Akamai

GUIA DO COMPRADOR

Como selecionar um gateway Web seguro na nuvem

Proteja a equipe de trabalho remota e simplifique a segurança empresarial

Sumário

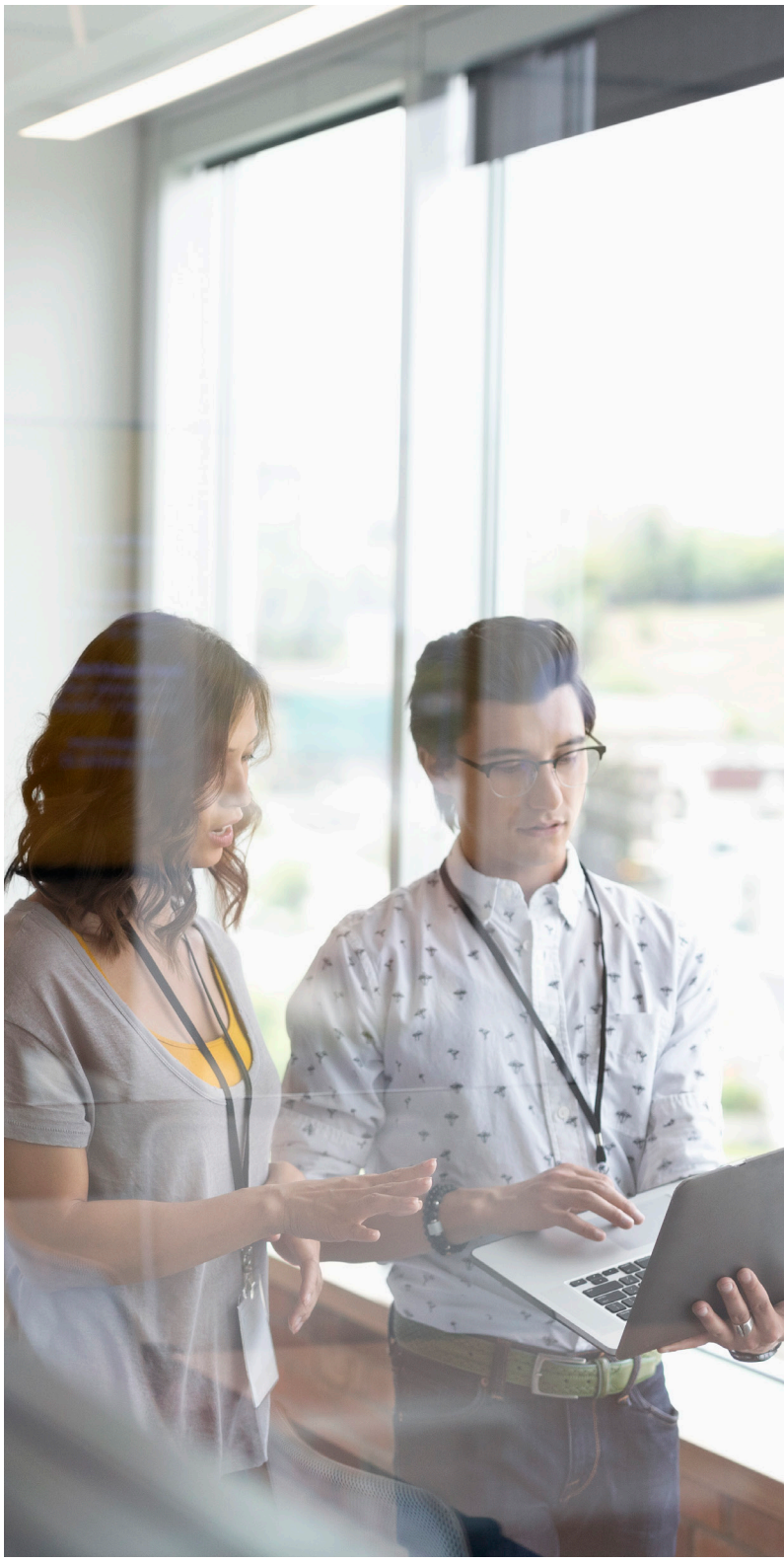
Proteção da empresa moderna: repense o backhaul do data center

Computação em nuvem, SaaS (software como um serviço), mobilidade e arquiteturas atualizadas de rede revolucionaram as práticas empresariais. Mas elas também criaram o pior cenário para as equipes de TI que tentam proteger a equipe de trabalho sem limitar o valor dessas novas tecnologias. Agora, há um novo desafio: Independentemente de onde as empresas estavam na transformação digital, muitas tiveram que se adaptar rapidamente para oferecer suporte ao aumento drástico de usuários remotos em 2020.

