O Guia Empresarial para os Fundamentos da Segurança na Nuvem

Forcepoint

Folheto

Sumário:

Visão Geral do Cenário: Segurança na Nuvem e Migração para a Nuvem

Se você tem a impressão de que a nuvem está cada vez mais em todo lugar, tem razão. Mas o que está impulsionando essa aceleração rápida e furiosa de tudo o que se refere à nuvem? Na verdade, é o consumismo. Sim, o tipo B2C.

A forma como as pessoas consomem a nuvem todos os dias impulsiona a forma como as empresas adotam e protegem a nuvem.

A segurança na nuvem é impulsionada pelas pessoas.

A nuvem é acesso instantâneo.

E a nuvem é uma expectativa.

Com acesso constante a conteúdo, aplicativos, dispositivos—todos interconectados de forma transparente, o tempo todo, sem interrupção—a nuvem é uma parte inseparável de nossas vidas diárias. Profundamente costurada no tecido de como a pessoa moderna inconscientemente funciona e opera. Portanto, no local de trabalho, a expectativa é a mesma. Você quer usar o que precisa, quando precisa. E quer uma experiência fluida, que não prejudique a sua produtividade e a estimule. Como se pode aumentar a produtividade com a nuvem? Como fazer mais com menos? Porque, na verdade, a nuvem é conveniência. Mas também é uma vulnerabilidade.

Em última instância, os trabalhadores são consumidores. Como as empresas protegem suas organizações, protegendo seus dados e suas pessoas, precisa corresponder à mesma expectativa e experiência que temos todos os dias em nossa rotina. E a segurança precisa evoluir para permitir essa fluidez, protegendo também o cenário de ameaças em expansão constante que acompanha essa liberdade e conveniência.

Essa é a cultura geral da nuvem. Mas quais são as circunstâncias específicas que estimulam a ação e impulsionam as organizações a repensar essa abordagem para a nuvem e a segurança como um todo? Elas incluem:

- A jornada da transformação digital, começando com adoção e implementação do O365
- Migração de aplicativos legados e personalizados para a nuvem, como sistemas EHR ou ERP
- Pessoas trabalhando além dos limites de um escritório, fora da rede corporativa ou atrás de outras defesas
- Empresas globais operando em ambientes altamente distribuídos, abrangendo sites que precisam do mesmo nível de segurança da sede—sem a necessidade de recriar um footprint caro e intensivo em hardware em cada local com tráfego em backhaul
- Esforços de otimização—seja consolidando pilhas de segurança, dinamizando fluxos de trabalho de equipes ou simplesmente reduzindo CapEx/OpEx
- Migração da infraestrutura para nuvens públicas, como AWS ou Azure

O Caminho Certo para a Nuvem

Segurança na nuvem significa coisas diferentes para pessoas diferentes. E muda constantemente e rápido. Como acompanhar? Como garantir que sua abordagem seja holística e eficaz? Para proteger a sua organização com eficácia, a segurança na nuvem precisa ser inclusiva.

Vamos pensar nos principais componentes da nuvem:

Dados na nuvem | **Usuários** na nuvem | **Apps** na nuvem | **Conectividade** na nuvem | **Infraestrutura** na nuvem | **Segurança** na nuvem

Na essência, é o que constitui a segurança na nuvem. E todos os componentes da nuvem precisam ser considerados, administrados e protegidos para evitar falhas de segurança, e manter os usuários e os dados seguros. Embora a segurança na nuvem não tenha uma definição estática, há um caminho certo para a "nuvem."

E como é?

