
vmware
intel
TRANSFORME A SEGURANÇA DA SUA TI EM TRÊS ETAPAS

SUMÁRIO

SEGURANÇA
É A PRINCIPAL PREOCUPAÇÃO DE TODAS AS EMPRESAS

À medida que pessoas, dispositivos e objetos se tornam mais conectados, torna-se cada vez mais importante proteger todas essas conexões e ambientes. Em uma pesquisa recente sobre prioridades de TI, 69% dos entrevistados disseram à Tech Pro Research que melhorar a segurança representou a principal iniciativa de TI para 2017.[1]

Na mesma pesquisa, os entrevistados também disseram que a segurança seria o maior desafio de TI no próximo ano. Isso acontece porque as organizações de TI precisam proteger todas as interações entre usuários, aplicativos e dados, independentemente de como e onde elas ocorrem. E isso precisa ser feito em um ambiente cada vez mais dinâmico e em constante mudança.

Os riscos à segurança são elevados para empresas de todos os setores e eles não param de crescer. De acordo com um estudo recente, o custo total médio de uma violação de dados aumentou de US$ 3,52 milhões para US$ 3,79 milhões em apenas um ano.[2] 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

- Crimes cibernéticos representam a causa de interrupções de data centers que mais cresce, aumentando de 2% em 2010 para 22% em 2016.[3]
- O custo médio de uma interrupção de data center aumentou para US$ 740.357 em 2016.[4]

1 "IT Budget Research: Where CXOs are placing their bets for 2017", Tech Pro Research, julho de 2016.

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

3 "Cost of Data Center Outages", Ponemon Institute, janeiro de 2016.

4 Ibid.

RISCOS CRESCENTES EM UM CENÁRIO DINÂMICO DE AMEAÇAS

Agora, todas as empresas são digitais; essa transformação deu origem a mudanças significativas no cenário de TI e, consequentemente, gerou novos desafios para a segurança de TI.

Comece com a evolução das infraestruturas de aplicativos, que passaram de data centers locais que executam infraestruturas físicas a ambientes altamente dinâmicos que residem em nuvens públicas e privadas. Pense também em como os próprios aplicativos estão mudando. As organizações estão migrando de grandes pilhas de aplicativos para aplicativos distribuídos e de multicamadas baseados em microsserviços. À medida que a força de trabalho se torna mais móvel e distribuída, os ambientes dos usuários finais também evoluem. Antes, os usuários ficavam limitados a desktops administrados corporativamente, mas agora eles estão centrados em dispositivos móveis, estratégia BYOD e na Internet das Coisas (IoT, Internet of Things).

Como resultado, os modelos de segurança de perímetro de rede tradicionais já não são suficientes para proteger a expansão de aplicativos e usuários ou atender aos requisitos crescentes de conformidade. Ambientes e usuários não estão mais perfeitamente protegidos por firewalls de perímetro, eles precisam de uma proteção mais flexível e ágil contra invasores que se tornaram mais sofisticados. O ciberespaço está cada vez mais armado. Mesmo um hacker inexperiente que usa kits de ferramentas, como Zeus e BlackPoS, pode visar uma empresa com ataques avançados e causar danos reais à produtividade, aos recursos e à reputação dela.

Enquanto nos ajustamos para responder a esses novos desafios de desenvolvimento, os padrões de conformidade se tornam cada vez mais complexos e forçam a equipe de TI média a gastar 20% de seu tempo em esforços para manter a conformidade.

TRÊS ÁREAS DE FOCO PARA SEGURANÇA EFICIENTE DE TI

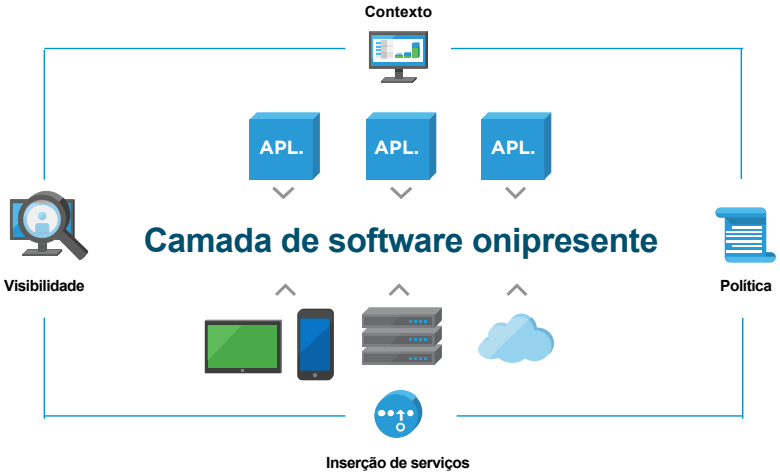
Proteger uma organização com uma solução de segurança robusta em conformidade não é fácil quando a infraestrutura e seus usuários mudam rapidamente. As antigas regras básicas de segurança de rede simplesmente não se aplicam mais, e as equipes de TI precisam acompanhar o ritmo de:

- **Mudanças de infraestruturas:** a infraestrutura utilizada para executar aplicativos como servidores Web e de banco de dados está evoluindo e ultrapassando os limites de ambientes locais 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 grande 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

Para ficar um passo à frente das mudanças nas suas necessidades de segurança, você precisa de visibilidade aprofundada em todas as interações entre usuários e aplicativos. Você também precisa de uma solução que forneça um contexto que ajude a entender o que essas interações significam. Quando combinados, maior visibilidade e contexto podem ajudar a alinhar os controles e as políticas de segurança aos aplicativos que você deve proteger.

Qual é a base para essa solução? Uma camada de software onipresente em toda a infraestrutura de aplicativos e endpoints que seja independente da infraestrutura física subjacente ou da localização.



Na verdade, uma segurança eficaz exige várias camadas de proteção. E a solução de software certa na infraestrutura fornece o melhor ponto de controle possível para aumentar a visibilidade, reforçar a política e permitir a inserção de serviços de terceiros para mais proteção inteligente.

Vamos dar uma olhada nas três principais etapas para a transformação da sua segurança de TI:

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

1. INFRAESTRUTURA DE APLICATIVOS SEGURA

Os modelos de infraestrutura de aplicativos evoluíram, e a abordagem tradicional de segurança de rede centrada no perímetro não consegue mais fornecer visibilidade e controle suficientes no data center. Ao mesmo tempo, os dados em repouso armazenados se tornaram um alvo muito mais valioso para os invasores. Para lidar com esses problemas, é necessário mudar a maneira de proteger 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, quer essa infraestrutura esteja no local ou na nuvem pública. Essa camada de abstração fornece visibilidade total no 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. A microssegmentação 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 serviços adicionais de terceiros a serem inseridos, a fim de garantir uma 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 eles caiam em mãos erradas.

2. IDENTIDADE E ENDPOINTS PROTEGIDOS

À medida que os seus negócios se tornam digitais, os dispositivos móveis crescem rapidamente. Organizações como a sua estão usando tudo, Android, iOS, Windows, MacOS e outros dispositivos para fortalecer a força de trabalho e repensar os 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.

Ao aplicar uma camada de software onipresente em todos os usuários e endpoints para verificar a identidade do usuário e a postura do dispositivo, você estará equipado para lidar com esse desafio. 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. Com uma camada de software, a TI pode adicionar uma camada de segurança adaptável e condicional em cada nível transacional, dos usuários aos recursos acessados. Essa camada ajuda a proteger os dados corporativos e reduzir a superfície de ataque cibernético, sem afetar a experiência do usuário.

Procure uma solução simples que possa proteger todos os endpoints, incluindo smartphones, tablets, laptops, acessórios e dispositivos de IoT. Como resultado, a TI pode implantar facilmente qualquer aplicativo, incluindo aplicativos nativos, Web, remotos e virtuais, além de desktops Windows, por meio de um único catálogo de aplicativos com logon único integrado, segurança de dados e conformidade de endpoint. Para os espaços de trabalho dinâmicos atuais, você deve usar uma solução que estenda a segurança além da interface de desktop virtual (VDI, Virtual Desktop Interface) e dos endpoints móveis no data center com microssegmentação.

Como cada empresa possui necessidades de segurança específicas, sua solução também deve ajudar a personalizar o ambiente para se alinhar às suas prioridades. Você terá uma base para trabalhar com parceiros de segurança, que podem aproveitar os pontos de visibilidade e controle fornecidos para complementar a solução com suas próprias ofertas de serviços.