Um gateway Web seguro é um componente essencial para proteger uma equipe de trabalho corporativa, mas muitas empresas ainda estão usando equipamentos físicos implantados em data centers. Esse hardware requer manutenção, atualizações e gerenciamento contínuos e usa o complexo backhaul de tráfego para inspecionar e controlar o tráfego da Web, o que acaba degradando o desempenho.

As organizações precisam de uma abordagem moderna e simplificada para proteger essa nova realidade de um ambiente corporativo distribuído. A solução: Elimine os equipamentos físicos e mova o recurso de gateway Web seguro para a nuvem.

Este guia do comprador descreve os benefícios dos gateways Web seguros baseados na nuvem e quais recursos devem ser procurados em uma tecnologia de gateway Web moderno.



O aumento do trabalho remoto cria novas demandas de TI e segurança

Na última década, as organizações têm aumentado suas forças de trabalho remotas constantemente. Essa tendência só se acelerou em meio ao despertar da COVID-19, e espera-se que continue por muito tempo depois da pandemia. O Gartner descobriu que, após o término da pandemia, 74% dos CFOs entrevistados moverão pelo menos 5% da equipe de trabalho que, antes, trabalhava no local para cargos permanentemente remotos.[1]

Ao mesmo tempo, o número de ataques direcionados sofisticados, como phishing, ransomware e malware, cresceu rapidamente. 53% dos entrevistados em uma pesquisa recente disseram ter testemunhado um aumento na atividade de phishing desde o início da pandemia da COVID-19.[2] Um recente comunicado do Departamento do Tesouro dos EUA informou que a demanda por pagamentos de ransomware aumentou durante a pandemia da COVID-19, conforme os ciberagentes passaram a visar a sistemas online que as pessoas usam para continuar realizando negócios.[3]

Tradicionalmente, as organizações protegiam o acesso à Internet para os usuários locais das matrizes e filiais e para os funcionários remotos instalando equipamentos de segurança, como gateways Web seguros, em seus data centers. Em seguida, elas faziam o backhaul de todo o tráfego da Web para um local central para inspeção e controle.

As empresas têm usado esses gateways Web seguros para filtrar o malware indesejado do tráfego da Web iniciado pelo usuário, impedir que os usuários acessem websites mal-intencionados e aplicar políticas corporativas e regulamentares.

Originalmente, essas soluções de gateway eram projetadas e implantadas em ambientes onde a maioria dos funcionários usava dispositivos gerenciados pela empresa em suas mesas. Mas, à medida que o número de usuários que trabalha remotamente e em filiais cresceu, e mais tráfego foi transmitido à Internet pública para acessar aplicações de SaaS, as organizações começaram a instalar vários gateways Web seguros redundantes no data center central para manter um desempenho satisfatório. A compra e o gerenciamento desses equipamentos tornaram-se cada vez mais complexos, caros e demorados.

> **"A porcentagem do orçamento de TI gasto em data centers diminuiu nos últimos anos e, agora, representa apenas 17% do total."**
>
> — Gartner, dados das principais métricas de TI de 2019

Como alternativa, as organizações adicionaram equipamentos de gateways Web seguros às filiais, enquanto faziam o backhaul do tráfego para todos os usuários remotos. Essa redundância gerou a proliferação adicional de equipamentos e seus custos associados, além de uma implantação e um gerenciamento trabalhosos.

Também ficou cada vez mais difícil manter políticas consistentes de segurança em muitos locais. Mesmo quando as organizações implantavam equipamentos virtualizados para reduzir a proliferação de equipamentos, elas ainda tinham que implantar e gerenciar hardware extra.

Uma terceira abordagem foi a implantação híbrida, na qual as organizações continuavam usando gateways Web seguros no local para as principais localizações e enviavam o tráfego da Web das filiais para um gateway Web seguro baseado na nuvem, isso enquanto faziam o backhaul do tráfego dos funcionários remotos. Essa abordagem preservou os investimentos de hardware feitos em equipamentos locais. No entanto, ela acrescentou complexidade, já que as organizações acabaram gerenciando sistemas diferentes. Além de os equipamentos extras e o gerenciamento adicional serem muito mais caros que uma abordagem de nuvem pura, também era difícil manter políticas consistentes em sistemas locais e baseados na nuvem.

