COMO SIMPLIFICAR A SEGURANÇA E REDUZIR A SUPERFÍCIE DE ATAQUE

Implantação de proteção integrada na infraestrutura de aplicativos

vmware® | intel®

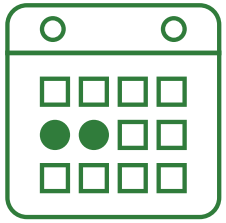
A superfície de ataque é maior do que você pensa

Não é segredo que tudo está se tornando mais conectado. Da proliferação de aplicativos aos dispositivos móveis e aos appliances em rede, vivemos em um mundo hiperconectado. As organizações estão lidando com essa explosão de endpoints ao mesmo tempo que se expandem para novos ambientes, usando data centers e várias nuvens para ajudar a gerenciar tudo.

A superfície de ataque aumenta a cada nova conexão

Agora, há mais pontos de vulnerabilidade do que nunca (e em mais lugares) e eles só aumentarão nos próximos meses e anos. Hackers e criminosos cibernéticos não perdem tempo ao explorar essas vulnerabilidades. Além de criar novos vetores e metodologias de ataque diariamente, eles também desenvolvem ferramentas fáceis de usar que permitem que as pessoas sem conhecimento técnico entrem no jogo.

Aqui, você aprenderá como a redução da superfície de ataque pode ajudar a proteger a infraestrutura de aplicativos em meio às crescentes ameaças.



Em média, são necessários **197 dias** para identificar uma violação de segurança e **69 dias** para contê-la[1]

1 Ponemon Institute, 2018 Cost of Data Breach Study, julho de 2018

Segurança que oferece suporte à agilidade nos negócios

Ao longo dos anos, a segurança ficou famosa por limitar ou desacelerar os negócios, mas isso está mudando. A natureza persistente do cenário de ameaças fez com que a segurança não fosse apenas uma medida de precaução, mas algo vital para a integridade das empresas de todos os setores.

No entanto, nem todas as soluções são iguais: As soluções que tornam a segurança simplificada, automatizada e integrada oferecem uma vantagem significativa.

As soluções de segurança devem oferecer suporte aos objetivos de negócios, permitindo que você:

- Aprenda continuamente sobre ameaças e use formas inovadoras de solucioná-las
- Previna, detecte, responda e preveja em um ciclo tranquilo e contínuo
- Proteja a mobilidade e o perímetro com táticas comprovadas para garantir a segurança de dispositivos e aplicativos
- Aprimore o ecossistema de segurança geral com visibilidade, contexto e controle superiores

Lembre-se: não adianta correr atrás das ameaças

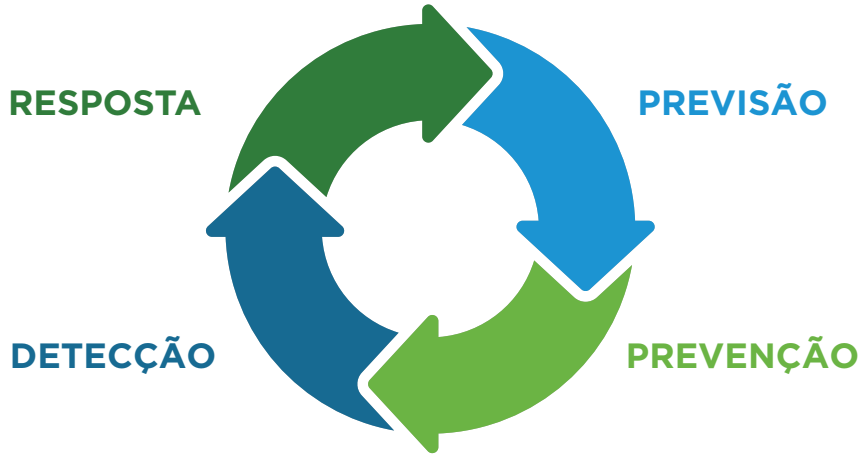
Reconsiderar a abordagem de segurança é o primeiro passo para criar uma infraestrutura de aplicativos mais segura. Para combater o crime cibernético, as organizações de TI geralmente se concentram em ameaças ou vulnerabilidades específicas e são pegas de surpresa quando os invasores mudam de tática. Para permanecer à frente é necessário ter uma visão mais ampla e não perseguir ameaças individuais. Estudar e entender as tendências atuais relacionadas às ameaças pode ajudar você a abordá-las de maneira mais completa e obter melhores resultados ao longo do tempo.

