RESUMO DE SOLUÇÃO DA IDC

Avaliação do valor comercial do Data Center Seguro

Oferecimento: Cisco

Pete Lindstrom Richard L. Villars
Matthew Marden
Dezembro de 2014

RESUMO

O mundo da TI está passando por uma enorme mudança estrutural: da "2ª plataforma" baseada em cliente/servidor, voltada para empresas, para o que a IDC chama de a era da "3ª plataforma" criada com base em tecnologia móvel, social, de Big Data e de nuvem. Hoje em dia, praticamente toda a inovação de negócios é baseada nesta nova plataforma, com centenas de milhares a milhões de soluções e serviços de alto valor que transformam o setor e mudam a experiência do cliente final que surgirá com essa nova plataforma. As três características que definem data centers na 3ª plataforma são:

- **Escala**: sustenta o aumento de até 10 vezes na quantidade de usuários e/ou conjuntos de dados sem aumento correspondente no tamanho do data center
- **Velocidade:** cria e atualiza aplicativos e serviços em semanas/dias, e não anos/meses, sem aumentar os níveis das operações de TI e das equipes de desenvolvimento
- **Escopo:** possibilita a coordenação de vários aplicativos e fontes de dados, internas e externas, para oferecer aos clientes novos serviços sem sacrificar a integridade dos dados e a experiência do usuário

Neste mundo de mercados inteligentes, móveis, de nuvem e de Big Data, o data center não pode mais ser apenas o lugar onde uma empresa mantém seus servidores e armazena seus dados corporativos. Ele é o primeiro ponto de contato com os clientes da empresa e, por isso, o data center deve oferecer os serviços mais seguros e mais confiáveis. O data center é a base para novos modelos de negócios em um grupo em expansão de mercados.

Com a mudança nas arquiteturas e nos casos de uso do data center como reação a esses acontecimentos, as questões relacionadas à segurança do data center estão se tornando fundamentais para as empresas. Com as recentes invasões em algumas das maiores instituições varejistas e financeiras do mundo, tem havido uma preocupação crescente, que atingiu até mesmo os executivos e membros da diretoria. Firewalls de próxima geração, soluções de sandbox, gateways da Web seguros e outras soluções ajudam a lidar com essas questões no perímetro. No entanto, o data center apresenta um conjunto diferente de problemas, aos quais as soluções de segurança devem atender.

Em primeiro lugar, o processo de gerenciamento e provisionamento é muito diferente no perímetro em comparação ao data center. Como mencionado anteriormente, a natureza dinâmica do data center atual requer soluções de segurança que respaldem o gerenciamento de políticas e a escalabilidade em um ambiente, onde novos recursos são constantemente criados, alterados e divididos. Pedir para os administradores concluírem essas etapas manualmente não é uma opção, e essa ação frequentemente leva a um afrouxamento dos procedimentos de segurança. As soluções de segurança devem ser completamente integradas aos outros componentes da malha do data center, para garantir uma abordagem coerente e uma orquestração simplificada.

Além disso, muitos data centers aproveitam várias tecnologias. Apenas algumas empresas são capazes de criar seus data centers do zero, enquanto a maioria faz um mix de sistemas e aplicativos novos e antigos que utilizam recursos físicos e virtuais. Consequentemente, as soluções de segurança devem atender tanto aos atuais ambientes diversos, como oferecer um caminho para ambientes mais inteligentes que aproveitam as soluções de rede definidas por software e facilitam o uso de novas soluções de virtualização de função de rede (NFV) dos provedores de serviço de rede. Essas funções de rede inteligentes facilitarão o desenvolvimento e respaldo da nuvem híbrida e ambientes dispersos geograficamente, ao tratar toda a infraestrutura como uma única localização lógica.

Supondo que esses critérios iniciais de implantação e desenvolvimento sejam atendidos, as implicações de segurança dos diferentes padrões de tráfego presentes nos data centers devem ser levadas em consideração. Em primeiro lugar, grande parte do tráfego no data center se desloca através de máquinas virtuais, sem jamais chegar a uma ferramenta física. É essencial ter visibilidade e controle deste tráfego, para se ter um design de data center seguro. Sem uma instância de segurança virtual que possa verificar o percurso do tráfego entre máquinas virtuais, para se ter um design seguro seria necessário rotear o fluxo de fora do segmento virtual para uma ferramenta física, para inspeção, antes de rotear novamente para o destino virtual. Esse modelo causa impactos negativos no desempenho e gera latência. Além disso, com os recursos espalhados por vários locais e sendo migrados frequentemente, as soluções de segurança devem ter a capacidade de inspecionar fluxos de tráfego assimétricos sem degradar o desempenho.

