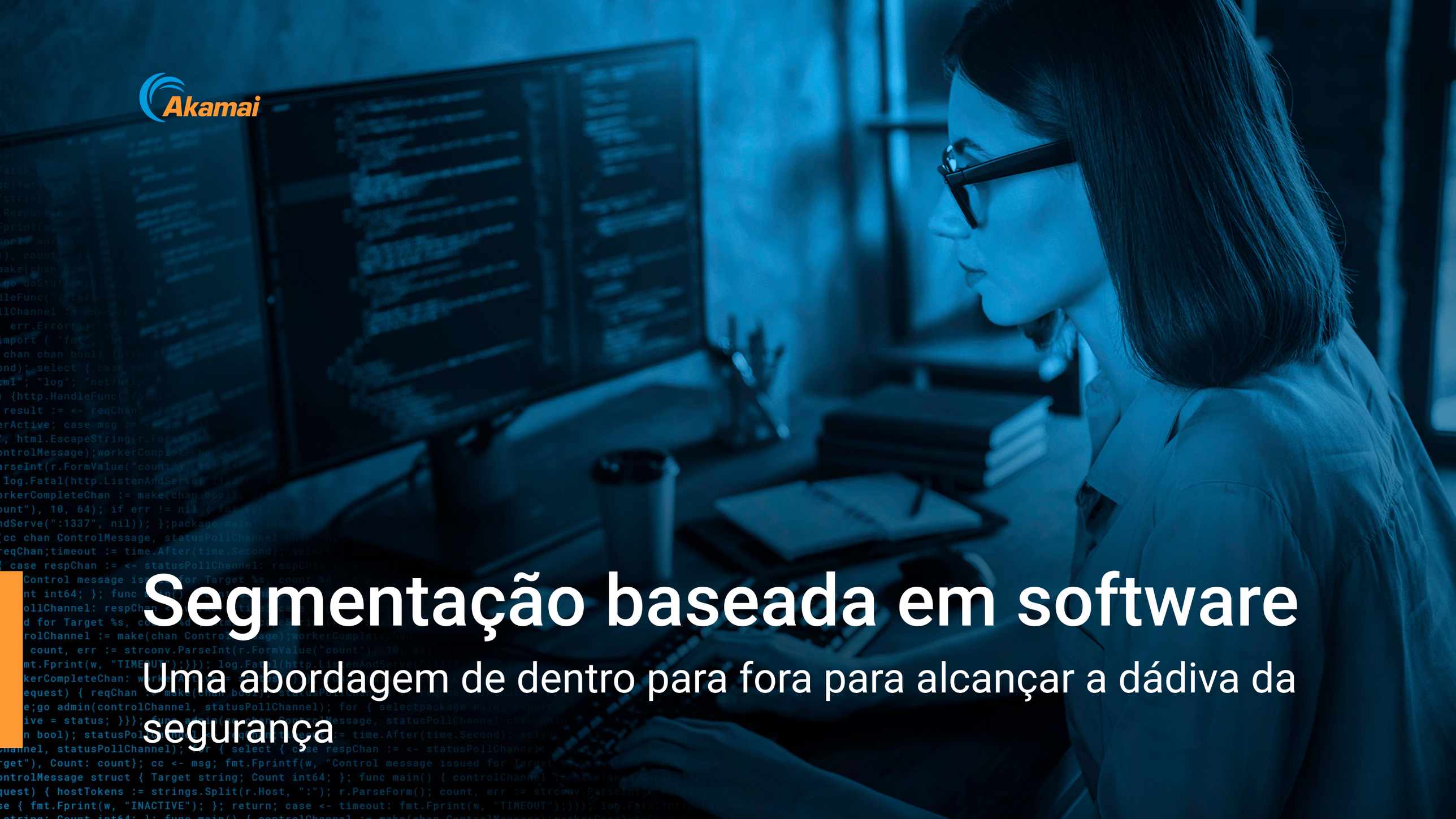


Segmentação baseada em software

Uma abordagem de dentro para fora para alcançar a dádiva da segurança

SUMÁRIO

Mude dos firewalls legados do passado	03
Resolvido! 3 problemas com firewalls legados	04
4 fundamentos da segmentação	09
Mito x realidade: 5 mitos de segmentação desmascarados	10
Reduzir o risco internamente	11
Sua lista de verificação Zero Trust: 6 maneiras de obter controle explícito	13
Últimas considerações	14