> **O Gartner prevê que, até 2025, 80% das empresas fecharão seus data centers tradicionais.[4]**

Para piorar as coisas, mesmo quando as organizações adotaram essas soluções cada vez mais complexas, elas começaram a enfrentar uma escassez de recursos de segurança cibernética. Um estudo da (ISC)[2] descobriu que um aumento de 62% seria ideal para preencher a atual escassez de profissionais de segurança necessários nos Estados Unidos.[5]

Por que usar um gateway Web seguro baseado na nuvem?

As organizações precisam de uma abordagem moderna para a segurança na Web que se compare à estratégia de nuvem das empresas, que permita e dê conta do trabalho remoto. Um gateway Web seguro baseado na nuvem proporciona às organizações um alto nível de segurança e, ao mesmo tempo, reduz a complexidade, conectando-se diretamente à Internet para evitar a necessidade de vários equipamentos e de fazer backhaul.

Com um gateway Web seguro baseado na nuvem, as organizações podem se beneficiar de:

Menor complexidade da segurança: Como um serviço na nuvem, esses gateways Web seguros eliminam a necessidade de implantar hardware ou equipamentos virtuais e de configurar, gerenciar e substituir/atualizar hardware a cada três anos.

Menos gargalos de desempenho: Um gateway Web seguro baseado na Internet elimina a necessidade de adicionar equipamentos extras para lidar com mais cargas de tráfego da Web e níveis crescentes de tráfego criptografado. Os clientes podem simplesmente incluir serviços adicionais, conforme necessário, com impacto mínimo sobre o desempenho.

Backhaul/Hairpinning menos dispendiosos do tráfego: Os gateways Web seguros baseados na nuvem aplicam segurança ao tráfego da Web, sem fazer backhaul do tráfego, para permitir a conexão direta com a Internet, o que reduz os custos de rede do Multiprotocol Label Switching.

Melhor eficiência da equipe de segurança: Como os gateways Web seguros na nuvem não exigem manutenção contínua de hardware ou software, a escassa equipe de segurança tem mais tempo para se concentrar em outras medidas proativas de segurança.

Políticas consistentes de segurança: As organizações podem usar políticas gerenciadas centralmente, mas implantadas globalmente, para todos os usuários que se conectam a partir de qualquer dispositivo. Mesmo que a organização tenha políticas diferentes para diferentes regiões, ela pode usar a mesma interface de usuário para gerenciar todas elas.

Principais requisitos de um gateway Web seguro

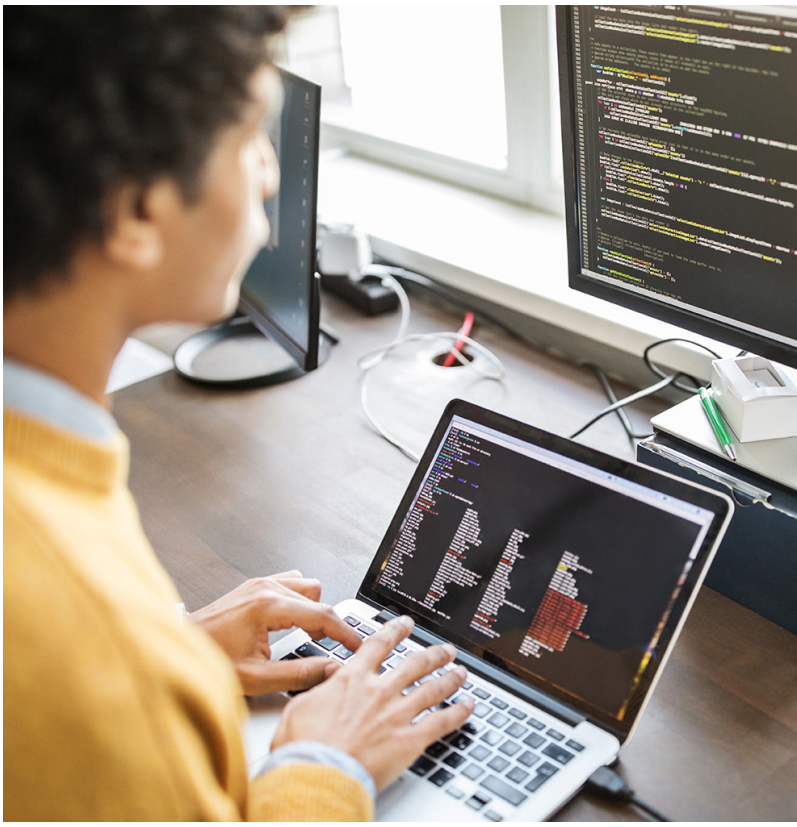
Ao selecionar um gateway Web seguro baseado na nuvem, é importante reconhecer que a segurança é o requisito principal. Muitos gateways Web seguros preexistentes incluem recursos que resolvem problemas que não existem mais. Por exemplo, eles incluem o controle de largura de banda, que foi projetado para um momento em que a largura de banda era cara. Ou impedem que os funcionários usem o YouTube ou o Facebook durante o horário de trabalho. Atualmente, esses recursos não são mais necessários porque a largura de banda é abundante e tantas pessoas usam seus dispositivos móveis que as organizações não estão mais preocupadas em bloquear esses serviços em dispositivos corporativos.