Por fim, o tráfego de aplicativos no data center é muito diferente do tráfego no perímetro empresarial. Por ser a origem dos aplicativos empresariais personalizados, o data center não é a melhor opção para abrigar tecnologias de firewall de próxima geração tradicionais (NGFW), que são mais bem equipadas para defender a borda de rede corporativa contra ameaças que surgem dos aplicativos da Web pública, como o Facebook, Twitter e YouTube. As soluções de segurança do data center devem respaldar a visibilidade dos aplicativos corporativos personalizados, bem como o uso de recursos de dados corporativos digitalizados, para que seja possível compreender o contexto de segurança e garantir o melhor desempenho.

Vantagens para a empresa com o data center seguro

Antes de tudo, as soluções de segurança no data center devem fazer parte do processo de gerenciamento central, seja do ponto de vista da segurança geral, ou de uma perspectiva da orquestração de uma rede definida por software (SDN). A equipe de TI não pode configurar a segurança manualmente no ambiente do data center. As soluções de segurança, que não respaldam o provisionamento dinâmico e não se ajustam ao consumo de recursos, não serão utilizadas.

As empresas podem aproveitar os produtos de segurança do data center orientados por políticas, escaláveis e resistentes para possibilitar eficiências significativas para suas equipes de segurança. O tempo gasto pela equipe ao tentar monitorar e identificar ameaças à segurança pode ser redirecionado para outras atividades mais relevantes. As soluções de segurança orientadas por políticas ajudam as empresas a captar os benefícios da eficiência da automação, e a centralização das soluções de segurança de data center permite a identificação mais consolidada e eficiente das ameaças e dos esforços de correção. Como resultado, a equipe de segurança de TI recupera o tempo gasto, gerenciando suas soluções de segurança e consolidando as informações de partes separadas das arquiteturas de segurança do data center.

A eficácia da segurança tem a mesma importância para o gerenciamento. As soluções devem ser capazes de detectar tanto as ameaças conhecidas, como as desconhecidas, além de auxiliarem na correção. As empresas compreendem cada vez mais que precisam das soluções de segurança para respaldar políticas proativas com o objetivo de gerenciar ameaças, em vez de direcionar seus recursos para políticas reativas. Ao identificar mais ameaças à segurança do Data center, antes de elas causarem interrupções ou problemas, as empresas podem conquistar eficiências comerciais e da equipe de segurança.

A equipe de TI gasta menos de seu tempo respondendo aos incidentes e lidando com o trabalhoso processo de limpeza, quando identifica e lida com ameaças à segurança de forma proativa. E pode direcionar seus recursos para tarefas criadas para ampliar a produtividade da empresa, como teste e desenvolvimento de novas aplicaçõe e serviços. Ter uma solução sólida de segurança do data center é um componente importante para ajudar a equipe de TI a identificar ameaças à segurança e evitar invasões e infecções, enquanto a análise avançada pode ser aproveitada para limitar o impacto dos eventos sobre os usuários, quando ocorrerem. Ao limitar a frequência, em que ocorrem os eventos de segurança, as empresas não só podem reduzir proporcionalmente o tempo que a equipe gasta na resposta ao incidente, mas também podem reduzir o fardo das responsabilidades associadas, como atender às exigências de auditoria.

Além disso, as soluções de segurança do data center melhoram a segurança e o desempenho dos aplicativos comerciais, para que os usuários finais sejam mais produtivos. Como os usuários finais dependem bastante do desempenho e da disponibilidade dos aplicativos comerciais, que são frequentemente aplicativos desenvolvidos de forma personalizada, a produtividade aumenta quando há menos e mais curtas interrupções do serviço nesses aplicativos. E, também, as empresas que confiam na segurança da infraestrutura fundamental de TI, como data centers, estão frequentemente mais dispostas a explorar novas oportunidades de negócios. Isso pode ajudá-las a captar mais receita e implementar estratégias comerciais mais proativas e voltadas para o futuro. Além disso, a perda de receita como resultado da inoperância do data center é uma preocupação constante para muitas empresas; além de limitarem a inoperância planejada devido a incidentes de segurança, elas também podem reduzir as interrupções à receita, quando os sistemas e os aplicativos usados pelos clientes externos e internos saem do ar.

