Akamai

WHITE PAPER

Um modelo para a criação de arquitetura Zero Trust

Índice

Introdução

O conceito de Zero Trust surgiu por volta de 2009, quando a Forrester Research o promoveu pela primeira vez, alertando as organizações de que era hora de reformular o método tradicional de conceder acesso irrestrito a qualquer usuário ou aplicativo que passasse pelo perímetro da rede. Em vez disso, todos os dispositivos, usuários e fluxos de rede deveriam ser verificados antes que o acesso total fosse concedido. Nos anos seguintes, a urgência de adotar o conceito de Zero Trust só cresceu graças a muitos fatores. A pandemia da COVID-19 criou um aumento repentino no número de funcionários trabalhando em locais remotos, fora do perímetro da rede. Os ataques de ransomware tornaram-se mais frequentes e sofisticados, ampliando as chances de um invasor violar suas defesas e aumentando o prejuízo. O prejuízo médio de uma violação de dados atingiu um recorde de US$ 9,44 milhões nos Estados Unidos, de acordo com o relatório IBM Cost of a Data Breach 2022. Além disso, o crescimento de dispositivos conectados à rede, como dispositivos de IoT (Internet das coisas), e a inclusão de requisitos adicionais para acesso à rede por parceiros e clientes se combinaram para expandir significativamente a superfície de ataque de uma empresa. Em meio a esse cenário de cibersegurança em constante evolução, os fornecedores de software de rede e segurança apressavam-se para comercializar os produtos existentes como Zero Trust ou para introduzir novos produtos, enquanto consultores e analistas adotavam novos acrônimos e definições de mercado. Isso deixou as equipes de segurança com dificuldades para explicar conceitos às vezes complexos e tomar decisões de compra que definem a base da mudança para uma estratégia Zero Trust.

Este white paper foi projetado para fornecer às equipes de segurança um plano para fazer investimentos na tecnologia Zero Trust, identificando onde começar e descrevendo os principais fatores de diferenciação.

Trabalho remoto, apps em nuvem rompem o paradigma de segurança de rede

Quando, como e onde as pessoas trabalham não está mais limitado às quatro paredes de um escritório.

Com isso, o perímetro da rede não existe mais, pelo menos não de uma forma reconhecível. É possível que seus usuários estejam dentro dos limites de segurança ou fora deles. Isso também vale para as aplicações que eles usam, já que o SaaS (software como serviço) e implementações multinuvem estão proliferando. Com ameaças avançadas e persistentes, é provável que você deixe inadvertidamente que os agentes mal-intencionados tenham acesso total aos seus ativos mais valiosos, assim que conseguirem entrar na rede. Ao conseguirem entrar, sem um programa Zero Trust abrangente, os agentes mal-intencionados têm liberdade para acessar o que quiserem.

E isso não é apenas teoria. É evidente pelas violações generalizadas e custosas de dados nos últimos anos, cuja grande maioria aconteceu como resultado do excesso de confiança dentro do perímetro da rede.

Entretanto, as aplicações que foram projetadas para ficar dentro de um perímetro de rede geralmente têm os piores perfis de segurança. Afinal, se você fosse um desenvolvedor que presumisse que apenas funcionários autorizados com boas intenções poderiam acessar seu sistema, teria ficado tão defensivo quanto o codificador de hoje, que sabe que vastos exércitos de hackers tentarão explorar sua aplicação baseada na Internet?

A solução para esses desafios, em todo o mercado, é o Zero Trust.

