvem:

práticas recomendadas para garantir a segurança de aplicativos essenciais

WHITE PAPER

Índice

Para muitas organizações, a migração de data centers tradicionais locais para plataformas de nuvem pública está em sua reta final, e a conclusão pode estar a apenas alguns anos de distância. Até 2027, a Gartner prevê que 90% das organizações manterão pelo menos alguns de seus aplicativos em nuvens públicas[1]. No ano seguinte, a computação na nuvem terá completado sua transição de tecnologia disruptiva para necessidade empresarial[2]; e por um bom motivo.

Os ambientes na nuvem permitem que as organizações expandam rapidamente seus recursos, implementem novos serviços e reduzam os custos de infraestrutura em comparação com as configurações locais tradicionais. Ao priorizar a adoção da nuvem para cargas de trabalho essenciais, as empresas podem se adaptar, inovar e prosperar rapidamente no cenário dinâmico atual.

Mas novas oportunidades também trazem maiores riscos.

Na corrida para migrar para a nuvem, algumas organizações priorizaram a rápida transformação digital em detrimento das práticas de segurança recomendadas, deixando-as vulneráveis. Consequentemente, os ciberataques veem os alvos baseados na nuvem como caminhos potencialmente fáceis para ganhos substanciais e estão aprimorando suas táticas para explorar essas vulnerabilidades.

No atual cenário híbrido e multinuvem, as organizações têm mais liberdade do que nunca para criar e implantar soluções onde e quando quiserem. Mas isso se contrapõe à preocupação generalizada com a segurança das nuvens públicas, sinalizando a necessidade de adotar melhores ferramentas e práticas de segurança.

Para lidar com esse cenário cada vez mais complexo, as empresas estão recorrendo ao zero trust, uma estrutura de segurança moderna e nativa da nuvem que garante que somente usuários e dispositivos autorizados tenham acesso a recursos críticos na nuvem. Com uma estratégia de segurança na nuvem bem projetada, as organizações podem avançar significativamente na prevenção de violações, no aprimoramento da conformidade e no fortalecimento da confiança dos clientes.

À medida que as organizações movem seus aplicativos críticos para a nuvem, é crucial repensar suas estratégias de segurança, principalmente com relação à governança de dados e conformidade sob o microscópio regulatório.

Este documento técnico destaca os principais riscos que os líderes de TI e as equipes de segurança na nuvem enfrentam ao proteger as transformações na nuvem. Também examinaremos mais de perto as estratégias comprovadas e as práticas recomendadas que as empresas estão usando para proteger aplicativos essenciais em ambientes de nuvem pública.