Exemplo de solução de segurança: arquitetura do data center seguro da Cisco

A abordagem da Cisco para oferecer recursos de segurança escaláveis e dinâmicos para ambientes do data center é interligada à maior parte de seu portfólio de produtos. As integrações entre os principais

produtos de rede, ofertas e computação unificada e a virtualização e portfólios SDN apresentam uma visão holística do data center. A segurança se tornou parte essencial da estratégia central da Cisco nos últimos 12 meses e, por isso, é parte importante do conjunto de soluções do data center. Os Cisco Validated Designs (CVDs), que proporcionam as melhores práticas para implantar os produtos de segurança da Cisco, de maneira fácil e efetiva, ajudam os clientes a implantar a combinação certa de soluções para lidar com seus ambientes específicos. A Solução de data center seguro da Cisco é oferecida de três maneiras: através do Cisco ASA 5585-X, FirePower Services e ASAv:

- O Adaptive Security Appliance 5585-X é o principal produto de firewall da Cisco. Criado especialmente para ambientes de data center, o ASA 5585-X aproveita uma arquitetura modular de dois blades para oferecer um rendimento de 40 Gbps, 350.000 conexões por segundo e 10 milhões de conexões concomitantes como uma ferramenta autônoma de 2 RU. Quando necessário, a densidade da porta pode ser aumentada através de módulos adicionais de I/O. O 5585-X também respalda cluster de até 16 aplicativos individuais para oferecer escalabilidade de rendimento linear de até 640 Gbps. O aplicativo 5585-X pode ser implantado como um firewall de camada 2 ou 3 tradicional e um concentrador de VPN, ou utilizar os FirePower Services para recursos mais avançados.
- Os FirePOWER Services para firewalls ASA, ou ferramentas autônomas do FirePOWER, oferecem detecção avançada de ameaças em vários casos, inclusive o data center. IPS de próxima geração (NGIPS) e Proteção avançada contra malware (AMP) protegem contra ataques direcionados utilizando malware personalizado. O FireSight Management Center correlaciona indicadores de comprometimento através de toda a infraestrutura para acelerar os esforços de correção e limitar o tempo que os invasores têm para acessar os recursos. Além do mais, os FirePOWER Services recebem informações sobre as ameaças através do grupo TALOS da Cisco (a principal equipe da Cisco na condução de pesquisas de segurança sobre malware, ataques e outras ameaças, apoiando outros grupos), para melhorar a detecção em toda a base de clientes.
- Por fim, a ASAv é uma instância completamente virtualizada da Cisco Adaptive Security Appliance física. A ASAv é um hipervisor independente, que proporciona visibilidade mais profunda do tráfego do data center entre máquinas virtuais e seu controle, independentemente da plataforma. Os perfis de política podem ser gerenciados através do Cisco Security Manager para garantir a coerência nos ambientes físico e virtual, ou através do Application Policy Infrastructure Controller (APIC) da Cisco para implantações da Application Centric Infrastructure (ACI). Através do APIC, as políticas de segurança podem ser associadas a aplicativos específicos e serviços de segurança que mudam à medida que mudam as demandas da rede.