Por exemplo, o ransomware pode tirar proveito de variações e vulnerabilidades diferentes. A compreensão das tendências em ataques de ransomware ajudará a proteger a infraestrutura e os dados críticos. Muitos ataques contra organizações maiores acontecem apenas uma vez, pois são especificamente criados e direcionados contra essa organização. Portanto, criar uma resposta para um tipo de ataque em particular não é eficiente.

Em vez disso, concentre-se na forma como a redução da superfície de ataque pode limitar a exposição e os danos causados por um invasor.

Uma estrutura de aprendizado contínuo para a segurança

Em 2016, o Gartner lançou um modelo de segurança baseado em quatro princípios importantes que informam continuamente um ao outro quando criar um processo proativo para proteção dos aplicativos.[2] Essa abordagem em camadas não se concentra em uma ameaça específica, mas representa uma mentalidade que permite que a TI evolua junto com as ameaças.



Reduzir a superfície de ataque faz parte da fase de **prevenção**. Isso prepara você para as etapas seguintes, possibilitando detecção aprimorada devido a uma visibilidade maior e um monitoramento contínuo. Com isso, é possível responder mais rapidamente e atualizar os protocolos de segurança para prever ameaças futuras.

2 Gartner Research, Using the Predict, Prevent, Detect, Respond Framework to Communicate Your Security Program Strategy, abril de 2016

Proteger um alvo em movimento é complicado

Pouco tempo atrás, os aplicativos ficavam confinados no data center, onde podiam ser cuidadosamente monitorados e protegidos. Isso não acontece mais. Os aplicativos não estão mais em pilhas monolíticas em um único servidor. Eles estão distribuídos em muitos servidores virtuais, contêineres e servidores físicos. Eles também são altamente dinâmicos e movem-se entre locais, data centers, nuvens e redes de filiais. O perímetro do data center, que anteriormente era a primeira linha de defesa, agora é permeável.

Arquiteturas em evolução exigem uma resposta evoluída às ameaças

À medida que a natureza dos aplicativos muda, eles se tornam cada vez mais importantes para o sucesso dos negócios. Para fornecer proteção adequada, os controles de segurança devem ser tão onipresentes e ágeis quanto os próprios aplicativos.

As empresas têm **27,9% de chance** de sofrer violações recorrentes nos próximos dois anos[3]

3 Ponemon Institute, 2018 Cost of Data Breach Study, julho de 2018

O status quo precisa ser desafiado: a segurança intrínseca representa o avanço

A infraestrutura centrada em hardware não está adequadamente equipada para lidar com os aplicativos modernos e as ameaças sofisticadas e rápidas. As abordagens legadas exigem implantação, configuração e gerenciamento manuais. Elas também dependem de tecnologias de segurança adicionais que demoram a se adaptar e deixam lacunas.

Uma infraestrutura virtual definida por software cria uma malha digital que fornece conectividade onipresente e segurança intrínseca aos aplicativos, independentemente de onde eles estejam, desde o data center até a nuvem e o perímetro.

Com o Virtual Cloud Network, você pode:

- Proteger aplicativos por padrão
- Obter visibilidade dos aplicativos em vários ambientes
- Adotar uma abordagem centrada em aplicativos para as políticas de segurança

Vejamos esses recursos com mais detalhes.

