SOPHOS

Desvendando o Zero Trust

A era da rede corporativa e de um único perímetro de segurança está chegando ao fim. Progressivamente, mais e mais usuários estão trabalhando remotamente, realizando suas tarefas através da Internet pública. O aumento dos aplicativos Software como Serviço (SaaS), plataformas na nuvem e outros serviços baseados na nuvem diluiu a eficácia de uso da rede como elemento básico para proteger um recurso. Não podemos mais contar apenas com uma rede corporativa hermética e única e simplesmente confiar em todos os sistemas que residem nela – as bordas entre redes estão nebulosas.

Assim, chega o Zero Trust: uma filosofia sobre como pensar sobre a segurança e como concretizar a segurança. Zero Trust é um conceito baseado no princípio "confie, mas confira" que foca na proteção dos recursos, independentemente de onde estão física ou digitalmente, e se atém a nunca confiar em nada.

Nenhum fornecedor, produto ou tecnologia lhe dará a confiança plena que o conceito implica. Melhor dizendo, seria necessária uma guinada cultural e muitas soluções diferentes para mudar os paradigmas que formam o arsenal de segurança dos nossos recursos.

Este documento fala sobre o conceito Zero Trust, os benefícios de implementar um modelo Zero Trust, e descreve os passos que as organizações precisam seguir para fazer a transição para essa nova era.

Os tempos mudaram

O conceito de "confiança" que a palavra trust implica tem seus perigos quando se trata da tecnologia de informação, especialmente se combinada com outras palavras, como "inadequada" ou "duvidosa".

Criar um perímetro de segurança de rede corporativo amplo e hermético e confiar em tudo o que adentra suas divisas demonstrou repetidamente ser algo não tão confiável. Mas para os hackers, isso é como um sonho. Uma vez que entram, se tornam etéreos. Fluindo pela rede, acessando sistemas importantes... Tudo isso se torna trivial, pois os controles de segurança e as verificações robustas ocorrem apenas no perímetro.

Goste você ou não, esse perímetro cedeu.

Os usuários querem trabalhar remotamente e em redes não confiáveis, como no Wi-Fi público de um café no aeroporto. Eles querem que seus dados sejam armazenados na nuvem, para poder acessá-los quando precisarem. Eles querem usar seus próprios dispositivos pessoais para acessar dados e recursos corporativos, e querem acesso fácil, pois, assim, podem trabalhar quando, onde e como lhes apetecer.

O uso de aplicativos Software como Serviço (SaaS), plataformas na nuvem e outros serviços baseados na nuvem coloca os dados para fora do perímetro corporativo, e as plataformas na nuvem pública hoje abrigam os dispositivos e serviços que antes viviam cercados pelo perímetro da rede, deixando-os soltos no mundo. Nossas cargas de trabalho se movem em busca da melhor relação entre custo e benefício para o seu processamento, distanciando-se das redes que possuímos, controlamos e confiamos.

Tudo está em toda parte. O antigo modelo de "rede corporativa" com defesas estáticas desapontou as empresas pela falta de oferta de uma nuvem que funcione e ao mesmo tempo proteja seus dados, seus usuários e seus clientes. É preciso uma mudança de paradigmas.

Entre na era Zero Trust

Zero Trust é uma abordagem holística de segurança que trata das ameaças e mudanças no modo como as empresas trabalham. É uma filosofia e um modelo de como pensar sobre segurança e como colocá-la em prática.

Nada nem ninguém deve ser classificado como confiável à primeira vista, seja dentro ou fora da sua rede corporativa – nem a própria rede. A confiança implícita baseada na localização da rede, com defesas estáticas como um firewall tradicional, deve ser limitada.

Ocasionalmente, precisamos confiar em algo, mas com o Zero Trust, essa confiança é temporária e é estabelecida dinamicamente a partir de múltiplas fontes de dados – mais do que já usamos no passado, sendo constantemente reavaliada. Fontes de dados incluem informações sobre a solicitação de acesso, informações sobre o usuário, informações sobre o sistema, informações sobre os requisitos de acesso e a inteligência de ameaças. Além disso, o acesso a dados e/ou recursos é concedido apenas quando necessário, baseado na conexão.

Temos bastante experiência com rede não confiáveis através do nosso uso diário da Internet. Computadores que encaram a Internet pública são protegidos de uma maneira muito diferente daqueles dentro desse perímetro tradicional, o que exige escrutínio e camadas extras de defesa para protegê-los contra ameaças externas.

O modelo Zero Trust o orienta a tratar todos os dispositivos como se interagissem diretamente com a Internet, em lugar de operar dentro de um único perímetro, e você deve criar vários microperímetros (ou microssegmentos), aplicando verificações e controles ao redor de tudo e entre tudo.