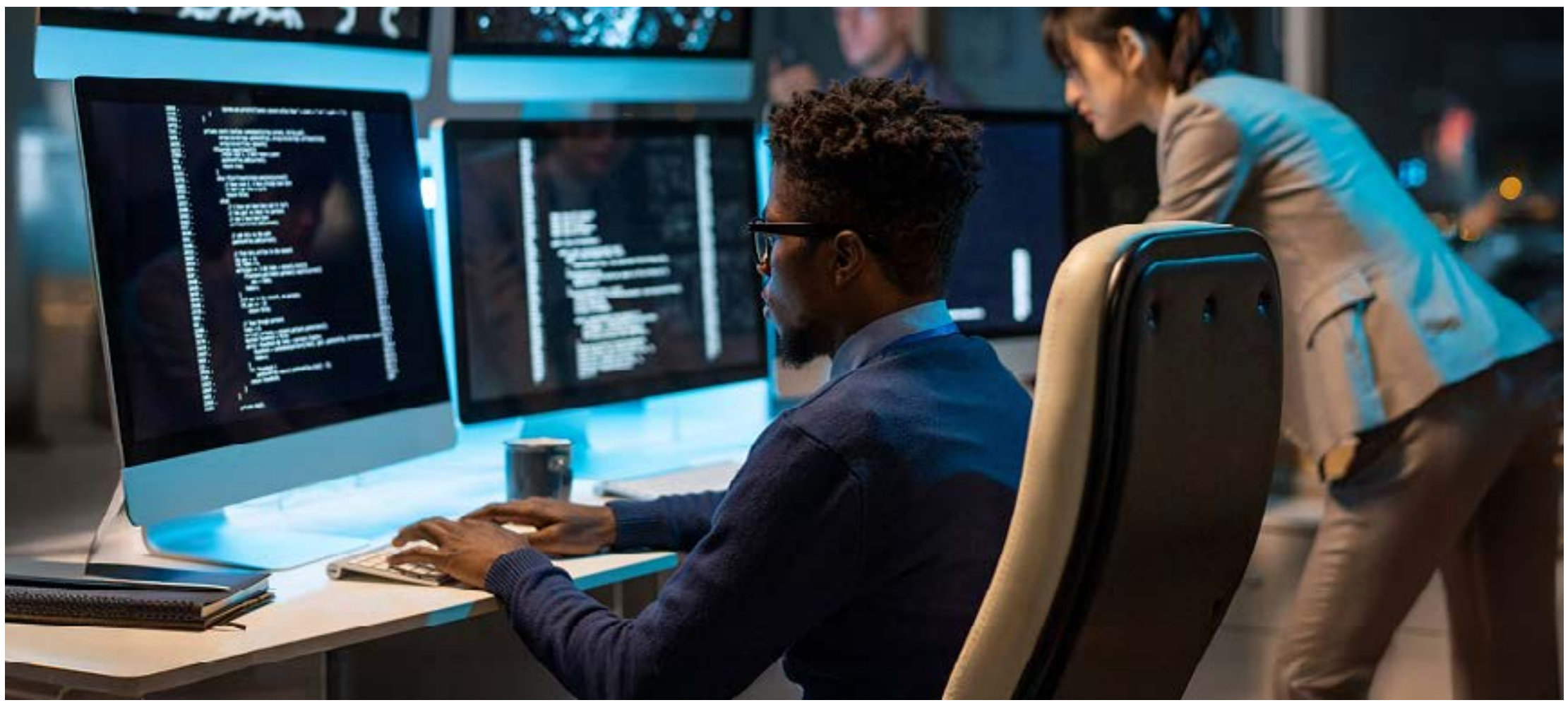
O que acontece quando os aplicativos migram para a nuvem pública?

Quando os aplicativos migram para a nuvem pública, eles trocam suas antigas casas físicas por apartamentos modernos e elegantes em uma metrópole movimentada. Veja o que acontece nessa transição emocionante, porém complexa:

- **Do monólito aos microsserviços:** em vez de um grande aplicativo, pense em uma coleção de serviços menores e independentes, ou microsserviços. Cada microsserviço é projetado para executar funções específicas e pode ser desenvolvido, implantado e expandido de forma independente.

- **APIs interativas:** os aplicativos nativos da nuvem usam APIs para se comunicar, criando um ambiente altamente interativo onde os serviços interagem constantemente. Embora aumentem a flexibilidade e a capacidade de dimensionamento, as APIs também aumentam a vulnerabilidade a ameaças de segurança.

- **Cargas de trabalho em trânsito:** os aplicativos não estão mais confinados a uma única sala de servidores, mas espalhados por diferentes ambientes na nuvem em várias regiões, zonas de disponibilidade e configurações híbridas.



A importância de proteger aplicativos essenciais na nuvem

Aplicativos essenciais são a força vital de qualquer empresa, o coração pulsante que sustenta as operações comerciais. Esses aplicativos vitais, que podem incluir sistemas de transações financeiras, plataformas de assistência médica, automação industrial e sistemas de planejamento de recursos empresariais (ERP), exigem disponibilidade inabalável, processamento instantâneo em tempo real e conformidade regulatória rigorosa.

O problema é que qualquer interrupção pode levar a danos comerciais, financeiros e de reputação significativos.

Portanto, embora a migração de aplicativos essenciais para a nuvem tenha os seus benefícios, como capacidade de dimensionamento, agilidade e economia de custos, para citar alguns, ela também apresenta uma série de desvantagens potenciais, como:

- **Maior exposição a ameaças cibernéticas:** aplicativos que processam dados altamente sigilosos são os principais alvos de invasores que buscam explorar vulnerabilidades.
- **Complexidade operacional:** a mudança para ambientes multinuvem introduz arquiteturas distribuídas, comunicação orientada por API e cargas de trabalho dinâmicas, o que aumenta a superfície de ataque.
- **Desafios de conformidade regulatória:** empresas que operam em setores como saúde, finanças e governo devem aderir a estruturas de conformidade rigorosas, como HIPAA, GDPR e PCI DSS, tornando a governança da segurança na nuvem crítica. Em vez de um grande aplicativo, pense em um conjunto de serviços menores e independentes, ou microsserviços. Cada microsserviço é projetado para executar funções específicas e pode ser desenvolvido, implantado e dimensionado de forma independente.

