INFRAESTRUTURA DE APLICATIVOS SEGURA

Aplicação de modelos inovadores para transformar a segurança

Ameaças em evolução exigem novos modelos de segurança

Nos últimos anos, empresas de todos os setores têm enfrentado diversas violações de dados sofisticadas que comprometem informações sensíveis, custando às organizações bilhões de dólares e causando danos imensuráveis às marcas. Apesar da variação dos métodos específicos, a maioria das violações adotou uma estratégia comum que expõe o ponto fraco fundamental do modelo de segurança de rede centrado no perímetro. Normalmente, as organizações se dedicavam a proteger o data center com firewalls de perímetro. Entretanto, as ameaças modernas estão cada vez mais se infiltrando na segurança de perímetro e depois se proliferando lateralmente, de servidor para servidor (leste-oeste).

Para tentar resolver esse problema, muitas organizações implantaram um array de produtos unitarefa, criando uma rede de sistemas complexa e desconectada. Essas soluções ad hoc são inflexíveis, difíceis de aprovisionar e não se alinham aos aplicativos que devem proteger. Ao mesmo tempo, os invasores estão cada vez mais sofisticados, e as ferramentas disponíveis a eles também estão mais avançadas e fáceis de usar, permitindo que um conjunto maior de agentes realizem ataques maliciosos.

AMEAÇAS DE SEGURANÇA SÃO UM ASSUNTO SÉRIO

- O crime cibernético representa a causa de maior crescimento das interrupções de data centers, tendo aumentado de 2% em 2010 para 22% em 2016.[1]
- O custo da espionagem cibernética global é de aproximadamente 500 bilhões de dólares por ano, atingindo um trilhão de dólares se forem incluídos os custos associados ao roubo de propriedade intelectual.[2]
- O custo médio de uma violação de dados subiu para quatro milhões de dólares em 2016, ou 158 dólares por registro perdido ou roubado.[3]

As empresas precisam de agilidade para impulsionar o crescimento

À medida que as organizações procuram acelerar o tempo de colocação no mercado e o retorno de valor das linhas de negócios e de outras partes interessadas internas, elas também precisam controlar a segurança e gerenciar o risco de forma mais eficaz. É mais importante do que nunca que as empresas não só reduzam o risco de uma violação de dados, mas também o impacto no caso de ocorrer algum problema. Entretanto, a segurança e a conformidade podem afetar a agilidade comercial. As equipes de TI nem sempre têm as ferramentas e os recursos necessários para acompanhar o ritmo das operações comerciais mantendo a segurança da infraestrutura.

A TI precisa de segurança e agilidade

Para atender às expectativas dos líderes de negócios, as organizações de TI precisam fornecer os serviços e aplicativos necessários rapidamente, mas com segurança. No entanto, à medida que se esforçam para proteger o negócio, as equipes de TI enfrentam inúmeros obstáculos, incluindo:

- Mudança das arquiteturas dos aplicativos, desde os monolíticos no local até os aplicativos e microsserviços distribuídos
- Falta de visibilidade e contexto do tráfego de rede
- Políticas e modelos de segurança rígidos e centrados no perímetro
- Dificuldade em cumprir, manter e demonstrar conformidade

[1] Cost of Data Center Outages, Ponemon Institute, janeiro de 2016

[2] https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/

[3] 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, junho de 2016

A abstração de aplicativos da infraestrutura oferece vantagens

Para enfrentar esses problemas, as organizações precisam transformar fundamentalmente a maneira como protegem a infraestrutura de aplicativos. A VMware oferece um portfólio completo de soluções que permitem que as equipes de TI implantem uma plataforma virtualizada capaz de abstrair a infraestrutura dos aplicativos executados nela, esteja essa infraestrutura no local ou na nuvem pública. Com o VMware vSphere® e o VMware NSX®, as organizações podem aproveitar plataformas de virtualização flexíveis e robustas para dar suporte a aplicativos existentes e novos, sem comprometer a segurança e a conformidade. O VMware vRealize® Network Insight™ aprimora seus recursos por meio do gerenciamento de nuvem pronto para uso corporativo a fim de obter mais visibilidade e proteção.