Os benefícios básicos de adotar o Zero Trust

Adotar o modelo Zero Trust traz inúmeros benefícios, e, para facilitar a vida, selecionamos alguns dos principais.

Controle de todo o patrimônio de TI

Partindo de dentro do escritório e percorrendo todas as plataformas da nuvem que você usa. Assim não há mais falta de controle fora do perímetro corporativo ou contendas com usuários remotos.

Gerenciar e proteger todos os usuários da mesma forma

Sem olhar e classificar algo como dentro ou fora do perímetro corporativo, você pode tratar todos os usuários da mesma forma. Além de simplificar a segurança de TI, isso também garante que todos os dispositivos e usuários sejam tratados igualmente.

Manter a segurança mesmo quando você não tem controle total da infraestrutura em uso

Ao usar identidade, localização, integridade do dispositivo e autenticação MFA, e sobrepor monitoramento e análise, você continua capaz de ter segurança robusta em todo e qualquer tipo de ambiente, plataforma ou serviço.

Redução drástica no movimento de malware ou invasores

Ao invés de manter as rédeas de toda a rede depois de se infiltrarem, os invasores só têm acesso ao mínimo de sistemas que o usuário comprometido tinha acesso. Ao desconfiar continuamente do usuário autenticado, as verificações serão aplicadas entre esses sistemas, limitando ainda mais a capacidade de disseminação.

Um resumo do Zero Trust

Zero Trust é uma grande ideia, e muito se fala sobre o assunto. Em sua essência, podemos condensar os principais conceitos de Zero Trust em vários provérbios, que você deveria sempre se lembrar conforme segue a sua jornada.

Não existe "dentro" da rede

Façamos de conta que você está operando o seu negócio inteiramente de localidades não confiáveis, como Wi-Fis públicos, e que todos os seus dispositivos estão conectados diretamente à mais perigosa de todas as redes: a Internet pública. Imaginando que essa seja a sua realidade, você se vê forçado a aplicar a segurança de forma a nunca poder ficar por trás de um perímetro corporativo tradicional.

Sempre haverá redes corporativas "confiáveis" para sistemas administrativos e internos, mas a meta é manter os usuários comuns fora dessas redes, usando proxies de aplicativos e outras tecnologias, reduzindo drasticamente a superfície de ataque.

Confie, mas confira

Partamos do pressuposto de que os invasores estão dentro e fora de nossas redes e de que estão presentes o tempo todo, em constante ataque. Nenhum usuário ou dispositivo deveria ser automaticamente confiado e se autenticar antes que uma conexão possa ao menos ser cogitada. Imaginando-se sob ataque constante de todas as direções, você é levado a desenvolver um processo sólido de autenticação e autorização para os seus recursos, dispor suas defesas em camadas e monitorar e analisar constantemente o que acontece em todo o seu patrimônio computacional.

A segurança deveria se adaptar em tempo real

As políticas de segurança que você coloca em vigor para atingir o Zero Trust deveriam ser dinâmicas e mudar automaticamente com base em insights provenientes de muitas e diferentes fontes de dados, das mais diferentes tecnologias possíveis. Uma política estática do tipo "ESTE USUÁRIO" usando "ESTE DISPOSITIVO" pode acessar "ESTE RECURSO" não o protegerá se o dispositivo foi comprometido enquanto tal usuário estava em tal dispositivo. Se a sua política também considerou a integridade do dispositivo, como a identificação de comportamentos maliciosos, ela poderia usar isso para se adaptar dinamicamente à situação sem dar nenhum trabalho para o administrador.

Isso tem sido parte da estratégia e filosofia de segurança cibernética da Sophos há bastante tempo. Você provavelmente conhece isso como Segurança Sincronizada: quando seus produtos podem compartilhar insights únicos que descobrem entre eles. Isso nos permite ter políticas adaptativas e dinâmicas e aproveitar todos esses insights de modo que a política nunca se mantenha estática, o que facilitaria circunavegá-la.

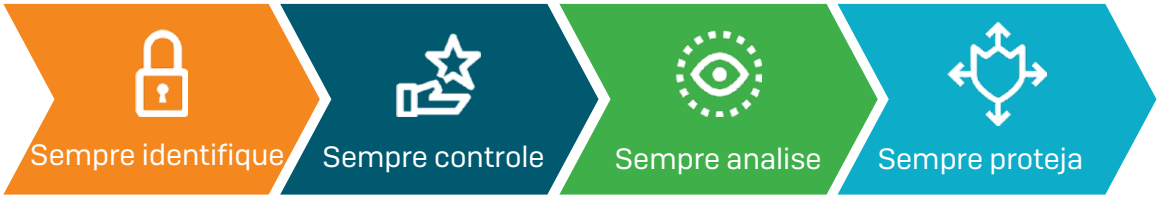
Muito disso se resume em uma boa política de segurança e boas práticas já vigentes, e se você se preparou para a regulamentação GDPR, já fez grande parte de todo esse trabalho.