Proteger aplicativos por padrão

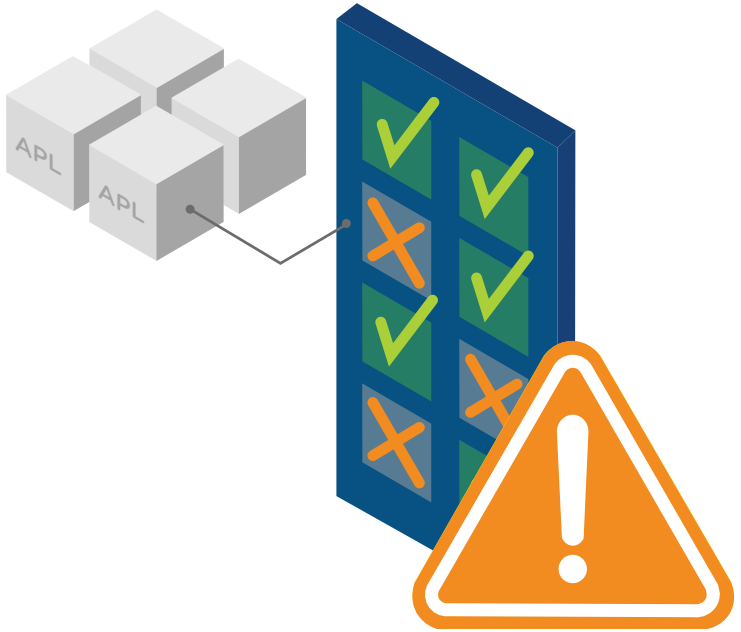
A VMware protege aplicativos e cargas de trabalho automaticamente, criando controles de segurança diretamente na camada de software onipresente onde os aplicativos residem.

Ao ativar novos endpoints de data center como parte de aplicativos, eles são automaticamente criptografados. Eles herdam políticas e controles de segurança que permanecem durante todo o ciclo de vida, mesmo quando se movem para diferentes ambientes.

Obter visibilidade dos aplicativos em vários ambientes

Com uma solução que ajuda você a entender os comportamentos de comunicação entre a rede e os aplicativos, você pode direcionar melhor o conhecimento da situação que oferece suporte às suas metas de segurança.

Uma infraestrutura de aplicativos segura fornece visibilidade crítica em todas as atividades de aplicativos: de processos de aplicativos a fluxos e padrões de comunicações de aplicativos. Procure uma solução que ofereça visibilidade de 360˚, abrangendo redes virtuais, físicas e multi-cloud.



Adotar uma abordagem centrada em aplicativos às políticas de segurança

A capacidade de projetar e aplicar políticas de segurança flexíveis e centradas em aplicativos pode ajudar você a reduzir a superfície de ataque geral de aplicativos e dados. As políticas de segurança devem ser desenhadas e aplicadas em função dos aplicativos e dados, independentemente de que residam na rede ou no endpoint do data center.

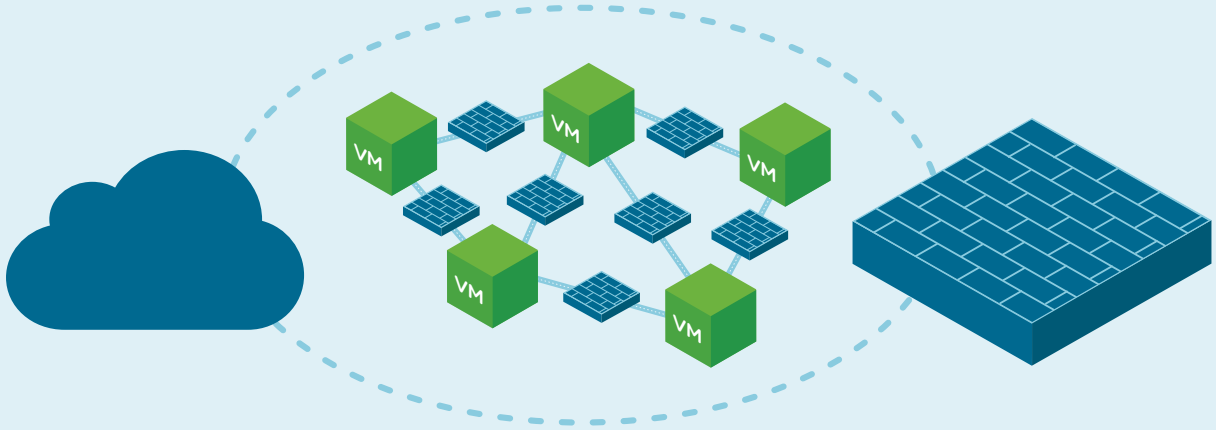
Você pode usar o estado e o comportamento desejados dos endpoints do data center onde os aplicativos residem para garantir que o funcionamento deles seja correto, em vez de ir atrás das ameaças.