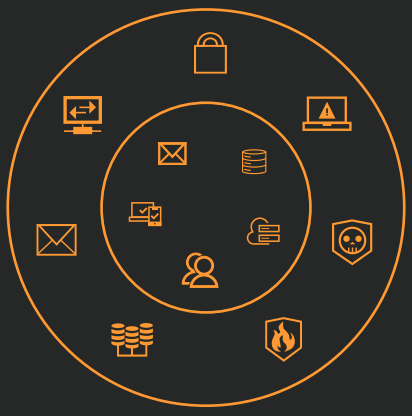
Uma arquitetura de segurança Zero Trust

O princípio por trás do Zero Trust é muito simples, mas muito poderoso: a confiança não é um atributo do local. Você não deve confiar em algo simplesmente porque está protegido por seu firewall. Em vez disso, qualquer ação, não importa onde ocorra, só deve ser confiável se tiver sido explicitamente permitida. Em última análise, apenas o que *deveria* acontecer *pode* acontecer. As organizações precisam remover toda a confiança implícita para ações que não são necessárias. Por exemplo, dar a todos os usuários da contabilidade acesso ao sistema financeiro, quando apenas alguns precisam dele, gera risco, mas não valor.

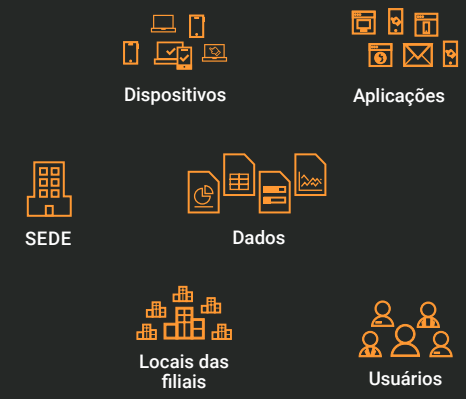
O método de comprovação disso é um sólido processo de autenticação e autorização e os sistemas não devem transferir dados até que a confiança seja estabelecida. Além disso, análises e registros devem ser utilizados para verificar o comportamento e observar continuamente os sinais de comprometimento.

Essa mudança fundamental supera uma grande quantidade de comprometimentos que vimos serem feitos na última década. Os invasores não podem mais passar tempo explorando as fraquezas de seu perímetro e, em seguida, explorar seus dados e aplicações confidenciais porque conseguiram ultrapassar os limites de segurança. Agora, não há mais barreira. Existem apenas aplicações e usuários, e todos eles devem se autenticar mutuamente e verificar a autorização antes que o acesso possa ocorrer.

Arquitetura de segurança tradicional



Realidade moderna



Como uma organização cria uma arquitetura Zero Trust?

Primeiro, todas as empresas precisam mapear uma estratégia para o cenário existente e determinar se e quando precisam contratar novos talentos para a equipe de trabalho. Um artigo inteiro poderia ser dedicado a essa etapa importante no processo, mas os reais produtos que podem ajudar a adotar uma estratégia Zero Trust devem ser orientados por três metas.

1. **Não confie em nenhuma entidade, verifique constantemente.** "Não confie e verifique constantemente" parece muito mais fácil na teoria. Se você simplesmente cortar todo o acesso a todos os sistemas e dados, você terá bloqueado sua rede. O verdadeiro desafio é verificar constantemente sem gerar grandes interrupções nos negócios, especialmente quando a maioria dos sistemas foi projetada tendo em mente a confiança implícita. Você precisa de ampla visibilidade e controle de todos os tipos de acesso e meios simples e práticos de aplicar e manter a política.
2. **Depois de verificar, forneça acesso mínimo.** Em um ambiente Zero Trust, depois que um usuário for verificado, ele deverá ter acesso apenas ao que é exigido pelo seu cargo.
3. **Monitore continuamente as ameaças.** Como a maioria dos especialistas do setor afirmará, Zero Trust é um esforço contínuo. Os agentes maliciosos estão se tornando cada vez mais sofisticados à medida que tentam violar as defesas de uma empresa. As organizações devem monitorar, verificar e limitar continuamente o acesso. Uma das vantagens de um modelo Zero Trust é que ele não está focado no que os invasores estão fazendo, mas sim no que o negócio em si está fazendo. Com uma verdadeira política Zero Trust em vigor, as cadeias de ataque são pressionadas a subverter tudo que seu negócio precisa para funcionar de uma só vez. Você poderá interromper cada ataque em algum momento da cadeia. Isso inclui a capacidade de interromper ataques que ainda não foram concebidos. Não importa se for um ataque de dia zero ou não, o Zero Trust pode ajudar a mitigá-lo.