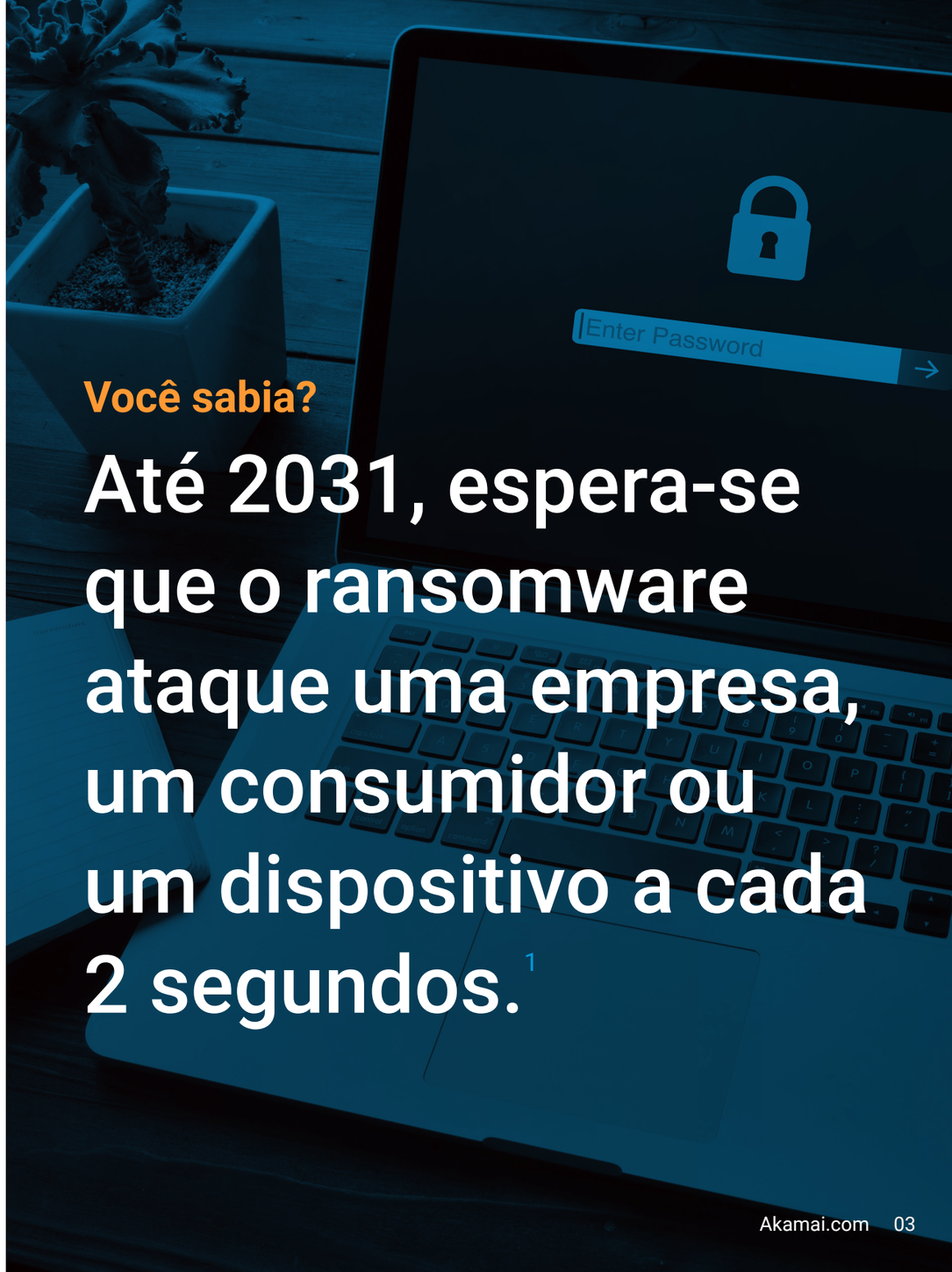
Mude dos firewalls legados do passado

A gente entende. Você está cansado de seus antigos firewalls locais. Os ambientes de TI e os requisitos de segurança estão agora anos-luz à frente do motivo para o qual foram originalmente criados. E o cenário de segurança virtual também evoluiu. Os métodos de ataque se tornaram mais sofisticados e há mais cibercriminosos do que nunca. Uma arquitetura de dispositivos com décadas de uso simplesmente não consegue dar conta dos mais recentes malwares, ataques de botnet, esquemas de phishing, engenharia social e extorsão de dados.

Mas, mesmo com sua miríade de problemas (eles são caros, imóveis e não têm visibilidade, para citar apenas alguns dos problemas), a realidade é que os firewalls antigos ainda serão necessários por algum tempo. Eles têm uma função importante no perímetro, lidam com o tráfego norte-sul e fornecem uma estrutura rígida ao redor da organização.

Mas os firewalls não conseguem gerenciar o tráfego leste-oeste nos data centers locais e na nuvem.

Este é um trabalho para a segmentação baseada em software.



Você sabia?

Até 2031, espera-se que o ransomware ataque uma empresa, um consumidor ou um dispositivo a cada 2 segundos.[1]

Resolvido!

3 problemas com firewalls legados

1. O problema: **falta de visibilidade**

   A falta de visibilidade do fluxo de dados dificulta a implementação e a manutenção das regras. Por isso, os firewalls geralmente têm conjuntos de regras extremamente longos e muitas delas são excessivamente permissivas ou desnecessárias.

A solução

