GUIA PARA REPENSAR SUA SEGURANÇA DE TI

Resposta ao desafio de segurança de um cenário de TI dinâmico

vmware® | intel®

Definição de uma era de transformação digital

Ao observar o surgimento de empresas que nasceram na era digital (pense em Uber e Airbnb), percebemos como a tecnologia serve de diferencial competitivo para essas empresas. A Uber, por exemplo, se tornou o maior serviço de táxi do mundo sem possuir nenhum carro; e a Airbnb surgiu como a maior empresa de hospedagem do mundo sem possuir nenhum imóvel.

Remodelagem de empresas tradicionais

Ao mesmo tempo, também podemos ver como a tecnologia está transformando as empresas mais antigas e tradicionais. As empresas industriais, por exemplo, consideram essencial adotar o software como o meio para tornar as operações mais eficientes e produtivas. Jeff Immelt, presidente e CEO da General Electric, diz de forma sucinta: "Sabemos que, se você for dormir como uma empresa industrial, acordará como uma empresa de software." O que a GE e outras empresas estão aprendendo é que competir no ambiente de negócios atual significa ser uma empresa digital.

Dimensionamento do desafio de segurança

Acompanhando essa onda crescente de transformação digital está o crescimento colossal e contínuo no número de usuários finais com dispositivos digitais, bem como no volume de aplicativos e dados que devem ser gerenciados. É um fenômeno que gerou uma enxurrada de ameaças de segurança para organizações de TI. Os data centers que foram instalados no local de forma segura evoluíram para um ambiente multi-cloud público e privado altamente dinâmico. E os usuários que já trabalharam em desktops corporativos estão constantemente em movimento fora do local de trabalho, esperando acessar redes corporativas em seus próprios dispositivos e até mesmo pela Internet das Coisas (IoT, Internet of Things).

Uma crescente onda de risco

Com esses fatores em ação, a exposição ao risco continua aumentando. Além disso, os invasores sofisticados pretendem explorar essas vulnerabilidades de data center. Em uma pesquisa recente que avaliou a segurança de TI corporativa global, 75% dos entrevistados admitiram que provavelmente estariam lutando contra um ataque cibernético em 2016.[1] As organizações de TI também enfrentam demandas crescentes de conformidade normativa. De fato, as responsabilidades de conformidade representam até 20% do tempo de um funcionário de TI.[2]

Nesse cenário de TI dinâmico, os desafios de segurança resultantes são claros, mesmo que não sejam simples de resolver: como protegemos as interações entre usuários, aplicativos e dados?

RESULTADO DO IMPACTO

- O custo médio de interrupção de um data center aumentou para US$ 740.357 em 2016.[3]
- Incluindo os custos associados à propriedade intelectual roubada, a espionagem cibernética global custa às empresas até US$ 1 trilhão por ano.[4]
- Em 2016, o custo médio de uma violação de dados aumentou para US$ 4 milhões ou US$ 158 por registro perdido ou roubado.[5]

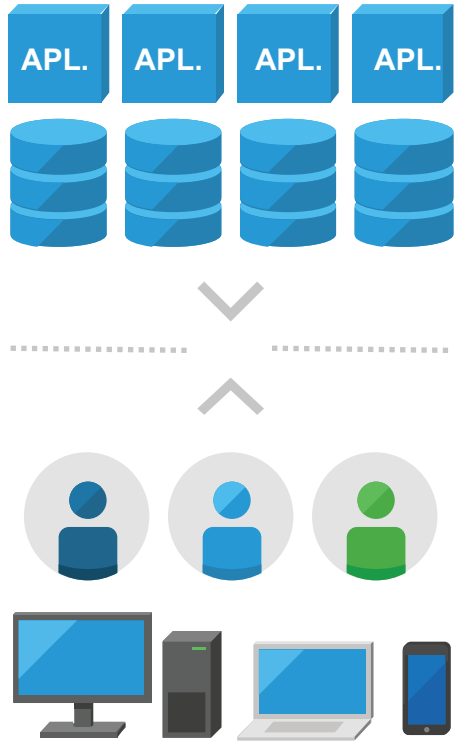


Figura 1. "A transformação digital afeta a TI e a segurança"

[1] State of Cybersecurity: Implications for 2016, ISACA, 2016.
[2] Cost of Data Center Outages, Ponemon Institute, janeiro de 2016.http://datacenterfrontier.com/white-paper/cost-data-center-outages/.
[3] Cost of Data Center Outages, Ponemon Institute, janeiro de 2016.
[4] https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/.
[5] 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, junho de 2016.