Contras do Zero Trust

No entanto, quando uma organização embarca na implementação do Zero Trust, também deve considerar o lado oposto de toda essa desconfiança e os limites de acesso. Um aspecto fundamental do Zero Trust é a restrição do acesso, principalmente por meio da lista de permissões. É a prática de decidir o que pode acontecer, todo o resto é negado por padrão. Ao diminuir a capacidade de um invasor de realizar uma campanha mal-intencionada, a organização pode aumentar a probabilidade de impedir acidentalmente que alguém consiga fazer seu trabalho. Por outro lado, verificações repetidas de cargas de trabalho e dispositivos podem causar atrasos e frustrações. Uma estratégia Zero Trust que impeça as pessoas de realizarem o próprio trabalho de forma eficaz não é bem uma estratégia.

Portanto, uma estratégia Zero Trust bem estruturada terá um equilíbrio entre segurança e acesso.
E também é necessário um equilíbrio entre o que pode ser efetivamente realizado e os recursos, tanto orçamentários quanto de pessoal, de sua equipe de segurança.

Elementos de Zero Trust

Já se passaram mais de 10 anos desde que a Forrester apresentou pela primeira vez o conceito de Zero Trust. Muitas organizações estão começando agora a jornada Zero Trust e estão enfrentando um mercado complicado de produtos de software. Alguns produtos existem há anos e abordam partes de uma arquitetura Zero Trust, outros novos produtos surgiram e muitos provedores de software foram rápidos em denominar as ofertas como Zero Trust. Além disso, como muitos analistas e observadores do setor afirmarão, "Zero Trust não é um produto, é uma estratégia abrangente" e "Zero Trust não é um destino, é uma jornada". No entanto, essas reivindicações frequentemente repetidas pouco ajudam aqueles que estão enfrentando decisões de compra de soluções de tecnologia Zero Trust e, na verdade, podem gerar mais confusão.

Como não há um produto único que leva uma empresa ao Zero Trust e, como as organizações individuais têm várias prioridades e vulnerabilidades diferentes, o ponto de partida varia para cada empresa. Mesmo assim, graças aos avanços tecnológicos e à consolidação do setor, as empresas agora podem obter as ferramentas necessárias para implementar uma política Zero Trust por meio de uma única fonte. As empresas de análise também estão começando a reconhecer isso. A Gartner analisa o que chama de SSE (Secure Service Edge), uma combinação de gateway Web seguro, corretores de segurança de acesso na nuvem e ZTNA (Zero Trust Network Access). No relatório, What Are Practical Projects for Implementing Zero Trust?, a Gartner também inclui microssegmentação (que ela chama de segmentação de carga de trabalho para carga de trabalho), recomendando que "as organizações que desejam migrar para a implementação prática devem se concentrar em dois projetos principais: segmentação de usuário para aplicativo (ZTNA) e segmentação de carga de trabalho para carga de trabalho (segmentação baseada em identidade)".

Da mesma forma, a IDC analisa o acesso seguro e a segmentação, que ela define como uma visão abrangente das tecnologias emergentes e legadas usadas para proteger sistemas de computação, recursos e dados por meio de segmentação lógica, controle de acesso e detecção de ameaças.

A maioria dos especialistas espera que o mercado siga o processo de adoção de várias aplicações de um único fornecedor. No relatório Predicts 2022: Consolidated Security Platforms Are the Future, a Gartner prevê que "até 2025, 80% das empresas terão adotado uma estratégia para unificar o acesso à Web, aos serviços de nuvem e às aplicações privadas por meio de uma plataforma SSE (Security Service Edge) de um único fornecedor".