Hoje, as organizações precisam de um gateway Web seguro baseado na nuvem, projetado especificamente para lidar com as preocupações modernas de segurança. Em particular, a solução deve seguir uma estratégia de defesa profunda que utilize várias medidas de segurança para oferecer o mais alto nível de proteção. Essa abordagem deve abranger todos os ângulos de segurança cibernética e apresentar medidas de segurança redundantes. Assim, se uma linha de defesa for comprometida, camadas adicionais de defesa estarão em vigor para impedir que ataques entrem pelas rachaduras. Essa abordagem em camadas garante que ameaças como malware, ransomware e phishing sejam bloqueadas mais cedo e mais rapidamente, e antes que o dispositivo do usuário seja comprometido.

Um gateway Web seguro que implanta uma estratégia de defesa profunda deve oferecer os seguintes recursos de segurança:

Avaliação de todas as solicitações de DNS e URL

Uma solução de gateway Web seguro baseado na nuvem deve avaliar todas as solicitações de URL e



DNS em relação à inteligência de ameaças em tempo real e bloquear solicitações mal-intencionadas logo no início da cadeia de eliminação. Se o gateway Web seguro puder bloquear ameaças antes que uma conexão de saída seja feita, o recurso da Web não precisará abrir nem inspecionar qualquer conteúdo exibido. Essa eficiência evita um processo com uso intenso de recursos de computação e reduz a quantidade de tráfego que o gateway Web seguro deve analisar na fase de carga útil. O resultado? Melhor desempenho geral do gateway Web seguro.

A inteligência de ameaças deve oferecer proteção contra malware, ransomware, phishing e exfiltração de dados baseada em DNS com baixa taxa de transferência. Ela também deve ser desenvolvida especificamente para oferecer uma proteção atual, relevante e que apresente baixas taxas de falsos positivos.

Várias técnicas de análise de carga útil

Como todas as ameaças são diferentes e, portanto, não há uma técnica ou abordagem única de detecção que possa abranger todos os tipos de malware, a solução de gateway Web seguro deve incluir vários mecanismos de análise de malware. Esses mecanismos devem verificar cargas úteis de HTTP e HTTPS em linha ou offline usando várias técnicas de identificação, como identificação com e sem assinatura, aprendizado de máquina e área de segurança. Essa análise oferecerá proteção abrangente de zero-day o contra arquivos possivelmente mal-intencionados, como arquivos executáveis e de documentos.

Detecção de phishing de zero-day

Os funcionários remotos continuam enfrentando o aumento dos ataques de phishing desde o início da pandemia da COVID-19. Agentes mal-intencionados iniciam ataques de phishing por e-mail, mídias sociais e aplicações de mensagens instantâneas, além de canais de colaboração e compartilhamento online de arquivos, para roubar credenciais corporativas que dão a eles acesso à rede das empresas. A partir daí, os invasores podem se mover lateralmente para encontrar e exfiltrar dados e propriedades intelectuais ou para divulgar campanhas de ransomware.

Para identificar e bloquear o acesso a uma página de phishing, a maioria dos fornecedores de segurança faz o seguinte:

1. **Observa o tráfego incomum que atinge um domínio**
2. **Analisa esse domínio**
3. **Determina se ele é um domínio de phishing**
4. **Adiciona-o à lista de bloqueios**
5. **Envia a atualização da lista de bloqueio para os clientes**

Esse processo pode levar horas. E, pior ainda, os criminosos cibernéticos de hoje usam kits de phishing para criar e lançar facilmente ataques de curta duração, o que dificulta ainda mais a detecção. Quando o domínio ou URL de phishing é encontrado, o ataque já terminou. De fato, quanto mais sofisticado e direcionado for o ataque de phishing, menor será a duração dele.