Para proteger e conectar a nuvem, as organizações devem:

- Proteger o acesso ao conteúdo da web e aos aplicativos na nuvem para qualquer usuário, em qualquer lugar e em qualquer dispositivo
- Ter visibilidade e controle na organização para impulsionar a estratégia de segurança na nuvem
- Proteger os dados que trafegam na nuvem
- Habilitar conectividade direta com a nuvem para usuários e sites sem backhauling
- Otimizar infraestrutura e fluxo de trabalho
- Proteger contra ameaças avançadas, incluindo exploits de dia zero

Excelente, agora que você sabe o que fazer, como isso é concretizado? Muitas organizações podem ter produtos existentes para algumas capacidades essenciais, ou utilizam diferentes equipes que são responsáveis por determinados elementos da segurança na nuvem. Mas o que toda organização de segurança quer evitar é sobrecarregar ainda mais suas equipes de segurança, implementando produtos pontuais múltiplos, que não são integrados e não conversam entre si. O que as organizações realmente precisam é de uma solução singular—e não uma colcha de retalhos de produtos de vários fornecedores. Sim, existem dependências—como a necessidade de ter visibilidade para ter controle, ou a necessidade de migrar a segurança web local para a nuvem a fim de proteger os usuários fora da rede. Em seu estado ótimo, a segurança na nuvem é uma solução unificada, que envolve dados, acesso à web, acesso à nuvem e aos dados na nuvem, e conectividade. Tem a função de aliviar todos e quaisquer pontos de dificuldade para a sua equipe de segurança e evitar falhas de segurança. Não importa se isso é alcançado com um fornecedor ou três, as empresas devem garantir que o que têm, o que querem e onde querem estar estejam alinhados para alcançar os resultados de negócios principais.

Abordando Preocupações sobre a Nuvem

Migrar os dados para a nuvem é um empreendimento significativo—e se você sente alguma ansiedade com isso, não está sozinho. Como manter propriedade e controle? Como continuar a manter as ameaças à distância? Como garantir o desempenho?

Vamos solucionar alguns dos pontos mais comuns em questão.

Latência

A cobertura é crítica para reduzir a latência. Um footprint expansivo com PoPs abundantes no mundo inteiro fornecerá baixa latência e outros benefícios que impulsionam a produtividade, como localização do conteúdo. **Redes Tier 1 e datacenters Tier 4** ajudam a garantir um alto nível de alcance, redundância, conectividade e qualidade, ideal para aplicações sensíveis à latência.

Visibilidade

Você não pode proteger o que não consegue ver. E não pode fazer mudanças ou definir políticas sem saber o que afetarão. Emparelhar um **gateway da web entregue na nuvem** com um **firewall** oferece visibilidade e aplicação consistentes para usuários e locais, incluindo aplicação de políticas e controle de TI sombra. E a funcionalidade **CASB** ajuda a proteger as empresas, fornecendo visibilidade sobre o que usuários de apps aprovados e não aprovados estão fazendo na nuvem, para entender os riscos e proteger usuários e dados.

Conformidade

Confie em certificações de programas—e não apenas uma conformidade auditada por conta própria. Os padrões relevantes para a sua organização provavelmente incluem:

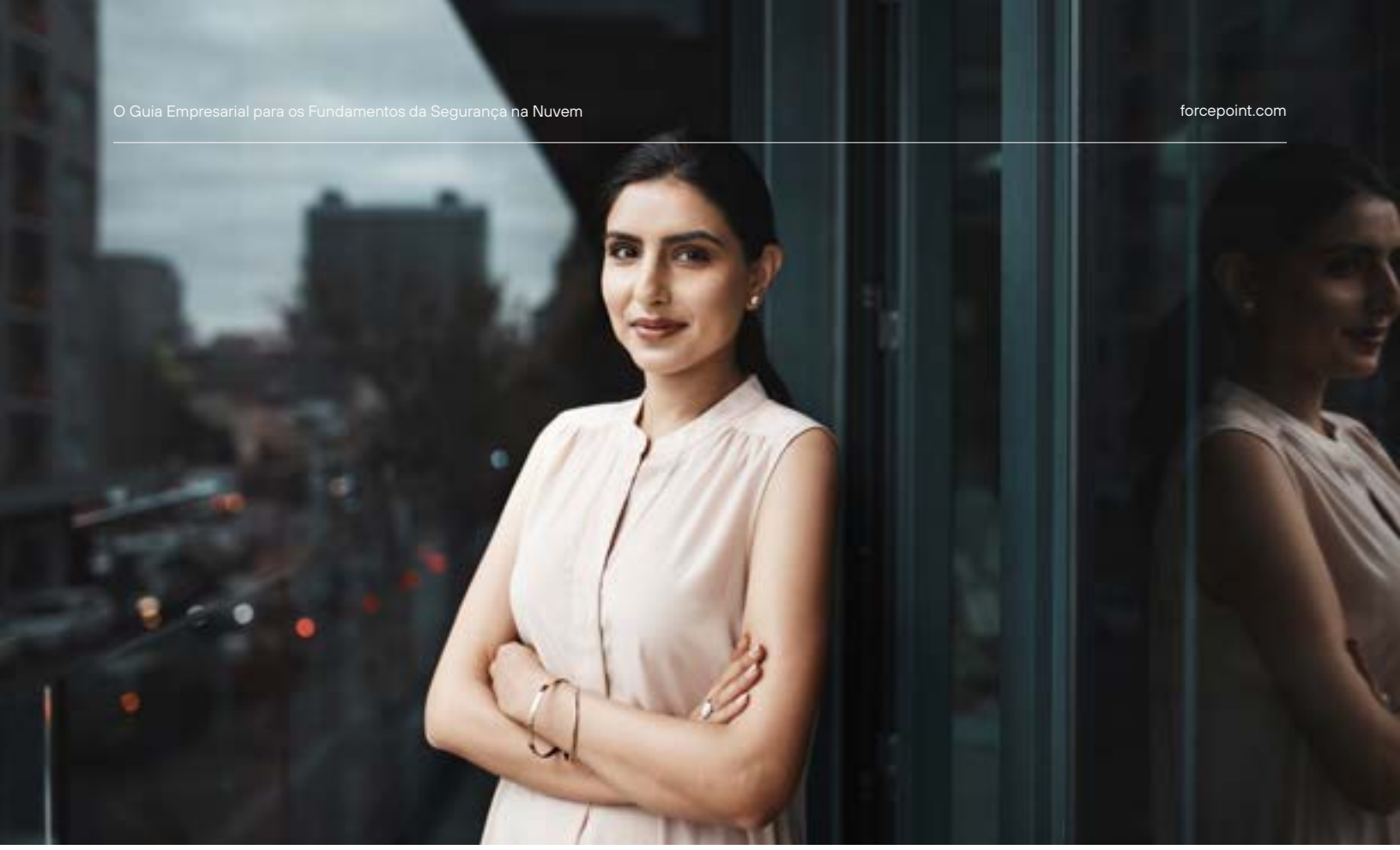
- **ISO 27018**, que rege informações de identificação pessoal (PII, Personally Identifiable Information)
- **ISO 27001**, uma certificação multisites para desenvolvimento, garantia da qualidade, implementação e operações de suporte
- **CSA**, que rege segurança de software e operações multifuncionais em um ambiente de nuvem (e se baseia no Código de Conduta do Regulamento Geral sobre Proteção de Dados da UE)
- **SOC2**, com foco em controles de relatórios não financeiros relacionados a segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade, em acréscimo a testes de datacenter e eficácia operacional

Soberania dos Dados

Embora a nuvem em si não tenha limites concretos, não está isenta das consequências jurídicas de fronteiras e limites geográficos. Os dados digitais estão sujeitos às leis em que esses dados residem. Usar **datacenters em nuvem localizados nas regiões onde a sua empresa opera** é essencial para conformidade com as leis e regulamentos locais, e também desempenho.

Perda de Dados

Uma abordagem unificada tem mais êxito. Com **soluções de proteção de dados** integradas, você pode ampliar suas medidas de segurança do local para web, e-mail, endpoints, rede e nuvem. Alavancar as suas políticas existentes para proteger dados armazenados na nuvem e dados em trânsito.