No entanto, a combinação desses sistemas separados em uma estratégia coesa torna-se o principal desafio. Quais são os principais elementos e o que os CIOs, CISOs e outros profissionais de segurança devem considerar ao criar uma arquitetura Zero Trust eficiente para a organização?

Os princípios do Zero Trust

Acesso à rede Zero Trust

Às vezes confundido com a abordagem geral de Zero Trust, o ZTNA é uma parte fundamental da pilha de tecnologia. O acesso seguro é a principal etapa inicial em qualquer estrutura Zero Trust. Infelizmente, como tantos elementos do processo, ele rapidamente se torna mais complexo do que parece. O acesso seguro não é uma decisão binária. Fornecer o nível certo de acesso à aplicação certa para os usuários certos no momento certo tornou-se muito mais complexo à medida que os usuários e as aplicações se tornaram mais amplamente distribuídos. Na verdade, a própria definição de um usuário agora significa muito mais do que apenas um funcionário e pode incluir clientes, fornecedores e parceiros. Enquanto isso, as aplicações podem incluir apps preexistentes, SaaS ou apps para dispositivos móveis e exigir acesso com origem e destino para data center, Internet ou ambientes de nuvem.

Uma solução ZTNA eficaz verificará a identidade do usuário e dos dispositivos e confirmará se eles podem acessar as aplicações que precisam, estejam onde estiverem, reduzindo a possível área de ataque e melhorando a flexibilidade e o monitoramento. Durante décadas, as organizações confiaram em VPNs (Virtual Private Networks) compatíveis com provedores de identidade para fornecer acesso. Essas VPNs, projetadas para uma era diferente, não são mais suficientes para o tamanho e o escopo da força de trabalho distribuída de hoje. O ZTNA evoluiu para se tornar mais do que apenas uma substituição para VPNs e agora concede acesso com base não apenas na verificação da identidade do usuário e dos dispositivos, mas também em atributos como hora e data, geolocalização e postura do dispositivo para proporcionar o nível apropriado de confiança.

Principais considerações para a compra de soluções de acesso à rede Zero Trust

À medida que as empresas começam a substituir as VPNs antigas por soluções mais sofisticadas de gerenciamento de identidades, há inúmeras áreas a serem consideradas. Atualmente, as soluções mais avançadas combinam gerenciamento de identidade e acesso, segurança de aplicação, MFA (autenticação multifator) e login único, tudo com visibilidade e controle de gerenciamento em uma única interface. As organizações que buscam iniciativas Zero Trust devem procurar soluções que possam atender às suas necessidades atuais, mas também expandir com os negócios, permitindo que elas integrem rapidamente funcionários de uma fusão ou aquisição de uma empresa, possibilitem a fabricação ou produção em diferentes mercados ou regiões geográficas, adicionem e removam facilmente os prestadores de serviços para se adaptar às necessidades de negócios em constante mudança e migrem as aplicações para a nuvem de forma econômica, sem sacrificar a segurança.

As organizações devem buscar soluções que possam se integrar diretamente às infraestruturas de identidade existentes, mesmo que incluam vários diretórios e provedores de serviços de identidade. Isso permite que o serviço ZTNA seja implantado rapidamente, sem a necessidade de alterar a arquitetura ou a infraestrutura de identidade existente.

Pense na edge

Há também um diferencial significativo entre os produtos no mercado que as equipes que tomam decisões de compra Zero Trust podem não levar em consideração, mas definitivamente deveriam. As soluções combinadas com plataformas de nuvem de edge podem oferecer outros benefícios, atuando como um proxy com reconhecimento de identidade que abstrai a conectividade com a plataforma de edge, garantindo que toda a autenticação seja feita na edge e longe do data center. Embora algumas empresas recorram a arquiteturas de proxy de acesso executadas em DMZ, elas não aproveitam a capacidade da nuvem de absorver melhor os ataques, fornecer largura de banda para armazenamento em cache e escalonamento automático conforme necessário. Um proxy com reconhecimento de identidade integrado à nuvem pode ser dimensionado sob demanda, executar recursos pesados de CPU e absorver ataques. Além disso, ele fica em um endereço IP privado que não é acessível diretamente da Internet. As atividades que são mais sensíveis em termos de desempenho e segurança ocorrem na edge, mais próximas do usuário final. Além disso, o caminho sensível de entrada na aplicação acontece por meio de um túnel de aplicação reversa, removendo efetivamente a visibilidade do IP do perímetro e reduzindo o risco de ataques volumétricos.