Metodologia da IDC para quantificar os benefícios comerciais do data center seguro

Para compreender os benefícios comerciais à empresa do uso de produtos de segurança do data center, como soluções de arquitetura do Cisco Secure Data Center, a IDC transformou as principais métricas em economias financeiras com base na pesquisa realizada ao longo dos dois últimos anos com usuários desses tipos de produtos de segurança do data center. Para isso, a IDC analisou as principais métricas relacionadas aos esforços de TI, para manter a TI e os ambientes de data center seguros, incluindo: a capacidade das equipes de segurança de TI identificarem ameaças de forma proativa, o tempo necessário para as equipes de segurança de TI reagirem a essas ameaças, os custos com o tempo da equipe de segurança de TI e dos usuários finais associados a incidentes de segurança de data center, e outros custos que as empresas tiveram como resultado das quebras de

segurança do data center. A IDC agrupou os benefícios gerados pelo uso dos produtos de segurança do data center em três categorias principais de economia de custos: maior produtividade da equipe de TI, maior produtividade do usuário final causada pela redução do risco de segurança e maior produtividade do usuário final causada por eficiências operacionais. Normalizamos esses resultados, ao expressá-los como benefícios em dólares para uma empresa média com 1.000 usuários finais de TI.

Redução de custos

As empresas têm a possibilidade de alcançar vários tipos de economias de custos com produtos de segurança de data center. Quando compram produtos de segurança do data center que oferecem melhor visibilidade e desempenho, as empresas são capazes de reduzir os custos de produto relacionados à segurança, inclusive a quantidade de firewalls que adquirem. Além disso, a melhor integração entre os produtos de segurança e o hardware e o software que os apoia pode reduzir os custos de hardware e software. Por exemplo, a integração mais intensa dos produtos de segurança de data center possibilita às empresas ampliar a virtualização, reduzindo os custos. E também, os produtos de segurança do data center, que tiverem melhores desempenhos, poderão ajudar as empresas a reduzir os custos de largura de banda ou aprimorar seu desempenho de rede, sem ter que aumentar os gastos com a largura de banda. Além disso, a diminuição da quantidade de eventos de segurança graves relacionados ao data center reduz a exposição das empresas a multas, custos de reembolso e taxas jurídicas associadas às quebras de segurança.

Produtividade da equipe de TI

As equipes de segurança de TI são mais eficientes e produtivas com soluções de segurança de data center centralizadas e consolidadas à sua disposição. Elas podem gastar menos tempo monitorando soluções separadas e tentando obter informações úteis dessas soluções. Além disso, quando as soluções de segurança do data center limitam a quantidade de quebras e infecções que impactam o usuário, a equipe de segurança de TI pode gastar menos tempo tendo que lidar com inoperância relacionada à segurança e a incidentes de serviço de apoio. A maioria das empresas tem pequenas equipes de segurança de TI, então desviar a atenção desses membros da equipe das tarefas reativas para responsabilidades estratégicas inovadoras e com foco no futuro pode ser uma vantagem operacional significativa. Para quantificar as vantagens das economias de tempo de TI associadas ao uso de produtos de segurança do data center, a IDC multiplicou as economias de tempo por um salário médio anual de US$ 100.000.

Redução de riscos/Produtividade do usuário final

As soluções de segurança do data center, que identificam e reduzem mais ameaças de segurança, criam vantagens de produtividade em suas bases de funcionários. Ao aprimorar a segurança do data center, as empresas reduzem a frequência, com que as quebras de segurança e infecções impactam a disponibilidade de aplicativos comerciais que são executados em seus data centers, além de minimizar o tempo necessário para reiniciar a operação desses aplicativos. Como resultado, os usuários finais, que dependem desses aplicativos, enfrentam menos interrupções e têm mais tempo de produtividade. A IDC calcula o impacto dos ganhos de produtividade do usuário e o tempo de maior disponibilidade dos aplicativos, programas e dados de que os usuários precisam para fazer seus trabalhos a um salário médio de US$ 67.500, escalado por um fator de produtividade para

compensar o fato de que os usuários podem continuar a trabalhar durante as interrupções causadas por eventos de segurança relacionados ao data center.

Resultados do valor comercial

A pesquisa da IDC sobre o uso dos produtos de segurança do data center pelas empresas mostra que elas podem gerar valor comercial ao limitar a quantidade de tempo produtivo perdido pelos usuários e equipe de TI devido às ameaças de segurança, e ao limitar os custos associados a essas ameaças. Apesar de os benefícios resultarem das operações das equipes de segurança de TI, eles são mais evidentes em termos de tempo gasto ao reagir a incidentes, tendo as empresas reduzido o tempo de reação a incidentes em 62,9%, em média. As empresas também se beneficiam dos produtos de segurança do data center ao reduzir o tempo necessário para realizar auditorias de segurança (28,2% menos) e para gerenciar e manter os esforços de segurança (15% mais eficiente).