40%

DAS VIOLAÇÕES DE DADOS ENVOLVERAM DADOS ARMAZENADOS EM VÁRIOS AMBIENTES.[3]

Não é de se surpreender que as arquiteturas legadas simplesmente não consigam lidar com a tarefa de proteger cargas de trabalho essenciais na nuvem. Isso acontece porque...

1. As soluções de segurança legadas, como firewalls, VPNs e defesas baseadas em perímetro, foram criadas para ambientes estáticos locais e não têm a flexibilidade necessária para proteger cargas de trabalho de nuvem altamente dinâmicas.
2. A segurança tradicional baseada em rede não fornece controles granulares no nível dos aplicativos, deixando brechas na proteção de arquiteturas baseadas em microsserviços e orientadas por API.
3. Os modelos de acesso legados dependem da confiança implícita, o que os torna vulneráveis a ataques baseados em credenciais, ameaças de movimentação lateral e riscos internos.

E NO MUNDO DE ALTO RISCO DOS APLICATIVOS ESSENCIAIS, UMA ÚNICA FALHA DE SEGURANÇA PODE DESENCADEAR UMA CASCATA DEVASTADORA DE CONSEQUÊNCIAS.

O tempo de inatividade pode:

- Paralisar ooperações
- Drenar receitas
- Corroer a confiança do cliente

Violações de dados expõem dados sigilosos que levam a:

- Multas regulatórias
- Batalhas jurídicas
- Danos irreparáveis à reputação

US$ 5,17 M

CUSTO MÉDIO DE DADOS VIOLADOS ARMAZENADOS EM NUVENS PÚBLICAS.[4]

Desafios na proteção de aplicativos essenciais

O modelo de responsabilidade compartilhada e suas armadilhas

Nos últimos anos, a nuvem evoluiu de uma tecnologia emergente para uma estrutura indispensável para as empresas modernas. É importante reconhecer que a nuvem, no entanto, não é inerentemente segura. Na verdade, a segurança na nuvem opera como uma responsabilidade compartilhada entre o cliente e o provedor de nuvem. Pense nisso como morar em um prédio onde o proprietário mantém a estrutura, mas você é responsável por proteger seu apartamento e pertences.

Nesse modelo de responsabilidade compartilhada, os provedores de nuvem protegem a infraestrutura da nuvem subjacente, enquanto os clientes são responsáveis por proteger suas cargas de trabalho, aplicativos e dados. Não é incomum interpretar mal esse modelo e presumir erroneamente que os provedores de nuvem protegem totalmente as cargas de trabalho dos clientes. Isso pode resultar em:

- **Buckets de armazenamento expostos,** armazenamento em nuvem mal configurado que leva a dados sigilosos acessíveis publicamente.
- **Controles de identidade e acesso fracos,** funções de IAM excessivamente permissivas, oferecendo acesso não autorizado a aplicativos essenciais.
- **Falhas de conformidade,** falta de monitoramento e fiscalização contínuos, levando a penalidades regulatórias.

Os principais desafios de segurança na proteção de aplicativos essenciais

Além das potenciais armadilhas do modelo de responsabilidade compartilhada, as empresas enfrentam riscos adicionais ao proteger cargas de trabalho essenciais na nuvem. Esses riscos variam de:

- **Movimentação lateral não autorizada:** modelos de segurança legados, como firewalls, VPNs e defesas baseadas em perímetro, têm dificuldade para proteger ambientes de nuvem dinâmicos, aumentando o risco de acessos não autorizados e movimentação lateral.
- **Brechas de visibilidade:** manter políticas de segurança consistentes em ambientes híbridos e multinuvem é difícil, o que leva a posturas de segurança fragmentadas e brechas na visibilidade.
- **Padronização de políticas deficiente:** a complexidade de várias nuvens cria riscos adicionais, pois diferentes provedores de nuvem têm estruturas de segurança inconsistentes, dificultando a padronização de políticas.
- **Falta de segmentação:** a deficiência de proteção de dados integrada e segmentação permitem que os invasores se espalhem por ambientes na nuvem em busca de um único ponto de comprometimento.