> **As soluções combinadas com plataformas de nuvem de edge podem oferecer outros benefícios, atuando como um proxy com reconhecimento de identidade.**

Considerações sobre autenticação multifator na criação de um modelo Zero Trust

O crescimento do trabalho remoto e a necessidade de mais acesso significam que a maioria das organizações já adotou a MFA e tem algum tipo de solução implementada. No entanto, é importante reconhecer que a combinação de acesso em toda a empresa e MFA é maior do que a soma das partes. A MFA é fundamental para o conceito de confiança, pois exige que você tenha mais do que simplesmente uma senha. Você precisa de uma segunda verificação para garantir que não esteja sendo vítima em uma das áreas de confiança mais violadas. Também é importante lembrar que nem todas as soluções MFA são criadas da mesma forma.

Ao avaliar as soluções de MFA como parte de uma estratégia Zero Trust, as organizações devem procurar soluções que sejam:

- Integradas ao gerenciamento de identidades e ao acesso empresarial
- Compatíveis com o FIDO2 para garantir que as credenciais do usuário sejam descentralizadas, isoladas e criptografadas nos dispositivos pessoais dos usuários, o que é particularmente importante para impedir ataques de phishing
- Capazes de verificar usuários por meio dos smartphones sem depender de uma chave física

Microssegmentação

Não há um estado perfeito de Zero Trust. Inevitavelmente, haverá lacunas que os invasores mais persistentes poderão encontrar e explorar. Qualquer abordagem ampla para Zero Trust exigirá, portanto, microssegmentação. Atualmente, a maioria das redes não tem segmentos ou tem poucos segmentos. Na verdade, as organizações tradicionalmente protegiam suas aplicações essenciais com firewalls, mas isso pode ser difícil por vários motivos. Basicamente, os firewalls exigem que você aplique uma política de rede, criando um ponto de estrangulamento. Você precisa de conexões de rede para passar por um firewall, o que se torna caro rapidamente, não detecta muitos dos riscos no tráfego de rede moderno e é extremamente difícil de mudar. Em vez disso, as organizações estão recorrendo à microssegmentação baseada em software, o que simplifica muitos desses processos trabalhosos.

Diferenciais na microssegmentação

Embora seja um requisito fundamental de qualquer iniciativa Zero Trust, a microssegmentação tem sido frequentemente considerada à parte das principais soluções ZTNA. E, embora a microssegmentação seja vendida por provedores de plataformas de segurança e como uma solução independente, há algumas diferenças fundamentais que os compradores precisam entender.

Onde posso implantá-la? As soluções de microssegmentação que foram criadas como ferramentas de rede em vez de uma abordagem com foco na segurança ou aquelas criadas para sistemas locais devem gerar desconfiança para compradores potenciais. As ferramentas atuais devem ser implantadas na nuvem, em ambientes locais, em dispositivos (incluindo aqueles nos quais não é possível instalar agentes) e entre contêineres em ambientes híbridos. Isso normalmente exigirá software baseado em nuvem. Se uma solução de microssegmentação puder cobrir apenas 80% do seu ambiente, isso não será suficiente.