Três fundamentos para proteger a infraestrutura de aplicativos

Ao usar uma nova abordagem para proteger a infraestrutura de aplicativos, as organizações de TI podem aproveitar vários recursos avançados:

Abstração de aplicativos da infraestrutura

A abstração de aplicativos da infraestrutura permite total visibilidade do caminho de dados do aplicativo para obter uma melhor compreensão dos padrões de tráfego. Ela permite que a equipe de TI aprofunde significativamente o entendimento contextual de como a infraestrutura e os aplicativos interagem entre si e com os dados. Com uma visão completa e unificada de dados, aplicativos e infraestrutura, as organizações podem criar políticas e responder a ameaças com mais eficácia.

Política de segurança detalhada e alinhada ao aplicativo

Uma abordagem virtualizada permite que as organizações alinhem melhor a política de segurança aos aplicativos que elas devem proteger e os acompanhem à medida que eles transitam entre nuvens públicas e privadas. Ela permite que a microssegmentação da rede impeça a proliferação lateral de ameaças (de leste a oeste) entre cargas de trabalho e aplicativos. E isso facilita a inclusão inteligente de serviços de segurança de terceiros na plataforma quando novos recursos são necessários.

Proteção da infraestrutura baseada em hypervisor

Um modelo que abstrai aplicativos da infraestrutura subjacente também oferece um ponto ideal dentro da infraestrutura para impedir que ela própria seja comprometida. As organizações podem proteger dados em repouso por meio de criptografia no nível da carga de trabalho em cada host do hypervisor. E elas podem criptografar dados em trânsito para reduzir o risco de comprometimento de componentes de rede, como roteadores e switches.

Um portfólio de soluções para proteger a infraestrutura de aplicativos

Seja qual for a etapa das organizações na jornada de virtualização, a VMware oferece soluções líderes do setor que aprimoram os ambientes de segurança dos aplicativos.

VMware vSphere

Para proteger os recursos de negócios críticos em um ambiente virtualizado, as organizações precisam de administração simplificada e recursos de segurança operacionalmente simples e orientados por políticas.

O VMware vSphere, plataforma de virtualização líder do setor, dispõe de uma base avançada, flexível e segura para agilidade comercial que ajuda as organizações a acelerar a transformação digital para a computação em nuvem. A solução oferece suporte a aplicativos existentes e de próxima geração por meio da experiência do cliente simplificada para automação e gerenciamento em escala; segurança completa integrada para proteção de dados, infraestrutura

e acesso; e plataforma universal de aplicativos para executar qualquer aplicativo, em qualquer lugar. Com o vSphere, as organizações podem executar, gerenciar, conectar e proteger os aplicativos em um ambiente operacional comum, em nuvens e dispositivos.

O VMware vSphere inclui recursos avançados de segurança que ajudam as organizações a proteger os ambientes e atenuar problemas se ocorrer uma violação.

- Segurança em escala: segurança orientada por políticas, que torna a proteção da infraestrutura operacionalmente simples.
- Criptografia: a criptografia no nível da VM protege contra acesso não autorizado aos dados em repouso e em movimento.
- Registro em log com qualidade para auditoria: registro em log aprimorado que fornece informações forenses sobre as ações do usuário.

Um ecossistema de fornecedores terceirizados líderes também presta suporte de segurança aprimorado para o VMware NSX.

VMware NSX

Para oferecer proteção contra as ameaças sofisticadas de hoje, as organizações precisam de um ambiente de rede virtual que permita dividir o data center em segmentos lógicos.

Quando um invasor consegue passar pelas defesas do perímetro do data center, torna-se essencial impedir que a ameaça se movimente lateralmente. Uma abordagem virtualizada permite que as equipes de TI definam políticas de segurança para cada carga de trabalho, com base em grupos dinâmicos de segurança, para que possam responder imediatamente às ameaças no data center. O VMware NSX é a plataforma de virtualização de redes que fornece o modelo operacional de uma máquina virtual para a rede do data center. Com o VMware NSX, as organizações podem criar, capturar, armazenar, mover, excluir e restaurar redes inteiras de maneira programática com a mesma simplicidade de apontar e clicar e a velocidade de uma máquina virtual, garantindo níveis de segurança, agilidade e disponibilidade antes indisponíveis com as abordagens de operação tradicionais ou centradas em hardware. A solução permite que as organizações apliquem políticas de segurança ao nível da máquina virtual individual.