Mas, embora essas campanhas possam acabar rapidamente, um mecanismo avançado de detecção de phishing de zero-day pode identificá-las e bloqueá-las. Os elementos recorrentes desses ataques baseados em kits podem ser vistos no código das páginas de phishing. Usando essas informações, é possível identificar "impressões digitais" dessas páginas que permitem uma identificação precisa.

Uma solução de gateway Web seguro deve incluir um mecanismo de detecção de phishing de zero-day que possa analisar as páginas da Web solicitadas e compará-las com as "impressões digitais" das páginas de phishing observadas anteriormente.

Inspeção de tráfego criptografado

A Internet é um canal inerentemente inseguro para a transferência de dados. Como resultado, agora, a criptografia do tráfego da Web é onipresente para impedir as tentativas dos invasores de interceptar, falsificar ou adulterar o tráfego. TLS (Transport Layer Security) é o padrão de criptografia de fato para entregar navegação segura na Web. O TLS cria um túnel seguro entre dois endpoints, como um navegador cliente e um servidor da Web.

> **A porcentagem do tráfego da Web criptografado na Internet vem aumentando constantemente, de cerca de 50% em 2014 para 80% a 90% hoje. A maioria (96%) dos 100 maiores sites do mundo usa HTTPS por padrão.**
>
> — Relatório de transparência do Google, 2020

Mas nem todo tráfego de HTTPS é benigno. Os invasores e criadores de malware também usam criptografia para ocultar suas atividades, impedir que os usuários acessem arquivos (por meio de ransomware) e proteger a comunicação de rede mal-intencionada. Um estudo recente descobriu que quase um quarto dos malwares que fizeram uma conexão à Internet usaram TLS para se comunicar.[6]

Para inspecionar e controlar proativamente o tráfego da Web de HTTPS, é necessário olhar dentro do túnel seguro e examinar o tráfego criptografado, usando um servidor proxy (intermediário confiável). O servidor proxy deve descriptografar o tráfego de HTTPS em texto sem formatação, analisá-lo, criptografar o tráfego novamente e, em seguida, criar outra conexão segura em uma técnica chamada MITM (machine-in-the-middle). O MITM inspeciona os URLs solicitados para determinar se eles são seguros ou mal-intencionados, oferece visibilidade sobre o tráfego criptografado por TLS e protege a empresa contra ameaças, enquanto preserva a confidencialidade e a integridade do tráfego para os websites de origem.

As inspeções do MITM exigem uma capacidade considerável de processamento. Portanto, a navegação na Web pode ficar lenta devido à latência. O gateway Web seguro deve oferecer serviços que melhorem o desempenho das aplicações. Ele deve incluir uma rede globalmente distribuída de servidores e software inteligente, localizada próxima aos usuários e data centers do mundo todo, para permitir otimizações da Web que melhorem o desempenho e a disponibilidade das aplicações.

Além disso, a técnica MITM deve verificar se o fornecedor do gateway Web seguro na nuvem mantém uma lista centralizada de domínios e URLs que não funcionam corretamente e que devem ser contornados. O gateway Web seguro na nuvem também deve poder contornar a inspeção do MITM em busca dos tipos específicos de conteúdo confidencial da Web, como nos setores de serviços financeiros e de cuidados com a saúde.

Prevenção integrada contra perda de dados

Impedir proativamente a perda de PII (informações de identificação pessoal) e outros dados empresariais confidenciais é algo essencial, considerando-se o potencial de prejuízos financeiros ou danos à reputação. O gateway Web seguro na nuvem deve incluir uma prevenção integrada contra perda de dados que seja fácil de configurar e rápida de implantar. Os dicionários atualizados com frequência devem abranger normas de proteção e privacidade de dados, como PII, PCI-DSS e HIPAA, e as organizações devem conseguir criar dicionários personalizados facilmente.

Identificação e gerenciamento de TI sombra

Os usuários têm centenas de milhares de aplicações ao seu alcance para baixar, instalar e usar em dispositivos gerenciados sem que a equipe de segurança empresarial saiba disso. Mas o uso de aplicações não aprovadas pode expandir significativamente a superfície de ataque da organização e aumentar seu perfil de risco.

> **A empresa média usa mais de 1.295 aplicações e serviços de nuvem. Mais de 95% deles não são gerenciados, sem direitos de administração de TI.**
>
> — Cybersecurity Insiders,
> Relatório de segurança na nuvem, 2019

Um gateway Web seguro na nuvem deve poder identificar quais aplicações estão sendo usadas, detectar quantos usuários instalaram aplicações específicas e destacar as aplicações que podem apresentar um risco de segurança possivelmente grave. Depois de identificada, a solução deve poder bloquear toda a aplicação ou operações específicas dela (por exemplo, permitir uploads, mas não downloads).