Qual é a visibilidade que ela oferece? Embora as soluções de microssegmentação restrinjam o acesso, uma restrição excessiva pode interromper os processos de negócios e levar a chamadas do COO. A microssegmentação requer um entendimento sofisticado do seu ambiente. Quais servidores podem acessar quais servidores? Você pode definir políticas entre um cluster do Kubernetes e um servidor Windows 2008? Muitas ferramentas não têm agentes que remontem a 2008 ou que sejam tão inovadoras quanto a aplicação de políticas no Kubernetes. Seu software de microssegmentação deve conseguir lidar com esses tipos de complexidades se você implantar o Zero Trust de forma eficaz. Além disso, os compradores de software de microssegmentação precisam considerar a granularidade das políticas às quais o produto oferecerá suporte. A maioria dos sistemas aplicará políticas na camada de aplicação entre portas e processos. Produtos mais sofisticados podem impor políticas na camada de microsserviços. Por exemplo, os invasores podem usar alguns dos serviços do svchost, como o agendador de tarefas, para mover-se lateralmente por toda a rede. No entanto, as empresas não podem bloquear o svchost por completo porque ele possui funções importantes. É aí que uma solução de microssegmentação que aplica a política na camada de microsserviços pode fazer a diferença.

Qual é o grau de dificuldade da implementação? A facilidade de expressar a política que você precisa agora e, igualmente importante, que você precisará no futuro deve ser uma das principais considerações para qualquer solução de microssegmentação. Quer se trate de uma política de tempo de paz quando se está em uma fase de planejamento ou de uma política de tempo de guerra quando existe uma ameaça para o seu ambiente e você precisa bloqueá-la, é necessário ter certeza de que o mecanismo em que você investe suportará facilmente as duas. Por exemplo, começar com lista de permissões em um projeto de microssegmentação pode ser intimidador para as equipes de segurança, graças aos riscos de negar incorretamente uma aplicação ou serviço necessários. Uma solução sofisticada de microssegmentação deve vir com modelos de listas de negações que as equipes podem implementar de forma rápida e fácil para estabelecer prontamente alguns ganhos para o projeto. Assim que isso for feito, as organizações podem continuar a jornada rumo à ampla proteção da lista de permissões que inclui recursos precisos de dependência e mapeamento de inventário contextual.

> **As soluções de microssegmentação que foram criadas como ferramentas de rede em vez de uma abordagem de segurança em primeiro lugar ou aquelas criadas para sistemas locais devem gerar um sinal de alerta para compradores potenciais.**

Gateway Web seguro

Em um ambiente Zero Trust, não são apenas as pessoas que podem não ser confiáveis, mas a própria Internet. Os funcionários precisam de acesso à Internet e, como aplicações móveis e SaaS, serviços de nuvem, trabalho remoto e dispositivos de IoT se expandem, o mesmo ocorre com a superfície de ataque de uma organização. Proteger a organização e os usuários contra ameaças como malware, ransomware, phishing e exfiltração de dados se torna exponencialmente mais difícil. As organizações têm recursos limitados para gerenciar as complicações e complexidades dos pontos de controle de segurança e as lacunas de segurança nas soluções locais preexistentes.

Impor a Zero Trust entre uma pessoa e a Internet requer um SWG (gateway Web seguro), que se torna um recurso central de qualquer iniciativa Zero Trust.

Principais requisitos de Zero Trust em qualquer investimento gateway Web seguro

Embora aparentemente simples, há requisitos que os compradores de tecnologia devem considerar ao investir em um SWG. Muitas organizações implantaram SWGs no local, mas agora precisam estender essa proteção aos usuários, seja qual for a localização. Semelhante ao gerenciamento de identidades, os provedores que têm plataformas de edge robustas geralmente têm uma segurança SWG mais forte graças à inteligência da plataforma estendida. Os tomadores de decisão devem considerar cuidadosamente esses requisitos principais.