Procure soluções que integram o mapa visual, a classificação de ativos e o mapeamento da dependência de aplicações com a criação e o gerenciamento de políticas.

Resolvido!

3 problemas com firewalls legados

2. O problema: os firewalls são difíceis de manter

Os proprietários de aplicações e os administradores de firewall raramente conhecem as portas IP e os protocolos apropriados que precisam para se comunicar. Portanto, o gerenciamento de firewalls se torna um processo iterativo de solução de problemas.

A solução

Em vez de enquadrar políticas em torno da "conexão" fixa da rede, como IPs e portas, baseie-as em atributos significativos, como o processo que a aplicação usa, nomes de domínio totalmente qualificados (FQDN) e na identidade do usuário. Dessa forma, os atributos permanecem os mesmos, e suas políticas continuam funcionando, mesmo que você faça uma alteração no data center ou mova a carga de trabalho para a nuvem.

Resolvido!

3 problemas com firewalls legados

3. O problema: firewalls sem agilidade

Todas as alterações feitas em um firewall geralmente exigem um tempo de inatividade programado. Quando o proprietário da aplicação precisa fazer uma alteração, ele pode ter que esperar uma semana ou mais para que a alteração seja revisada e implementada durante uma janela de manutenção.

A solução

As organizações de TI modernas mudaram do modelo de janelas de alterações para o modelo DevOps, em que as aplicações aparecem e se atualizam continuamente. Encontre uma solução tecnológica que possa ser automatizada com as mesmas ferramentas DevOps que você usa nas aplicações. Dessa forma, à medida que as aplicações evoluem continuamente, a abordagem de segurança se adapta junto com elas.