O importante papel da microssegmentação

Hoje, não nos perguntamos se uma violação de segurança ocorrerá, mas quando ela ocorrerá. Como parte de uma abordagem definida por software, a microssegmentação limita a disseminação lateral de ameaças ao impor políticas de segurança de rede no nível mais granular: o endpoint do data center individual.

Com controle leste-oeste ativado pela microssegmentação, o alcance das ameaças não é mais ilimitado. A inserção de serviços dinâmicos permite que você direcione com eficiência o tráfego de rede por meio de outros serviços de segurança, como firewalls de próxima geração, sem a necessidade de intervenção manual.

A capacidade de operacionalizar a microssegmentação é fundamental para a eficácia dela. Uma solução deve fornecer visibilidade às comunicações com recomendações sobre como implementá-las.



O local é tudo

Uma solução que cria controles de segurança diretamente no hypervisor oferece uma segurança abrangente que começa no núcleo, com um modelo operacionalmente simples e orientado por políticas.

Benefícios da proximidade com o hypervisor:

- **Simplificação da implantação e do gerenciamento.** Devido à integração com as ferramentas de máquina virtual, é possível gerenciar isso como parte do conjunto de ferramentas e do processo normal de gerenciamento de VMs.
- **Melhoria de visibilidade e contexto.** O hypervisor permite que você veja todos os fluxos leste-oeste, norte-sul de e para máquinas virtuais junto com o contexto que indica se o tráfego é esperado ou potencialmente problemático.
- **Ativação de controles adicionais de segurança.** Ela aproveita o hypervisor para fornecer melhor visibilidade e segurança dos aplicativos, além do que você já implantou.

Comece reduzindo sua superfície de ataque

Os aplicativos modernos continuarão dinâmicos e distribuídos, e a superfície de ataque continuará aumentando. Para proteger sua empresa, você precisa de uma infraestrutura na qual a segurança seja um componente integrado e não uma solução adicionada posteriormente.

A VMware reduz a superfície de ataque do aplicativo, oferecendo segurança intrínseca e consistente do data center à nuvem e ao perímetro. O VMware NSX® permite a microssegmentação na rede para evitar a disseminação lateral de ameaças. O VMware AppDefense™ aplica o estado e o comportamento pretendidos do aplicativo nos endpoints do data center, enquanto o VMware vSphere® e o VMware vSAN™ fornecem criptografia de dados em repouso.

A VMware e a Intel transformam o sistema de rede e a segurança, usando uma solução holística entre software e hardware para conectar e proteger aplicativos e dados onde quer que residam, do data center à nuvem e ao perímetro.

DÊ O PRÓXIMO PASSO

Saiba mais sobre a infraestrutura de aplicativos segura >

Experimente as soluções NSX em um laboratório prático >

Junte-se a nós on-line:

vmware® | intel®

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.: (11) 5509-7200 www.vmware.com/br

Nº do item: TS-0508_VM_Intel_How-to-Simplify-Security-and-Shrink-the-Attack-Surface_Guide_080918_BR
08/18