TABELA 1

Melhorias relacionadas ao uso dos produtos de segurança do data center

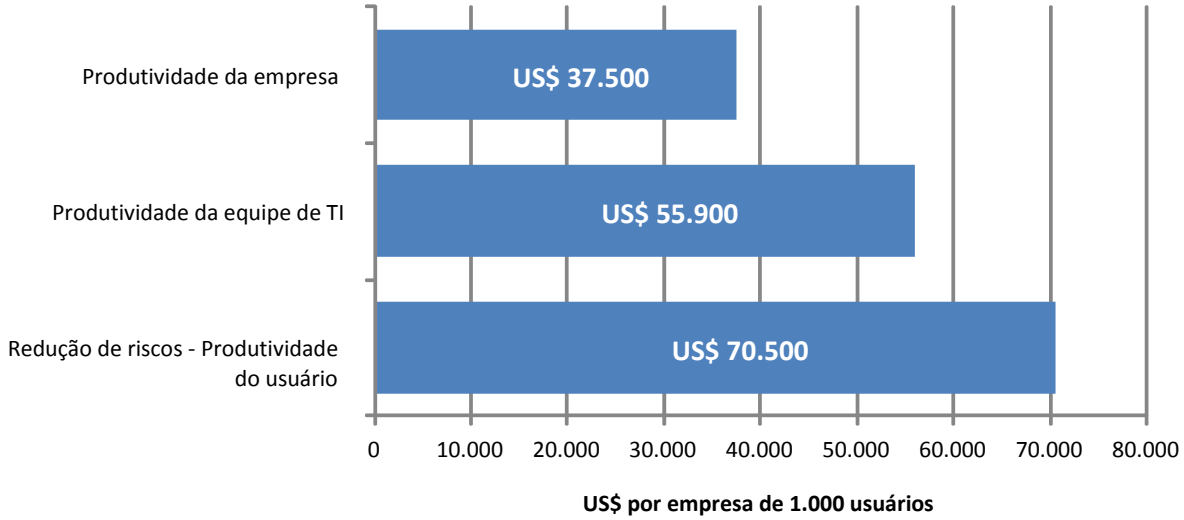
Benefícios de produtividade da equipe de TI	
Redução do tempo de gerenciamento da segurança	15%
Redução do tempo de reação a incidentes	62,9%
Redução do tempo de auditorias de segurança	28,2%
Benefícios da redução de riscos	
Redução do tempo de inoperância	51,9%

Fonte: IDC, 2014

A pesquisa da IDC demonstra que uma empresa de 1.000 usuários, que emprega soluções de segurança do data center, pode alcançar benefícios de produtividade do usuário resultantes de menos quebras, infecções e inoperâncias que impactam o usuário em US$ 70.500 ao ano. Essas soluções de segurança do data center também criam eficiências e economias de tempo para a equipe de TI equivalentes em média a US$ 55.900 ao ano para uma empresa de 1.000 usuários. Além disso, ao impulsionar as eficiências operacionais, que resultam na captação de mais receita, as soluções de segurança do data center podem proporcionar, em média, um adicional de US$ 37.500 em benefícios para uma empresa de 1.000 usuários por ano.

FIGURA 1

Benefícios típicos para empresas de 1.000 usuários, ao limitar o impacto dos incidentes de segurança em operações do data center



Fonte: IDC, 2014

Sobre a IDC

A International Data Corporation (IDC) é a empresa líder em inteligência de mercado, consultoria e eventos nos mercados de tecnologia da informação, telecomunicações e mercados de consumo em massa de tecnologia. A IDC ajuda profissionais de TI, executivos e a comunidade de investidores a tomar decisões de compras de tecnologia e estratégia de negócios baseadas em fatos. Mais de 1.100 analistas da IDC oferecem conhecimento local, regional e global sobre as tendências e oportunidades de tecnologia e do setor em mais de 110 países. Há 50 anos, a IDC oferece informações estratégicas para ajudar nossos clientes a alcançarem seus objetivos de negócios. A IDC é uma subsidiária da IDG, a principal empresa do mundo em mídia, pesquisa e eventos de tecnologia.

Sede global

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com