Você pode levar com você

Vamos falar sobre os procedimentos tradicionais. São complicados. E não são adaptáveis. A abordagem tradicional de gerenciar firewalls antigos se baseia na segmentação no local, e esse local não pode ser alterado com facilidade. Geralmente, ela se baseia em um endereço IP codificado ou roteado para um data center. Isso significa que você precisa mover fisicamente o que quer que queira proteger para detrás do firewall, um processo que consome muitos recursos, é avesso a riscos e lento. Migração para a nuvem? Visibilidade? Segurança adequada? Esqueça.

Deixe os firewalls antigos onde estão. Respire fundo e adote algo novo. A segmentação baseada em software pode ser facilmente implementada junto aos firewalls existentes e é adaptável. Com a segmentação baseada em software, você consegue fazer alterações em seu ambiente, data center e rede e definir políticas com base no que você vê. A carga de trabalho e as políticas podem aparecer em qualquer lugar: na nuvem, no data center, seja onde for. Além disso, você pode aplicar e adaptar sua política de segurança sem fazer alterações na rede e sem tempo de inatividade do sistema.

Revele seus segmentos internos

Você confiaria em algo que não consegue ver? Acreditamos que não. Mas é exatamente isso que você está fazendo ao estabelecer políticas de segurança por trás de um firewall. Você não consegue ver o que está dentro. É como olhar para um edifício e não conseguir ver as pessoas que estão no interior dele.

A segmentação baseada em software não é baseada no acaso. Ela divide as partes para que você fique totalmente ciente de todas as atividades em que suas cargas de trabalho estão envolvidas. Depois de saber o que está dentro do ambiente, você pode criar um plano e dividir os segmentos em algo significativo e eficaz com base nos seus casos de uso específicos.

Segurança além do perímetro

Os firewalls antigos simplesmente não foram criados para serem alterados. Embora eles tenham um objetivo importante no perímetro, como a proteção contra ataques DDoS e filtragem e inspeção de tráfego, é difícil fazer a segurança dentro da rede com firewalls. Por quê? Eles foram implantados como pontos de redução naturais, ou seja, cada atividade de segmentação vem com obstáculos operacionais, como a necessidade de alterar e remover redes e aplicações. Isso é tedioso e consome muitos recursos.

A segmentação baseada em software pode ajudar a superar esses desafios operacionais e permitir que você continue suas práticas de segurança além dos pontos de extremidade e dos perímetros. Primeiro, ela apresenta uma abordagem de firewall distribuído (em vez de um ponto de redução). Segundo, ela é centrada na carga de trabalho, ou seja, ela pode coletar dados do sistema host e aplicá-los na classificação de ativos e pode adotar uma abordagem mais granular das regras, como conteúdo e políticas no nível do processo. Em geral, a segmentação baseada em software é uma opção mais adaptável e granular de proteger ativos essenciais dentro da rede e requer menos esforço e recursos que os firewalls.

4 fundamentos da segmentação

A segmentação é mais importante do que nunca. As superfícies de ataque estão maiores. Ataques sofisticados, como ransomware, movem-se lateralmente após uma violação. Você precisa pensar sobre as dependências da aplicação além do perímetro. Mas a segmentação não é uma abordagem única.

Veja aqui quatro tipos comuns de segmentação, suas diferenças e por que você precisa deles.

1. Segmentação do ambiente

separa os sistemas em diferentes ambientes de desenvolvimento, como desenvolvimento, QA, Staging e produção. Essa é uma versão ampla da segmentação, com o objetivo final de separar sistemas em diferentes ambientes para garantir que o acesso seja limitado apenas aos usuários e às aplicações necessárias. Muitas iniciativas de conformidade exigem a garantia de que os sistemas que não são de produção não possam acessar os sistemas de produção.

2. A segmentação de rede

é uma prática de arquitetura que divide a rede em várias sub-redes, cada uma sendo seu próprio segmento de rede menor. A segmentação de rede oferece às operadoras de TI uma ferramenta para controlar melhor o tráfego de rede, aumentar o desempenho e melhorar a segurança.