Proteção em qualquer lugar para qualquer dispositivo

A tendência de flexibilidade do estilo de trabalho aumentou significativamente na última década. Agora, os usuários trabalham em qualquer lugar, em qualquer dispositivo. E, como resultado do trabalho em casa durante a pandemia, 59% da computação de usuário final para empresas estão migrando para dispositivos móveis, aumentando ou substituindo o uso de computadores e notebooks. Prevê-se que essa mudança continue mesmo após o retorno ao trabalho no escritório.[7]

A migração para dispositivos móveis e o aumento do uso das redes Wi-Fi podem representar uma rachadura na postura de segurança de qualquer organização. As empresas precisam conseguir aplicar um nível de segurança uniforme e universal, sem comprometer o desempenho dos dispositivos.

Um gateway Web seguro na nuvem deve identificar, bloquear e aliviar proativamente ameaças direcionadas como malware, ransomware, phishing, exfiltração de dados de DNS e ataques de zero-day em qualquer dispositivo (iOS, Android OS, Chrome OS), em qualquer rede que o usuário ingressar. A solução de gateway deve oferecer controles onipresentes e gerenciamento simplificado globalmente, enquanto mantém o desempenho ideal dos dispositivos.

Acesso seguro a todas as aplicações empresariais

Um gateway Web seguro na nuvem protege os usuários e os dispositivos contra malware à medida que eles acessam a Internet pública. Mas, para uma empresa, essa é apenas uma peça do quebra-cabeça de segurança.

Para criar uma abordagem abrangente de segurança para toda a empresa, as organizações também precisam proteger as aplicações controladas e gerenciadas pela empresa (independentemente de elas residirem no data center corporativo ou em um ambiente de IaaS) contra atos abomináveis.

Os ataques de phishing empresarial estão em ascensão

Ataques observados de março a outubro de 2020

64%

AUMENTO NOS ATAQUES CONTRA

EMPRESAS

17%

AUMENTO NOS ATAQUES CONTRA

CONSUMIDORES

Fonte: Gateway Web seguro Akamai Enterprise Threat Protector

As ferramentas tradicionais de segurança de rede protegem o perímetro da rede, mas, se os invasores violarem o perímetro (por exemplo, roubando credenciais de usuário ou instalando malware no dispositivo de um usuário), eles poderão se mover livremente na rede.

As organizações precisam de um gateway Web seguro na nuvem que também ofereça uma tecnologia de ZTNA (Zero Trust Network Access) para proteger aplicações corporativas. ZTNA é um componente essencial da adoção da segurança Zero Trust, concedendo aos usuários o acesso somente a aplicações específicas (não a redes ou segmentos inteiros) com base na identidade do usuário. A solução protege a identidade do usuário por meio da integração ao gerenciamento de identidade e acesso, da MFA (autenticação de vários fatores) e das tecnologias de login único. Ao usar uma ferramenta de ZTNA, as organizações eliminam a complexidade do gerenciamento seguro de dispositivos ou da manutenção de uma conectividade complexa de rede de longa distância ou de rede privada virtual. Depois de devidamente autenticados, os usuários recebem acesso somente às aplicações e aos dados de que precisam, reduzindo a zero a superfície de ataque das aplicações e minimizando o risco de movimentação

lateral. Quando as organizações avaliam um gateway Web seguro na nuvem, elas devem considerar os recursos do serviço de ZTNA do fornecedor. O serviço pode oferecer acesso a aplicações modernas da Web, bem como a aplicações preexistentes que não são da Web? O serviço pode se integrar ao serviço existente do provedor de identidade da organização? Ele oferece suporte a MFA?