Cinco áreas para repensar a segurança de TI

Como já vimos, mesmo com os gastos apenas com segurança de TI atingindo US$ 80 bilhões em 2016[6], a antiga abordagem de segurança de TI não é suficiente para conter os crescentes níveis de ameaça. Com isso em mente, aqui estão cinco considerações para ajudar a repensar sua abordagem sobre a segurança de TI:

1. Alteração do modelo de segurança
   Usando soluções pontuais, caixas independentes ou produtos de software adicionais, os sistemas de segurança de TI tradicionais são complexos e mal-coordenados. É necessário um modelo holístico e planejado que ofereça segurança de forma simples e eficaz.
2. Implementação de uma camada de software onipresente
   Com uma camada de software onipresente em toda a infraestrutura de aplicativos endpoints, é possível abstrair a infraestrutura dos aplicativos em execução nela. Como resultado, você pode aplicar a segurança de forma fácil e eficaz em todo o data center.
3. Fornecimento de visibilidade e contexto máximos
   Ao abstrair a infraestrutura de seus aplicativos, você obtém visibilidade nos fluxos de dados do aplicativo e no contexto completo do início ao fim para interações entre usuários, aplicativos e dados.
4. Alinhamento de controles e políticas de segurança aos aplicativos
   Com os benefícios de visibilidade e contexto máximos, você pode começar a alinhar seus controles e políticas de segurança aos aplicativos que você está tentando proteger.
5. Inclusão de serviços de segurança adicionais de terceiros
   Ao alinhar controles e políticas de segurança aos aplicativos, você pode começar a inserir serviços de segurança adicionais de terceiros para camadas adicionais de proteção inteligente.

NOVAS REGRAS PARA SEGURANÇA DE REDE

As antigas regras básicas de segurança da rede simplesmente não se aplicam mais, e as equipes de TI precisam acompanhar o ritmo de:

- **Infraestrutura dinâmica:** a infraestrutura está evoluindo a partir 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:** as organizações enfrentam novos requisitos de conformidade normativa.

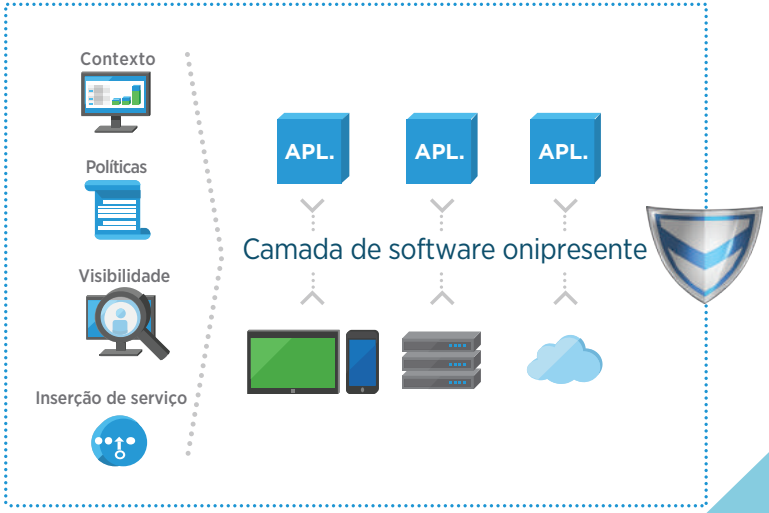


Figura 2. Uma camada de software onipresente significa que a segurança está em todo lugar

[6] "Segundo a Gartner, os gastos em segurança das informações em todo o mundo vão aumentar 7,9%, alcançando US$ 81,6 bilhões em 2016", Gartner Inc., agosto de 2016.

Adoção de uma abordagem tripla sobre segurança de TI

A transformação do ambiente de segurança para atender aos atuais desafios de segurança essenciais exige uma estratégia tripla.

Proteger o data center: repensar sobre o gerenciamento e a segurança do data center

Você precisa dos meios para "compartimentalizar" melhor os ativos sensíveis, alinhar os controles de segurança em torno desses ativos e obter mais visibilidade e controle para ajudar a detectar e responder às ameaças.