O VMware NSX oferece suporte a organizações que desejam aproveitar as vantagens de segurança e desempenho da virtualização. Os principais recursos incluem:

- Segurança: as funções de segurança incorporadas no hypervisor fornecem microssegmentação e segurança detalhada para a carga de trabalho individual.
- Automação: os serviços de rede e segurança são vinculados às cargas de trabalho usando uma abordagem orientada por políticas, para automação e desempenho aprimorado.
- Continuidade do aplicativo: a rede é abstraída do hardware subjacente e vincula políticas de rede e segurança às cargas de trabalho associadas.

vRealize Network Insight

Para gerenciar um ambiente de nuvem híbrida heterogêneo, as organizações precisam de uma plataforma de gerenciamento de nuvem corporativa, que é projetada para o ambiente.

O vRealize Network Insight fornece operações inteligentes para rede e segurança do data center definido por software (SDDC, Software-Defined Data Center), com visibilidade convergente nas redes virtuais e físicas, e faz recomendações de planejamento de microssegmentação e gerenciamento de operações para o VMware NSX.

O vRealize Network Insight fornece uma ampla gama de recursos que ajudam as organizações a otimizar a segurança.

- **Visibilidade:** proporciona visibilidade convergente em overlay e underlay, nuvem virtual e física, privada e pública, com integração entre camadas físicas e virtuais.
- **Comportamento de aplicação de modelagem de microssegmentação:** permite que os usuários compreendam com facilidade quem está falando com quem e qual fluxo precisa ser permitido ou bloqueado.
- **Auditoria e conformidade:** acompanha todas as mudanças para fins de auditoria e conformidade.

SAIBA MAIS

Saiba mais sobre as prioridades e iniciativas adicionais de TI em vmware. com/br/it-priorities/transform-security.

Infraestrutura de aplicativos segura com a VMware

As organizações de TI de hoje estão enfrentando desafios sem precedentes, impulsionados pela transformação digital e um cenário de ameaça que muda rapidamente. Neste ambiente dinâmico, é mais importante do que nunca se associar a um fornecedor de tecnologia comprovada para garantir que as operações dos negócios permaneçam seguras. A Coalfire, conselheira e assessora de gerenciamento de risco cibernético independente, aprovou recentemente os recursos da VMware em seu relatório de benchmark. O relatório concluiu que o produto VMware NSX "oferece controle detalhado das políticas de segurança e visibilidade do tráfego que operacionalizam a segurança e possibilitam que os clientes cumpram os requisitos de conformidade normativa". [4]

A VMware ajuda as organizações a transformar sua abordagem de segurança por meio de uma camada de software onipresente em toda a infraestrutura de aplicativos. Ao abstrair a infraestrutura dos aplicativos aos quais oferece suporte, a VMware permite que a TI amplie sua visibilidade do caminho de dados para melhorar as informações e o controle. Juntamente com a microssegmentação, a solução ajuda as organizações a simplificar a política de segurança e a alinhar melhor a proteção para atender às necessidades de aplicativos específicos. A VMware faz isso por meio de uma ampla variedade de soluções de segurança e virtualização, apoiada por um extenso ecossistema de parceiros. Com a implantação de uma robusta solução de segurança e conformidade, as organizações podem liberar as equipes de TI para que se dediquem à promoção do crescimento e da inovação nos negócios.

[4] "Micro-segmentation Cybersecurity Benchmark Report", setembro de 2016, Coalfire

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 EUA Tel.: 1-877-486-9273 Fax: 1-650-427-5001 www.vmware.com
Rua Surubim, 504 4º andar CEP 04571-050 Cidade Monções – São Paulo – SP Tel: (+55) 11 5509-7200 www.vmware.com/br