3. Microssegmentação

é uma opção mais granular de segmentação usada para isolar as cargas de trabalho umas das outras e protegê-las individualmente. Isso inclui a capacidade de definir regras de segmentação para elementos como processos, contêineres, usuários, nomes de domínio e dispositivos. Essa é uma abordagem superior para controle do tráfego leste-oeste e proteção contra a movimentação lateral.

4. Segmentação baseada em identidade

é mais abrangente do que a microssegmentação, que protege um único ponto de extremidade, dispositivo, carga de trabalho ou contêiner, porque habilita regras dinâmicas que avaliam a identidade, que pode ser do usuário, do dispositivo ou do contexto, como parte da determinação de permitir ou não a comunicação. As políticas de segmentação baseadas em identidade podem ser baseadas em configurações granulares, não apenas IP ou porta, como tags, tipo de SO ou caraterísticas da aplicação.

Mito x realidade: 5 mitos da segmentação desmascarados

Mito 1

Os projetos de segmentação são muito complexos e demoram para serem concluídos.

Realidade: começar com visibilidade e uma compreensão clara do que está acontecendo em seu ambiente reduz o tempo para concluir um projeto de segmentação de meses para semanas ou até mesmo dias. As tecnologias modernas de segmentação também podem usar a IA para acelerar ainda mais o processo.

Mito 2

Os projetos de segmentação exigem alterações na infraestrutura de rede e tempo de inatividade.

Realidade: a segmentação baseada em software dissocia a segurança da infraestrutura, para que a segmentação seja realizada independentemente da infraestrutura subjacente, sem alterações ou tempo de inatividade.

Mito 3

A segmentação bloqueia o tráfego legítimo na minha rede.

Realidade: a visualização do seu ambiente e o uso de políticas de segmentação baseadas em software permitem enxergar o efeito que essas políticas terão nas suas atividades de negócios antes que a execução em tempo real seja ativada.

Mito 4

A segmentação inibe o acesso do usuário e introduz uma latência desnecessária.

Realidade: usar políticas de segmentação distribuídas e baseadas em software, em vez de forçar todo o tráfego por meio de pontos de redução de firewall específicos, elimina os pontos de estrangulamento da rede. E políticas mais precisas que reconhecem aplicações e identidades reduzem o risco de problemas acidentais de acesso do usuário.

Mito 5

Não consigo usar na nuvem as mesmas ferramentas de segmentação que uso no local.

Realidade: se você dissociar as políticas de segmentação da infraestrutura, as mesmas políticas usadas no data center também poderão funcionar na nuvem.