3. CONFORMIDADE SIMPLIFICADA

O gerenciamento de riscos e a manutenção de conformidade contínua são sempre grandes preocupações. Esses fatores são especialmente importantes para setores como serviços financeiros, agências do governo e organizações de saúde, pois eles enfrentam requisitos rigorosos, como PCI, HIPAA, ECPA, a Diretiva relacionada à proteção de dados para a Europa e muito mais. Os regulamentos e os requisitos estão crescendo à medida que o cenário digital e as persistentes ameaças continuam evoluindo. Isso faz com que garantir e demonstrar conformidade sejam tarefas mais desafiadoras do que nunca.

Para complicar ainda mais, as organizações estão migrando rapidamente de data centers locais para a nuvem, o que dificulta o cumprimento de regulamentos, negócios e políticas.

Com uma camada de software onipresente em toda a infraestrutura de aplicativos e endpoints, você adotará uma abordagem holística sobre a conformidade.

Essa abordagem única oferece um ponto ideal para implementar controles de conformidade e obter a visibilidade necessária para demonstrar conformidade. A solução certa fornece uma plataforma tecnológica na qual as ferramentas e os serviços validados de parceiros do ecossistema podem ser inseridos dinamicamente para agilizar ainda mais o processo de conformidade.

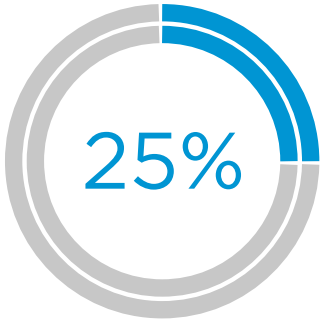
> “Quanto mais empresas competirem por talento em um mercado limitado, mais a falta de habilidades se tornará um problema. As empresas serão forçadas a repensar estratégias e procurar soluções (de segurança) que sejam mais proativas e exijam menos gerenciamento para permitir o melhor uso dos recursos.[5]”

JAMES MAUDE

ENGENHEIRO DE SEGURANÇA DA AVECTO

5 http://www.information-management.com/gallery/6-top-it-security-trends-for-2017-10030567-1.html.

Com uma estrutura de arquitetura de referência para conformidade, é possível vincular recursos integrados de software e hardware e controles regulatórios específicos com validação de auditoria independente. Além disso, você pode aproveitar um programa validado de forma independente para executar cargas de trabalho altamente regulamentadas com segurança. Quer use um ambiente de nuvem privada ou pública, você precisa de garantias que assegurem que sua organização permanecerá sempre em conformidade. Isso requer uma solução que tenha a velocidade, a eficiência e a agilidade necessárias e, ao mesmo tempo, simplifique o processo de conformidade.



Até 2020, mais de 25% de todos os ataques identificados na empresa envolverão a Internet das Coisas (IoT, Internet of Things).[6]

> "Os clientes estão se afastando das empresas que sofrem violações, e o ambiente regulatório está exigindo que as empresas adquiram proteção avançada, seja ela criada internamente ou terceirizada."[7]

FADI ALBATAL

VICE-PRESIDENTE SÊNIOR DA ABOVE SECURITY

6 "Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016", Gartner Inc., abril de 2016.

7 http://www.datacenterjournal.com/cybersecurity-trends-2017-companies-fight-back/.

SEGURANÇA PARA CENÁRIO E NECESSIDADES EM CONSTANTE MUDANÇA

Uma segurança robusta sempre foi essencial para as redes de negócios e, conforme o ritmo das mudanças aumenta, ela se torna mais necessária do que nunca. Enquanto a infraestrutura, os aplicativos e os modelos de força de trabalho tradicionais evoluem, sua equipe de TI sofre cada vez mais pressão para proteger a empresa contra novas ameaças.

Uma camada de software onipresente em toda a infraestrutura de aplicativos e endpoints pode ajudar a transformar sua segurança. Ela permite maximizar a visibilidade e o contexto da interação entre seus usuários e aplicativos para que você possa alinhar os controles e as políticas de segurança aos aplicativos protegidos. Além disso, com essa camada você pode complementar sua solução com serviços de segurança de terceiros a fim de oferecer mais proteção inteligente.

TRANSFORMAÇÃO DA SEGURANÇA

A VMware e a Intel transformam a segurança ao fornecer medidas abrangentes de segurança com base tanto em software quanto em hardware para infraestruturas e endpoints de aplicativos que maximizam a visibilidade, o contexto e o controle a fim de proteger as interações entre usuários, aplicativos e dados.

COMECE HOJE

Transforme a segurança de TI para o cenário atual
www.vmware.com/br/it-priorities/transform-security

Junte-se a nós on-line:

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-0318 Intel Co-Branded-Transform Your Security
07/17