Proteger o endpoint: repensar sobre o gerenciamento e a segurança da infraestrutura do usuário

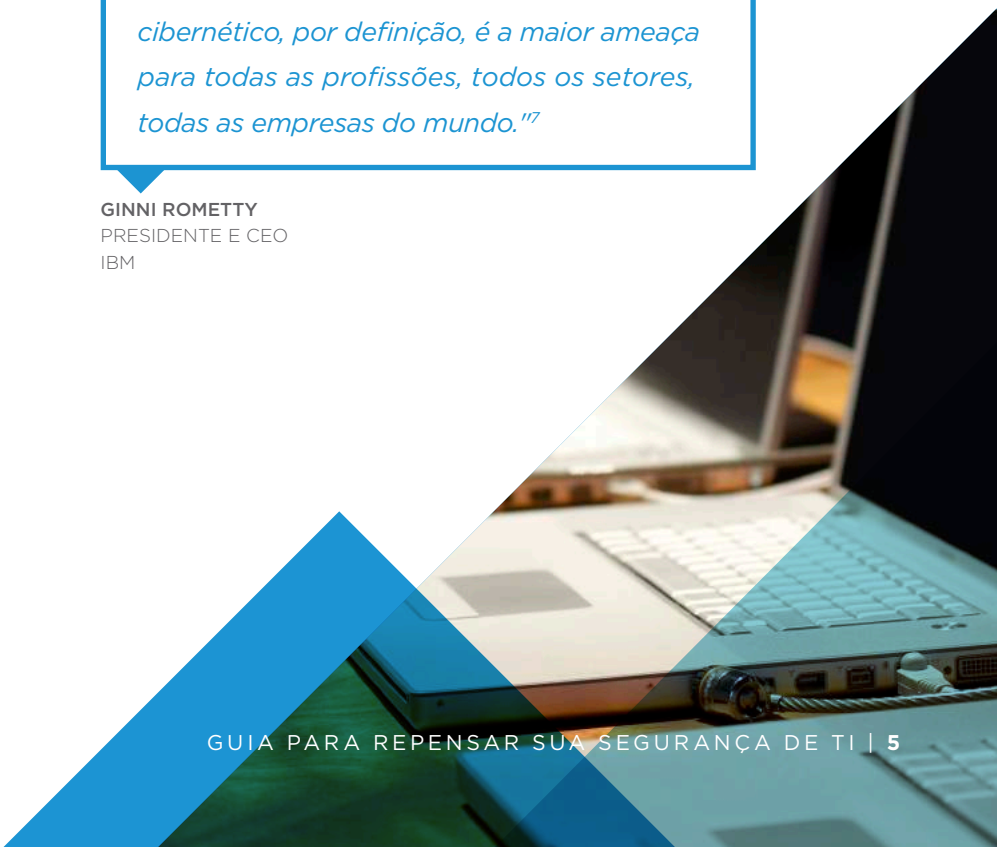
Com a proliferação de dispositivos móveis e sistemas operacionais, não há malha uniforme para a infraestrutura de usuários. Há um mundo enorme e heterogêneo lá fora. Você precisa de mais visibilidade e controle, não apenas de um ponto de vista de infraestrutura, mas de uma perspectiva centrada em aplicativos, sem prejudicar a experiência que os usuários esperam.

Proteger o usuário: repensar sobre os controles de usuário/acesso

O acesso de usuário é fundamental para capacitar a força de trabalho. Você precisa de uma abordagem que possa ajudar a reduzir a superfície de ataque, criar uma maior visibilidade nas interações do usuário e permitir uma resposta eficiente às ameaças de segurança inevitáveis.

> *"Acreditamos que os dados são o fenômeno do nosso tempo. São os novos recursos naturais do mundo. São a nova base de vantagem competitiva e estão transformando todas as profissões e o setor. Se tudo isso for verdade, mesmo que inevitável, o crime cibernético, por definição, é a maior ameaça para todas as profissões, todos os setores, todas as empresas do mundo."*[7]

GINNI ROMETTY
PRESIDENTE E CEO
IBM



[7] "CEO da IBM sobre hackers: "O crime cibernético é a maior ameaça a todas as empresas no mundo." Forbes. 24 de novembro de 2015.

Conclusão

A transformação digital representa uma grande oportunidade para os seus negócios. No entanto, com ela surgem riscos e um enorme desafio: proteger o número crescente de interações entre os usuários, aplicativos e dados.

Ao repensar a abordagem sobre segurança de TI, você pode responder a este desafio de segurança atual. A transformação da segurança começa ao se estabelecer uma camada de software onipresente em toda a infraestrutura de aplicativos e endpoints. Com essa camada de software implantada, você ganhará visibilidade profunda sobre essas interações que deseja proteger e sobre o contexto para entender o que elas significam.

A VMware e a Intel transformam a segurança ao fornecer medidas abrangentes de segurança com base tanto em software quanto em hardware na infraestrutura e nos 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

Obter ajuda para repensar a abordagem sobre segurança de TI

SAIBA MAIS >

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
Rua Surubim, 504 4º andar CEP 04571-050 Cidade Monções – São Paulo – SP Tel.: (11) 5509-7200 www.vmware.com/br

Item nº: 16-VMWA-4177_TS-0223_eBook_Rethinking_Security
05/17