TRANSFORMAÇÃO DA SEGURANÇA

Uma prioridade estratégica da TI

Segurança é a principal preocupação de todas as empresas

À medida que pessoas, dispositivos e objetos tornam-se mais conectados, proteger todas essas conexões e ambientes passa a ser mais importante do que nunca. As organizações de TI precisam proteger cada interação entre usuários, aplicativos e dados, independentemente de como e onde eles estejam se conectando. Elas precisam fazer isso em um ambiente cada vez mais dinâmico e que está em constante mudança.

Os riscos à segurança são elevados para empresas de todos os setores e continuam aumentando. De acordo com um estudo recente, o custo médio total de uma violação de dados aumentou de 3,52 milhões para 3,79 milhões de dólares em apenas um ano.[1] Para organizações que estão adotando ambientes em nuvem e virtualizados, visibilidade e controle máximos são fundamentais para atenuar esse risco.

A SEGURANÇA TEM MUITO A PERDER

O crime cibernético representa a causa de maior crescimento das interrupções de data centers, tendo aumentado de 2% em 2010 para 22% em 2016.[2]

O custo médio de interrupção de um data center aumentou para US$ 740.357 em 2016.[3]

Mudança das necessidades de TI em um cenário dinâmico de ameaças

Todas as empresas se tornaram digitais, e essa transformação levou a mudanças significativas no cenário de TI. As infraestruturas de aplicativos evoluíram de data centers no local com infraestrutura física para ambientes altamente dinâmicos que residem em nuvens públicas e privadas.

Os próprios aplicativos também estão mudando. As organizações estão migrando de pilhas de aplicativos monolíticos para aplicativos multicamadas distribuídos baseados em microsserviços. À medida que a força de trabalho se torna mais móvel e distribuída, os ambientes de usuários finais também evoluem. Eles não estão mais limitados aos desktops administrados por empresas, mas estão centrados em dispositivos móveis, estratégias BYOD e Internet das Coisas (IoT, Internet of Things).

Para a TI, os modelos de segurança de perímetro de rede tradicionais já não são mais suficientes para proteger a rápida proliferação de aplicativos e usuários e atender aos requisitos crescentes de conformidade. Os ambientes e usuários não estão perfeitamente protegidos por firewalls de perímetro; pelo contrário, eles exigem proteção mais flexível e ágil. Os invasores estão mais sofisticados, e o ciberespaço está cada vez mais armado. Atualmente, mesmo um hacker inexperiente que use kits de ferramentas, como Zeus e BlackPoS, pode direcionar ataques avançados a uma empresa e causar danos reais à produtividade, aos recursos e à reputação dela.

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

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

[3] Ibid.

A VMware possibilita que a TI transforme os ambientes e as operações de segurança para superar os desafios de hoje. Veja como:

- **Infraestrutura de aplicativos segura:** abstraia a infraestrutura dos aplicativos, melhorando a visibilidade e o alinhamento da segurança com os aplicativos.
- **Identidade e endpoints protegidos:** aplique uma camada de software onipresente a todos os usuários e endpoints para obter melhor visibilidade e controle, sem afetar a experiência do usuário.
- **Conformidade simplificada:** use o software em toda a infraestrutura de aplicativos, identidades e endpoints para simplificar a conformidade.

A segurança eficaz abrange diversas áreas

Proteger uma organização com uma solução de segurança robusta em conformidade não é fácil quando a infraestrutura e seus usuários estão mudando rapidamente. As antigas regras básicas de segurança de rede simplesmente não se aplicam mais, e as equipes de TI precisam acompanhar o ritmo de:

- Alteração de infraestruturas: a infraestrutura utilizada para executar aplicativos, como servidores Web e de banco de dados, está evoluindo de ambientes no local para oferecer suporte a aplicativos distribuídos e em nuvem.
- Aumento da mobilidade: a TI precisa expandir suas políticas de segurança para oferecer suporte a uma enorme quantidade de novos dispositivos e modelos.
- Maior conformidade: o ambiente de conformidade normativa torna-se cada vez mais complexo à medida que as organizações enfrentam novos requisitos.