79%

ORGANIZAÇÕES QUE CITAM A SEGURANÇA NA NUVEM COMO UM DOS PRINCIPAIS DESAFIOS.[5]

5 práticas recomendadas para proteger aplicativos essenciais na nuvem

Para proteger efetivamente aplicativos essenciais na nuvem, quais estratégias as empresas devem incluir em seu kit de ferramentas de segurança? Por não ser automaticamente impenetrável, isso requer planejamento estratégico e defesas robustas.

Pense nas cinco práticas recomendadas como a base da sua estratégia de segurança na nuvem, cada uma desempenhando um papel vital na proteção dos seus ativos baseados na nuvem e na manutenção da conformidade.

1 Implemente o acesso de privilégio mínimo com base em identidade e autenticação

- Adote controles de acesso zero trust para garantir que somente usuários, dispositivos e cargas de trabalho autorizados possam se comunicar com aplicativos essenciais.
- Oculte seus aplicativos não publicando endereços IP. O que está oculto não pode ser atacado por agentes maliciosos.
- Monitore e adapte continuamente as políticas de acesso com base no comportamento dos usuários e na análise de risco em tempo real.

2 Proteja aplicativos, não redes

- Abandone a segurança tradicional baseada em rede conectando aplicativos em vez de redes inteiras, eliminando a necessidade de backhauls, firewalls e VPNs.
- Adote soluções de segurança disponibilizadas na nuvem que protejam cargas de trabalho no nível dos aplicativos, garantindo conectividade direta e segura sem expor a rede em geral.
- Utilize o acesso à rede zero trust (ZTNA) para fornecer acesso granular e seguro a aplicativos sem
- aumentar a superfície de ataque.

3 Implante proteção integrada contra ameaças e inspeção de segurança em tempo real

- Implemente proteção avançada contra ameaças, incluindo detecção de invasão, análise comportamental e detecção de anomalias com tecnologia de IA para identificar e mitigar ameaças cibernéticas.
- Use soluções de proteção de dados que forneçam criptografia de ponta a ponta, prevenção contra perda de dados (DLP) e
- monitoramento contínuo.
- Utilize uma plataforma de segurança disponibilizada na nuvem capaz de inspecionar ameaças em tempo real e em larga escala para detectar atividades maliciosas antes que elas afetem os aplicativos essenciais.

4 Aplique segmentação de cargas de trabalho para evitar a movimentação lateral

- Aplique a microssegmentação para isolar cargas de trabalho, limitar o tráfego leste–oeste e impedir que invasores se movam lateralmente pelos ambientes de nuvem.
- Garanta a segmentação em várias camadas da nuvem, incluindo:

A. **Segmentação em nível de processo:** restrinja a comunicação entre cargas de trabalho dentro de um host.

B. **Segmentação de VPC e zona de disponibilidade:** limite o acesso entre diferentes ambientes de nuvem para minimizar a exposição.

C. **Segmentação multinuvem:** aplique políticas de segurança uniformes em infraestruturas da AWS, Azure, Google Cloud e híbridas.

5 Utilize a aplicação automatizada para garantir a conformidade regulatória

- Alinhe as estratégias de segurança na nuvem com regulamentações específicas do setor, como HIPAA, GDPR, PCI DSS e NIST.
- Use a aplicação automatizada de políticas e auditoria de conformidade para garantir a adesão contínua às estruturas de segurança.

Como a Zscaler ajuda as empresas a proteger aplicativos essenciais

A Zscaler é uma aliada poderosa para empresas que buscam proteger seus aplicativos essenciais. Com sua plataforma Zero Trust Exchange™ nativa da nuvem, a Zscaler oferece conectividade direta e segura entre cargas de trabalho, efetivamente eliminando a necessidade das tradicionais VPNs, firewalls e práticas de retorno de tráfego, mantendo os aplicativos protegidos contra as ameaças da internet. Ao inspecionar continuamente o tráfego, detectar ameaças e aplicar políticas em ambientes híbridos e multinuvem, a Zscaler garante visibilidade em tempo real e proteção robusta para cargas de trabalho na nuvem.