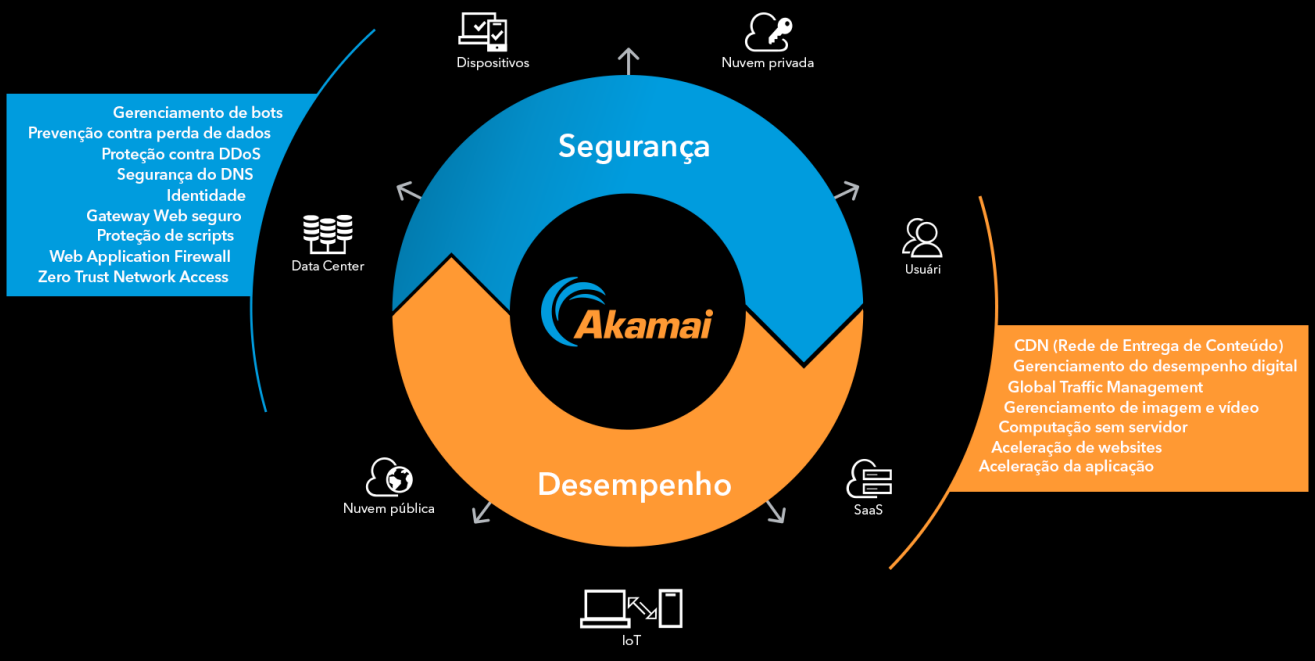
O gateway Web seguro deve se integrar ao serviço de ZTNA e funcionar em conjunto com ele para que, se um dispositivo for comprometido, ele seja impedido de acessar qualquer aplicação corporativa. Os logs de um gateway Web seguro podem ampliar outros sinais de ameaça para apresentar um panorama mais preciso da postura de segurança de um dispositivo. Por exemplo, se o dispositivo estiver acionando servidores de comando e controle, a solução deve usar isso como um sinal para limitar o acesso às aplicações até que o dispositivo seja corrigido.

Ao adicionar o gateway Web seguro e os recursos de ZTNA, as organizações avançam um passo rumo à adoção de uma estrutura SASE (Secure Access Service Edge). A SASE afasta o centro das iniciativas de segurança de uma organização das arquiteturas de segurança centradas em equipamentos de hardware e data center que não funcionam mais no ambiente empresarial e profissional altamente distribuído de hoje. Em vez disso, ela entrega acesso baseado em políticas de acordo com a identidade do usuário e/ou dispositivo. A SASE também oferece uma ampla variedade de controles adicionais de segurança, como Web Application Firewall, segurança de APIs, gerenciamento de bots e proteção distribuída contra negação de serviço para aplicações voltadas para a Web.

> **O ZTNA melhora a flexibilidade, a agilidade e a escalabilidade do acesso a aplicações, permitindo que as empresas digitais prosperem sem expor aplicações internas diretamente à Internet, o que reduz o risco de ataques.**
>
> — Gartner, Market Guide for Zero Trust Network Acces, Steve Riley, Neil MacDonald, Lawrence Orans, 8 de junho de 2020

Além disso, os controles de segurança são entregues na plataforma SASE na Internet a um passo do usuário, para oferecer acesso de baixa latência a usuários, dispositivos e serviços de nuvem em qualquer lugar.

SASE da Akamai entregue na nuvem



Desempenho ideal

Embora a segurança seja fundamental, ela não pode comprometer a experiência do usuário com desempenho lento. Além de oferecer uma abordagem de defesa profunda à segurança, um gateway Web seguro baseado na nuvem deve entregar os serviços acima sem introduzir latência.