Akamai

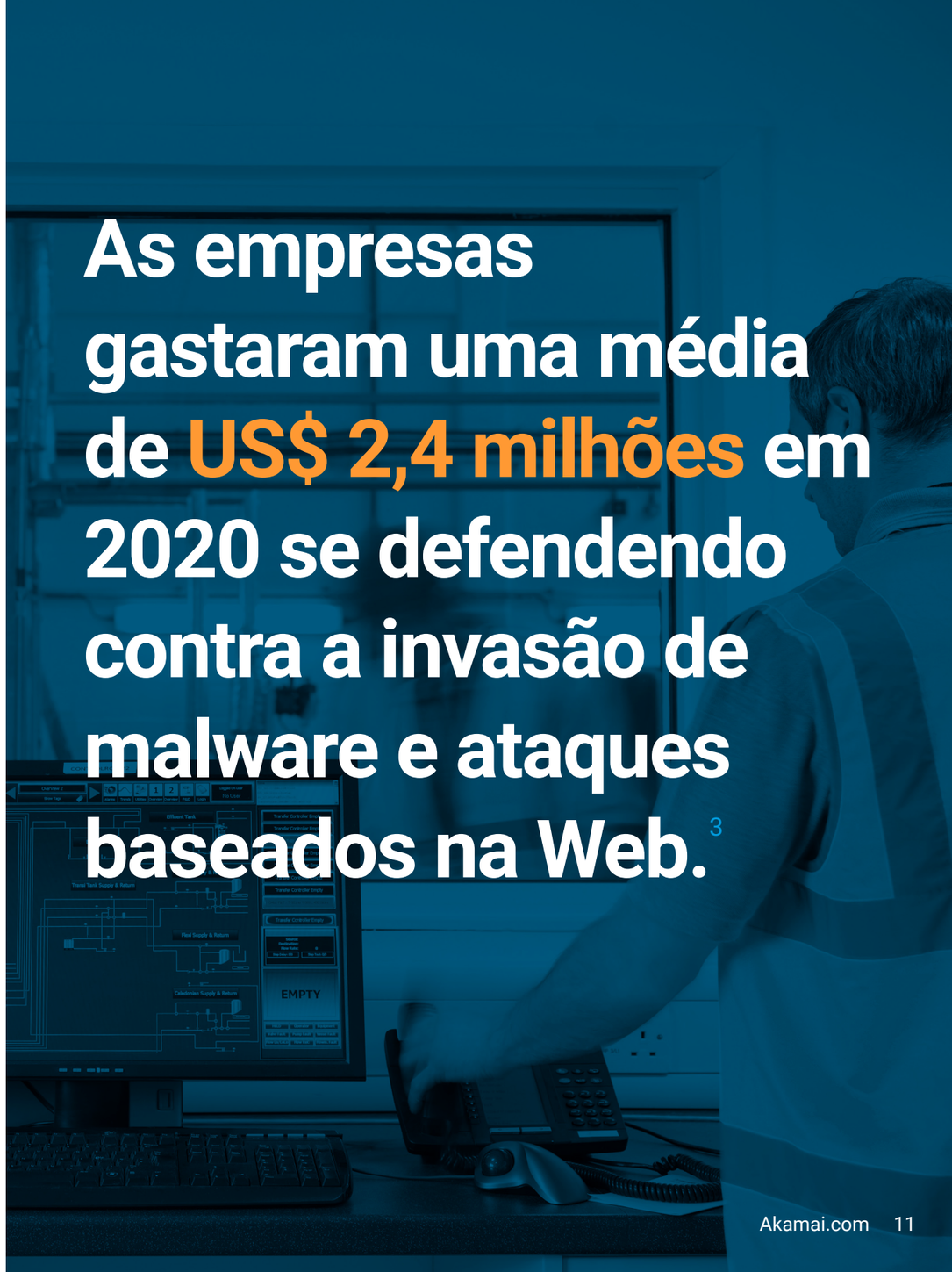
Reduza os riscos internamente

As violações vão ocorrer. E elas podem prejudicar seus negócios, comprometer os dados, danificar a marca e custar milhões.

Ainda acha que os firewalls podem fazer tudo isso? Pense novamente. Depois que o invasor viola uma rede, ambiente ou um data center, ele usa a movimentação lateral para roubar dados e causar estragos, como assumir o controle dos servidores de aplicações ou acessar os servidores do banco de dados.

Na verdade, 70% de todos os ataques agora envolvem tentativas de movimentação lateral.[2]

Enquanto os firewalls identificam a movimentação lateral como tráfego legítimo que acontece dentro de uma rede, a segmentação baseada em software a interrompe imediatamente. A segmentação baseada em software é um componente essencial do seu programa de segurança: permite restringir a movimentação lateral e, em caso de violação, torna a navegação do invasor pelo ambiente mais difícil. Você tem uma chance de lutar ao proteger os dados e aplicações essenciais, diminuindo o tempo de espera e até mesmo detectando o invasor. Essa abordagem é mais escalável, fácil de usar e permite que você implemente a segmentação de forma rápida sem fazer alterações na rede ou nos sistemas.