BYOD

A força de trabalho atual usa muitos aplicativos de nuvem aprovados e não aprovados, em dispositivos administrados e não administrados. Ao proteger usuários remotos e em roaming, as defesas de perímetro de rede e a proteção de endpoints não os proíbem. Você deve diferenciar entre dispositivos administrados e BYOD, usando **políticas de segurança granulares** para fornecer aos funcionários a flexibilidade para usar seus próprios dispositivos sem risco adicional. **Controles expandidos** oferecem segurança para usuários remotos que usam dispositivos da empresa para trabalho e uso pessoal.

Aceitando o Mínimo Necessário

Com pressa para ser mais ágeis, eficientes, etc., as empresas com frequência adotam uma abordagem de "decidir depois" em relação à nuvem. Mas implementar sem pensar com frequência sacrifica segurança e eficácia. Por exemplo, sozinha, a filtragem de URLs não é segurança—assim como uma solução de DNS recursivo não substitui um gateway da web completo. Você não pode obter proteção completa com apenas um elemento de uma solução. Além disso, a abordagem do mínimo coloca a segurança em uma posição de precisar reagir, em vez de ser proativa. Garanta que **segurança e redes funcionem juntas e tenham um lugar à mesa** quando a sua empresa cria o roadmap para a transformação digital—assim, trabalhamos em harmonia com os objetivos de negócios e podemos evitar ter que correr atrás.

Alcançando o Sucesso em um Mundo Conectado na Nuvem

No início, definimos que a segurança na nuvem é impulsionada pelas pessoas. É por isso que precisa ser centrada nas pessoas.

Graças à nuvem, **as pessoas são o novo perímetro.**

À medida que usuários, parceiros e clientes acessam os dados de sua empresa em qualquer lugar do mundo, a muralha artificial que protege os dados não é mais suficiente.

A segurança legada e centrada em infraestrutura que agrupa usuários confiáveis dentro e pessoas não confiáveis fora não é mais relevante.

A confiança inerente não pode ser parte de sua pilha de segurança.

E a sua pilha de segurança é integral—e não acessória—à sua transformação digital.

Para acelerá-la e protegê-la, estes são alguns princípios essenciais para ter em mente:

A nuvem no seu ritmo
Roma não foi construída em um dia. E a sua migração para a nuvem não vai ocorrer de um dia para o outro. A maioria das empresas estão operando em ambientes de TI híbrida/multinuvem—e continuarão assim no futuro previsível. Garanta que seu gateway de web segura tenha opções de implementação flexíveis que habilitem migração com base no que é certo para a sua organização hoje e no futuro. Isso permitirá que você migre em seus próprios termos, quando estiver pronto, mantendo a segurança em todos os níveis.

Estenda os seus limites
Proteja sua nuvem, rede e endpoints para satisfazer as suas necessidades de negócios em mudanças constantes. Uma plataforma convergente, com pouco uso de hardware e recursos de segurança modulares, oferece às organizações altamente distribuídas a extensibilidade e a agilidade de que precisam para aproveitar novos avanços, prevenir pontos cegos e conectar locais—de forma segura e administrável.

Zero Trust, Insight Total
"Nunca confie, sempre verifique" é um princípio essencial da estrutura de Zero Trust—o que significa que a forma como você protege os dados da sua organização é avaliando o acesso aos dados na interação entre usuário e dispositivo. Isso ajuda a entender "quem" e "como". E entender "por quê" ajudará você a ir além da consciência e chegar à prevenção. Utilize análises comportamentais para entender a intenção.

Está pronto para o futuro na jornada para a segurança na nuvem dimensionável?

› Confira o nosso e-book, Protegendo a sua Força de Trabalho em Qualquer Lugar, Sempre.

Forcepoint

forcepoint.com/contact

Sobre a Forcepoint

A Forcepoint é líder em cibersegurança para proteção de usuários e dados, com a missão de proteger as organizações ao impulsionar transformação digital e crescimento. As soluções da Forcepoint adaptam-se em tempo real a como as pessoas interagem com dados, fornecendo acesso seguro e habilitando os funcionários a criar valor. Com sede em Austin, Texas, a Forcepoint cria ambientes seguros e confiáveis para milhares de clientes no mundo inteiro.