Inspeção de DNS. Os provedores devem ser capazes de fornecer inspeções em tempo real de todos os domínios com inteligência contra ameaças sofisticada e bloquear automaticamente domínios mal-intencionados. As soluções também precisam ser eficazes em todas as portas e protocolos para proteger contra malwares que não usam portas e protocolos padrão da Web. A qualidade da inspeção de DNS pode variar muito entre os provedores, e os compradores devem procurar aqueles com experiência no mercado e sucesso do cliente estabelecido.

Inspeção de URL. Da mesma forma, HTTP e HTTPS solicitados precisam ser verificados em tempo real e URLs mal-intencionados devem ser bloqueados automaticamente.

Análise de carga útil. Todas as cargas úteis devem ser verificadas quanto a malware usando várias técnicas para fornecer proteção ampla de dia zero contra arquivos mal-intencionados. O ideal é que os sinais de seus produtos SWG sejam compartilhados com outros produtos de segurança para garantir o isolamento ou a restrição de acesso a ativos comprometidos.

Monitoramento de ameaças

A última parte da principal tecnologia Zero Trust é o monitoramento de ameaças. Embora a suposição de Zero Trust seja que nada é implicitamente confiável e seu SWG ajudará a bloquear ransomware e malware, as organizações precisam permanecer vigilantes para detectar ataques contínuos e emergentes, bem como possíveis riscos (como configurações incorretas ou direitos de acesso excessivamente permissivos). À medida que as equipes de segurança avaliam o software no mercado, elas devem analisar as três considerações a seguir para um monitoramento eficaz de ameaças.

Principais considerações

- **Algoritmos eficazes**
  Algoritmos sofisticados com histórico de sucesso baseado em anomalias de atividade do usuário e da rede, análise executável, análise de log, entre outros, devem fazer parte de qualquer serviço de monitoramento de ameaças.

- **Detecção de sinal forte**
  Embora o software e a inteligência artificial sejam ferramentas vitais para o monitoramento de ameaças, os tomadores de decisões da Zero Trust ainda devem avaliar a experiência interna dos fornecedores com quem estão trabalhando. Os serviços de monitoramento de ameaças precisam ser capazes de separar os bons sinais dos ruins para ajudar a evitar a fadiga do alerta e fornecer notificações imediatas de qualquer incidente. As organizações também devem esperar relatórios regulares com análises de quaisquer campanhas de alto perfil.

- **Equipe experiente**
  As equipes devem incluir pessoas com uma ampla gama de experiências, incluindo militar, ofensiva, resposta a incidentes e ciência de dados, e devem estar disponíveis 24 horas por dia, 7 dias por semana. Essa é uma área em que os provedores de fornecimento de conteúdo podem adicionar um benefício substancial. Os insights do monitoramento de centenas de terabytes por segundo contribuem para uma perspectiva única de qualquer detecção de sinal.

Por onde começar?

Uma iniciativa Zero Trust nunca está completa, por isso, para aqueles que consideram o software, o hardware e os requisitos de contratação, a pergunta principal costuma ser: "Com qual tecnologia começamos?"

Da mesma forma que outras questões, a resposta dependerá das necessidades individuais de uma empresa, das avaliações de risco e dos pontos fortes e fracos relativos. Para muitos observadores do setor, a resposta é começar implementando o ZTNA. Na verdade, proteger a organização contra o tráfego norte-sul mal-intencionado pode ser um ponto de partida prudente. No entanto, acredita-se também que uma abordagem leste-oeste com microssegmentação, especificamente a microssegmentação definida por software, é o melhor caminho.

Argumentos para começar a usar a microssegmentação

Se você acredita, como a maioria dos especialistas, que não há defesa perfeita e que um ataque mal-intencionado acabará ocorrendo, então você desejará proteger seus ativos mais valiosos. É isso que a microssegmentação oferece.

Uma das razões pelas quais as organizações podem estar relutantes em começar com a microssegmentação é a percepção da complexidade. Primeiro, a microssegmentação não é uma abordagem tudo ou nada. Assim como a Zero Trust, ela pode ser realizada em etapas. As organizações podem começar identificando os ativos mais valiosos. Você deve se concentrar no que é essencial. Certifique-se de que, se alguém entrar em seu sistema, isso não prejudicará seus negócios.