O Zero Trust não precisa ser complicado

O Zero Trust se trata de quem faz o que para quem e como faz. Em outras palavras, ter controle explícito sobre quem faz o que dentro da rede.

Ao fornecer a um usuário acesso total dentro da rede, você automaticamente concede muita confiança e, como resultado, coloca toda a organização em risco. Em primeiro lugar, os funcionários geralmente cometem erros, o que pode ter sérias implicações de segurança. E alguns são mal-intencionados.

Além disso, fora das redes VPN e dos dispositivos, há muitos pontos de entrada para o data center que você deve considerar. Por exemplo, os invasores podem entrar em uma rede por meio do servidor de produção (como no caso da violação SolarWinds), de uma aplicação internet que está vulnerável ou de uma VPN vulnerável, entre outros. Nesse caso, você confia em um servidor apenas porque ele está dentro da rede, mas, na prática, o invasor pode acessar tudo e se mover lateralmente sem restrições.

Para ter Zero Trust em sua rede de produção, você precisa bloquear todas as atividades que não são explicitamente permitidas.

Isso é algo que os firewalls antigos simplesmente não conseguem fazer em um nível granular, pois requer a identificação de atributos em um nível mais profundo do que os endereços IP e as portas.

Como alternativa, a segmentação baseada em software permite que você veja de fato o que está acontecendo com detalhes e crie políticas precisas e compreensíveis pelo ser humano e que incluem identidade.

Sua lista de verificação Zero Trust: 6 formas de obter o controle explícito

Vamos manter a simplicidade. A confiança deve ser baseada no tamanho do segmento. Quando se trata de proteger dados, ativos e aplicações essenciais, quanto menor o segmento, melhor. Aqui estão seis etapas para alcançar o Zero Trust sem a complexidade operacional.

1. Identifique seus dados confidenciais usando rótulos de visualização.
2. Mapeie os fluxos dos dados confidenciais usando o mapeamento automatizado do fluxo e da dependência.
3. Planeje seus microperímetros Zero Trust usando as ferramentas certas para definir qualquer política de segmentação ou microssegmentação rapidamente.
4. Monitore seu ecossistema Zero Trust continuamente por meio de acompanhamento e análise em tempo real.
5. Adote a automação e a orquestração de segurança com APIs e integrações de tecnologia.
6. Implemente recursos para invalidar a confiabilidade de usuários ou ações e, em caso de ataque, revogue a confiabilidade de qualquer máquina com atributos predefinidos, independentemente do usuário ou segmento.

Akamai

Últimas considerações

Agora, você provavelmente está se perguntando como romper com as soluções antigas para fortalecer sua postura de segurança dentro da rede.

Sem problemas.

Deixe os firewalls antigos onde estão. Eles são bons para proteger o perímetro da rede. Mas os benefícios realmente param por aí.

O que é mais importante reside no núcleo da sua organização, nos ativos digitais, nos dados e nas aplicações que existem além do perímetro: o núcleo da sua infraestrutura corporativa. Mudar seu foco de fora para dentro e implementar a segmentação baseada em software e uma estrutura Zero Trust fornecerá a visibilidade e o controle necessários para detectar e interromper a movimentação lateral, aplicar políticas granulares e adaptáveis e impedir a propagação de ataques cibernéticos como ransomware através da sua rede.

Solicite uma demonstração ou **saiba mais** sobre como a segmentação pode ajudar com ransomware, Zero Trust, segurança na nuvem e muito mais.

1 Cybersecurity Ventures. 2022 Who's Who In Ransomware Report (Relatório quem é quem no ransomware de 2022). Conceal, 2022.

2 Kellerman, Tom e Greg Foss. Global Incident Response Threat Report (Relatório Global de Ameaças de Resposta a Incidentes). VMware Carbon Black, outubro de 2020.

3 "2023 Cyber Security Statistics Trends & Data (Tendências e dados estatísticos de segurança cibernética de 2023)." PurpleSec, 22 de fevereiro de 2023.