- **Uma plataforma Zero Trust Exchange™** totalmente nativa da nuvem oferece conectividade direta e segura entre cargas de trabalho sem explor aplicativos à internet ou depender de VPNs, firewalls ou retorno do tráfego.

- **A visibilidade e a proteção em tempo real para cargas de trabalho na nuvem** inspecionam continuamente o tráfego, detectam ameaças e aplicam políticas em ambientes híbridos e multinuvem.

- **A aplicação automatizada de políticas para acesso seguro e em conformidade a aplicativos** garante políticas de segurança consistentes para aplicativos, reduzindo o risco de configurações incorretas e violações de conformidade.

Validando o impacto do Zscaler: insights da análise de produto do SANS

Uma análise de produto feita pelo instituto SANS fornece uma validação profissional das capacidades da Zscaler na proteção de aplicativos essenciais[6]. Veja a seguir um detalhamento das principais áreas em que a Zscaler se destaca, de acordo com a análise:

- **Modelo zero trust:** a Zscaler elimina superfícies de ataque conectando cargas de trabalho diretamente, reduzindo a exposição e os riscos. Essa abordagem garante que as cargas de trabalho sejam menos detectáveis e reduz os riscos de exploração.

- **Prevenção de movimentação lateral:** a Zscaler aplica microssegmentação e políticas baseadas em identidade em cargas de trabalho na nuvem, mitigando a movimentação lateral por meio da segmentação de aplicativo para aplicativo.

- **Mitigação de ameaças reais:** inspeção de tráfego em tempo real, monitoramento contínuo e análises de segurança orientadas por IA atenuam ameaças de forma eficaz, com proteção de dados por meio de DLP e SSL em larga escala.

- **Monitoramento e controle abrangentes:** a plataforma Cloud Connector da Zscaler monitora e controla o acesso a aplicativos e serviços na nuvem, gerencia o fluxo de dados e avalia a postura de segurança dos aplicativos.

- **Interface intuitiva:** a interface e o mecanismo de políticas são fáceis de usar, simplificando a configuração e o gerenciamento de políticas de segurança.

Em resumo, a análise do SANS confirma que o modelo de segurança nativo da nuvem da Zscaler é líder do setor, ajudando empresas globais como Siemens, Micron e Mahindra Group a proteger seus aplicativos mais essenciais, atender aos requisitos de conformidade e simplificar a complexidade da segurança multinuvem.

Obtenha segurança abrangente na nuvem

À medida que as empresas migram aplicativos essenciais para a nuvem, elas enfrentam riscos de segurança significativos que exigem atenção imediata. Mas as estratégias certas podem abrir caminho para operações seguras e eficientes.

Uma arquitetura zero trust moderna permite que as organizações conectem aplicativos com segurança em qualquer lugar para minimizar a superfície de ataque, evitar a movimentação lateral e reduzir os riscos de agentes mal-intencionados obterem acesso aos seus dados. Isso posiciona as empresas para navegar com confiança pelas complexidades da segurança na nuvem e obter proteção abrangente de seus ativos mais valiosos.

Dê o próximo passo para garantir a segurança e a integridade dos seus ativos baseados na nuvem. Solicite uma demonstração para ver em primeira mão como você pode simplificar radicalmente a proteção de cargas de trabalho na nuvem.

SOLICITE UMA DEMONSTRAÇÃO

Ou faça seu próprio teste da Zero Trust Cloud em nosso laboratório autoguiado.

VEJA O GUIA

[1] Gartner prevê que os gastos globais dos usuários finais da nuvem pública chegarão a US$ 723 bilhões em 2025

[2] Gartner afirma que a nuvem se tornará uma necessidade empresarial até 2028

[3] Relatório de custo de violação de dados da IBM, 2024

[4] Relatório de custo de violação de dados da IBM, 2024

[5] Relatório Flexera de 2023 sobre o estado da nuvem

[6] Como usar zero trust para proteger cargas de trabalho na nuvem pública, SANS, 2023

Sobre a Zscaler

A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A Zscaler Zero Trust Exchange™ protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange™ baseada em SSE é a maior plataforma integrada de segurança na nuvem do mundo. Saiba mais em **zscaler.com/br** ou siga-nos no Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/br**

zscaler™

Zero Trust Everywhere