Forneça visibilidade e contexto para transformação da segurança

A VMware pode ajudar as organizações a obter as informações necessárias para se anteciparem às mudanças das necessidades de segurança. No cerne das soluções VMware está uma camada de software onipresente que engloba toda a infraestrutura de aplicativos e endpoints e que não depende do local nem da infraestrutura física subjacente. Essa abordagem coloca o software da VMware em uma posição privilegiada dentro da infraestrutura para oferecer à TI visibilidade profunda de cada interação entre usuários e aplicativos. Um fato igualmente importante é que ela oferece contexto para compreender o que essas interações significam. Juntos, a visibilidade e o contexto mais profundo permitem que as organizações alinhem melhor seus controles e políticas de segurança aos aplicativos que estão protegendo.

A segurança eficaz requer várias camadas de proteção, e o local da VMware na infraestrutura proporciona o melhor ponto de controle possível para a TI aplicar a política e incorporar serviços terceirizados para reforçar a proteção inteligente.

Infraestrutura de aplicativos segura

À medida que os modelos de infraestrutura de aplicativos evoluem, a abordagem tradicional de segurança de rede centrada no perímetro não pode fornecer visibilidade e controle suficientes no data center. Ao mesmo tempo, os dados em repouso armazenados tornaram-se um alvo muito mais valioso para os invasores. Para resolver esses problemas, as organizações precisam transformar a maneira como protegem a infraestrutura de aplicativos.

A solução começa com a virtualização e a capacidade de abstrair a infraestrutura subjacente dos aplicativos que estão sendo executados nela, independentemente de estar no local ou na nuvem pública. Essa camada de abstração fornece visibilidade total do caminho de dados e um ponto de aplicação ideal para compartimentar aplicativos por meio da microssegmentação da rede. O uso de microssegmentação em softwares permite que as organizações simplifiquem a política de segurança e a alinhem melhor às necessidades dos aplicativos. Ele também permite que a política siga o aplicativo à medida que ele se move entre nuvens privadas e públicas. Além disso, uma camada de abstração fornece uma plataforma para a TI incluir serviços de terceiros adicionais para obter uma proteção de segurança mais avançada.

A microssegmentação ajuda a TI a evitar que ameaças de segurança violem as defesas, adotando o princípio do menor privilégio centrado no aplicativo, o que reduz a superfície de ataque da infraestrutura.

Uma camada de abstração entre os aplicativos e a infraestrutura subjacente não só ajuda a TI a evitar ataques, mas também fornece um ponto ideal para criptografar dados armazenados. Ao criptografar dados em repouso, no nível da carga de trabalho, as organizações podem garantir a segurança dos dados da infraestrutura de aplicativos, mesmo que caiam em mãos erradas.

"Com o VMware NSX®, agora disponibilizamos os dados críticos dos pacientes mais rapidamente para os médicos e pacientes do hospital, além de mantê-los seguros e segmentados."

CHRISTOPHER FRENZ
DIRETOR DE INFRAESTRUTURA DE TI,
INTERFAITH MEDICAL CENTER

Identidades e endpoints seguros

À medida que as empresas tornam-se digitais, os dispositivos móveis proliferam-se rapidamente. As organizações estão adotando dispositivos baseados em todos os sistemas operacionais, desde Android e iOS a Windows e macOS, para capacitar a força de trabalho e reinventar processos de negócios tradicionais. O suporte a todos esses dispositivos e plataformas é um desafio, especialmente porque as empresas adotam iniciativas de mobilidade corporativa, estratégia BYOD e IoT.

A VMware ajuda a TI a superar esse desafio aplicando uma camada de software onipresente a todos os usuários e endpoints para verificar a identidade do usuário e a postura do dispositivo. Essa abordagem proporciona total visibilidade e controle do usuário e do endpoint, estendendo-se até o data center ou a nuvem, onde reside a infraestrutura de aplicativos. O software da VMware permite que a TI adicione uma camada de segurança condicional e adaptável a cada nível de transação, do usuário aos recursos que eles acessam. Ela ajuda a proteger os dados corporativos e reduzir a superfície de ataque cibernético, sem afetar a experiência do usuário.