Para evitar latência, o gateway Web seguro na nuvem deve ser implantado globalmente com pontos de presença próximos ao local de conexão de todos os usuários. Afinal de contas, não faz sentido substituir um tipo de backhaul por outro.

A plataforma na nuvem também deve ser dimensionada rapidamente para evitar afetar a experiência do usuário final, mesmo em condições de pico. Essa capacidade é particularmente importante quando se trata de inspecionar o tráfego de HTTPS, que está crescendo exponencialmente e, em última análise, irá compor cerca de 100% do tráfego da Web. A inspeção do tráfego criptografado com impacto mínimo sobre os usuários finais é essencial, já que a grande maioria do malware agora é entregue via HTTPS. A plataforma também deve oferecer um SLA (Acordo de Nível de Serviço) de 100% de disponibilidade.

> **Agora, os usuários do Office 365 representam mais da metade dos 81% do total de organizações que mudaram para serviços de nuvem.[8]**

Integração com o Office 365: É especialmente importante garantir um alto nível de segurança e desempenho do Microsoft Office 365, pois muitas organizações dependem desse serviço como seu pacote essencial de produtividade. Um desafio ao implantar um gateway Web seguro na nuvem é que o O365, como muitas outras aplicações populares de SaaS, tem um desempenho ruim quando os usuários acessam suas aplicações por meio de um proxy de encaminhamento, que executa a inspeção MITM de TLS.

Para evitar afetar o desempenho do O365, é fundamental que o gateway Web seguro na nuvem seja entregue por meio de uma plataforma global de Edge que possa:

- Usar o IP de origem da solicitação para direcionar a solicitação ao data center do Microsoft O365 mais próximo do ponto de vista geográfico, em vez de fazer o backhaul de soluções de DNS que direcionariam a solicitação ao data center mais próximo do solucionador de DNS corporativo. Por exemplo, um usuário que acessar o O365 de Singapura e for encaminhado a um servidor do O365 em Nova York terá uma experiência de usuário terrível
- Certificar-se de que as locais de servidor do gateway web seguro estejam próximos dos data centers do Microsoft O365 e que, idealmente, esses servidores e data centers estejam interconectados
- Oferecer uma configuração de otimização do tráfego do O365 com um clique que use uma lista de domínios e endereços IP do O365 publicados e atualizados pela Microsoft. As solicitações a esses domínios devem ser enviadas diretamente aos servidores O365 de acordo com as recomendações da Microsoft, o que economiza tempo e esforço, eliminando a necessidade de atualizar firewalls e outros produtos de segurança manualmente quando a Microsoft adicionar novos domínios ou endereços IP

Mova a segurança para a edge

As forças de trabalho remotas em rápido crescimento estão cada vez mais vulneráveis a ataques cibernéticos que, por sua vez, estão se tornando mais frequentes e graves. As melhores soluções de gateway Web seguro baseado na nuvem se concentrarão exclusivamente em atender a essas demandas modernas de segurança, entregando uma funcionalidade comprovada de defesa profunda. Elas também ativarão modelos modernos de segurança empresarial, como Zero Trust e SASE, protegendo o acesso à Internet para todos os usuários, independentemente de sua localização.

Um gateway Web seguro na nuvem e abrangente deve avaliar todas as solicitações de DNS e URL, oferecer várias técnicas de análise de carga útil, abordar o phishing de zero-day, inspecionar o tráfego criptografado, integrar a prevenção contra perda de dados, identificar e gerenciar a TI sombra e oferecer proteção em qualquer lugar para qualquer dispositivo, tudo isso enquanto apresenta um alto nível de desempenho e se integra às tecnologias de segurança de aplicações empresariais. Com uma solução assim, as organizações podem reduzir a complexidade da segurança, eliminar o dispendioso backhaul, melhorar a eficiência da equipe de segurança e oferecer suporte a políticas consistentes de segurança.

Saiba mais sobre o Secure Internet Access, o gateway Web seguro da Akamai baseado na nuvem, e inicie uma avaliação gratuita em akamai.com.

1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
2. https://www.helpnetsecurity.com/2020/09/02/phishing-attacks-pandemic/
3. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
4. https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/
5. https://www.brinknews.com/a-global-shortage-of-cybersecurity-professionals-leaves-businesses-at-risk/
6. https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
7. https://www.mobolize.com/2020/10/29/mobolize-announces-technology-partnership-with-akamai-to-enable-security-on-mobile-devices/
8. https://blog.goptg.com/microsoft-office-365-statistics#:~:text=According%20to%20Bitglass%2C%20usage%20of,the%20shift%20to%20cloud%20services