A importância de um ativo pode ser baseada nos dados contidos nesse ativo ou no nível de proteção existente. Em muitos casos, isso significará seus sistemas legados, porque os provedores de segurança não são compatíveis com eles.

Em segundo lugar, a microssegmentação definida por software remove grande parte da complexidade percebida. Você não precisará lidar com hardware e chamar repetidamente os arquitetos de rede e de segurança. Você apenas implantará o software, o que reduz significativamente a barreira de entrada.

Depois que uma iniciativa de microssegmentação começar, os primeiros benefícios são claros e podem ajudar a impulsionar o restante do projeto. Por exemplo, agora você terá uma espécie de fonte da verdade para o que está acontecendo em seu ambiente. Você pode conseguir isso imediatamente, mesmo sem aplicar a política e, assim que o fizer, terá uma grande compreensão de como os fluxos estão acontecendo.

Além disso, assim que uma organização começa a delimitação de aplicações, você pode bloquear de forma rápida e fácil as aplicações essenciais para que se comuniquem apenas por portas e processos específicos. Como alternativa, uma vitória rápida pode ser visar políticas específicas de ameaças. Plataformas sofisticadas de microssegmentação terão listas de negações integradas. Isso significa que você pode criar rapidamente uma política para interromper conexões desnecessárias entre os serviços de desktop remotos e a Internet. As organizações podem rapidamente eliminar o tipo de vulnerabilidade que levou ao ataque Colonial Pipeline, por exemplo.

Seja qual for o ponto de partida, a chave para qualquer jornada contínua Zero Trust é o equilíbrio. Por exemplo, o gerenciamento de identidades de padrão internacional com baixa segmentação ou proteções de acesso à Web ineficazes não garantem uma boa segurança.

Plataforma versus ferramentas especializadas

Assim como em muitas decisões de tecnologia, comprar um software Zero Trust geralmente se resume à escolha entre especialistas individuais e uma plataforma que combina vários componentes. O impacto do Zero Trust entre equipes de segurança, integradores, arquitetos e analistas e a necessidade de manter a política em vários consoles, diferentes agentes e várias integrações oferece um caso convincente para seguir o caminho da plataforma. Isso é particularmente verdadeiro em um mercado de trabalho apertado com uma escassez de profissionais especializados em segurança virtual. O gerenciamento de soluções de vários fornecedores pode aumentar significativamente os custos de pessoal, já que as soluções que não se comunicam efetivamente criam falsos positivos, o que sobrecarrega os usuários finais e pode exigir suporte e treinamento adicionais.

Além disso, o interesse em estabelecer uma parceria quando se trata de suporte e negociações de contrato fornece uma justificativa convincente para implementar o Zero Trust com um provedor de plataforma.

> **Uma das razões pelas quais as organizações podem estar relutantes em começar com a microssegmentação é a percepção da complexidade.**

Revisão dos elementos de Zero Trust

Saiba quem são seus usuários. Assegure que eles foram verificados.

Proteja seus ativos. Autentique/autorize todas as transações.

Proteja os usuários. Impeça que malware infecte os usuários.

Conclusão

Em última análise, a maioria das organizações preocupadas com a proteção contra ataques cibernéticos reconhece a necessidade de começar a migrar para uma arquitetura Zero Trust mais cedo ou mais tarde. Muitos já começaram a jornada de forma gradual ou repentina como uma resposta ao crescimento do trabalho remoto. No entanto, à medida que os invasores se tornam mais sofisticados, as superfícies de ameaças se expandem e cada vez mais integrantes exigem acesso remoto, a necessidade de um portfólio abrangente de aplicações que funcionem em conjunto só aumenta.

Para obter detalhes sobre elementos específicos da abordagem da Akamai para Zero Trust, fale com um de nossos especialistas.