As organizações podem adotar uma única solução VMware para proteger todos os endpoints, incluindo smartphones, tablets, laptops, acessórios e dispositivos de IoT. Dessa forma, a TI pode implantar facilmente qualquer aplicativo, incluindo aplicativos nativos, Web, remotos, virtuais e desktops Windows, por meio de um único catálogo de aplicativos com logon único integrado, segurança de dados e conformidade de endpoint. Criada com foco nos espaços de trabalho dinâmicos de hoje, a solução VMware também permite que as empresas estendam a segurança além da interface de desktop virtual (VDI, Virtual Desktop Interface) e dos endpoints móveis para o data center com microssegmentação.

Como cada empresa tem necessidades de segurança específicas, a solução ajuda a personalizar os ambientes de acordo com as prioridades individuais. Ela serve como base para os parceiros de segurança da VMware, que podem aproveitar a visibilidade e os pontos de controle que a solução VMware oferece para complementá-la com ofertas de serviço próprias.

Simplificação da conformidade

O gerenciamento de riscos e a manutenção contínua da conformidade sempre são uma grande preocupação. Isso é importante principalmente para setores, como serviços financeiros, órgãos governamentais e organizações de saúde, que enfrentam requisitos rigorosos, como PCI, FISMA, HIPAA etc. Os regulamentos e requisitos estão aumentando, enquanto o cenário digital e as ameaças avançadas persistentes continuam a evoluir, o que torna mais difícil do que nunca garantir e demonstrar a conformidade.

Para complicar ainda mais, as organizações estão migrando rapidamente de data centers no local e adotando a nuvem, o que dificulta ainda mais atender às demandas de regulamentos, negócios e políticas.

A VMware oferece uma camada de software onipresente em toda a infraestrutura de aplicativos e endpoints, adotando uma abordagem holística em relação à conformidade. Essa abordagem única fornece uma localização ideal para implementar controles de conformidade e obter a visibilidade necessária para demonstrar a conformidade. A solução dispõe de uma plataforma tecnológica na qual a TI pode incluir dinamicamente ferramentas e serviços validados de parceiros do ecossistema da VMware para agilizar ainda mais o processo de conformidade.

Uma estrutura de arquitetura de referência de conformidade da VMware vincula os recursos integrados de hardware e software e os controles normativos específicos à validação de auditoria independente. As organizações podem aproveitar esse programa validado de modo independente para executar com segurança as cargas de trabalho altamente regulamentadas. Mesmo que adotem um ambiente de nuvem privada ou pública, as organizações podem confiar que estarão sempre em conformidade. A VMware entrega a velocidade, a eficiência e a agilidade que as empresas exigem e simplifica o processo de conformidade delas.

SAIBA MAIS

Saiba mais sobre essa prioridade de TI estratégica e as iniciativas correspondentes em www.vmware.com/br/ it-priorities/transform-security.

A VMware oferece segurança para um cenário de mudança de necessidades

Uma segurança robusta sempre foi essencial para as redes de negócios e, à medida que o ritmo da transformação digital se acelera, ela se torna mais necessária do que nunca. Enquanto a infraestrutura, os aplicativos e os modelos de força de trabalho tradicionais evoluem, a TI sofre cada vez mais pressão para proteger a empresa contra as novas ameaças que surgem.

A VMware capacita as organizações para transformar a segurança fornecendo uma camada de software onipresente em toda a infraestrutura de aplicativos e endpoints. Isso possibilita que as organizações maximizem a visibilidade e o contexto da interação entre usuários e aplicativos, de forma que possam alinhar os controles e as políticas de segurança aos aplicativos que elas protegem. E a VMware facilita a complementação da solução com serviços de segurança de terceiros para obter mais proteção inteligente.

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