Princípios do Zero Trust

Não confie em nada. Nunca. Quando você não confia, se vê forçado a buscar medidas relevantes de segurança sempre que houver algum risco.

Confira tudo. Não pense que uma simples conferência gera confiança. Ter credenciais não significa ser de confiança. Significa apenas que você tem credenciais. E credencias podem ser roubadas.

Podemos dividir isso em quatro princípios básicos para manter em mente.



Sempre identifique

Você precisa de uma fonte única e competente de identidade e sempre utilizá-la com logon único (SSO). Tudo deve ser autenticado, com autenticação multifator (MFA). Não importa onde o usuário se encontra ou o que está tentando acessar, valide suas credenciais, valide o segundo (ou terceiro) fator e, regularmente, exija a reautenticação.

Se as credenciais forem roubadas ou um sistema for sequestrado, MFA e reautenticação regular irão rapidamente bloquear um invasor.

Sempre controle

Aplique controles e verificações sempre que necessário e adote e execute o princípio do privilégio mínimo – os usuários devem ter acesso apenas ao básico de que precisam para realizar seus trabalhos. Se houver um sistema de recursos humanos usado apenas por funcionários na Alemanha, só a equipe alemã deverá ter acesso a ele. Ninguém mais deveria ter acesso, mesmo que o risco de ter tal acesso seja irrisório.

Sempre analise

Simplesmente porque a autenticação teve êxito, ou o acesso foi concedido a determinado usuário ou dispositivo, isso não significa que seja confiável. Ameaças internas e maus elementos podem pôr as mãos em credenciais válidas. Grave toda a atividade da rede e do sistema e regularmente analise e inspecione para verificar o que ocorre após a autenticação. SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), bem como MDR (Managed Detection And Response) surgiram exatamente para cumprir esse propósito.

Sempre proteja

Use uma abordagem à segurança cibernética "de dentro para fora". Você deveria focar nos seus dados importantes e cuidar deles, identificando pontos de vulnerabilidade na jornada de seus dados pela rede do momento que são criados até o momento que são destruídos.

Sempre considere o risco acima de tudo e não a conformidade ou regulamentações. Usar a segurança puramente para atender a uma verificação de conformidade ou requisito regulamentar é perigoso. Os requerentes de conformidade não sabem o que está na sua rede, seus fluxos e cargas de trabalho, sistemas e tecnologias. Eles não conhecem os riscos relevantes a cada um dos elementos da sua rede. Considerar o risco e modelar as ameaças que a sua organização enfrenta irá lhe assegurar onde a segurança deve ser aumentada, relaxada e microssegmentada.

Aproximando-se do Zero Trust

Como avançar para o Zero Trust e aproveitar todos os seus benefícios vantajosos?

Defina sua superfície e identifique recursos | Mapeie caminhos regulares e privilegiados | Arquitete uma rede Zero Trust | Crie políticas de Zero Trust | Monitore e mantenha seus perímetros

Defina sua superfície e identifique recursos

Primeiramente, você precisa definir qual superfície deseja proteger, controlar e monitorar. Quais são os recursos, serviços, aplicativos e dispositivos usados no seu negócio? Ter um escopo claro de tudo que está em uso na sua rede inteira ajuda na aplicação mental do nosso novo Zero Trust.

Mapeie caminhos regulares e privilegiados

Assim que tiver tudo claramente definido, você precisará mapear caminhos regulares: quais são os fluxos, comportamentos e relações entre tudo o que é regular e esperado? Este grupo de usuários acessará este aplicativo, este dispositivo se conectará a esta rede, este serviço usará este repositório de dados e assim por diante, mas também, quais são os caminhos privilegiados? Este administrador vai querer se conectar a este painel de gerenciamento e usar o protocolo RDP (Remote Desktop Protocol) para acessar o servidor que hospeda dados confidenciais, etc. Caminhos privilegiados muito provavelmente precisarão de segurança ou controles extras aplicados a eles.

Arquitete uma rede Zero Trust

Agora que você já sabe o que está no escopo e quais são as relações entre tudo, pode começar a aplicar a filosofia Zero Trust. Identifique quais medidas de segurança e controles de acesso deseja aplicar e onde, qual tecnologia irá melhor mitigar qual risco e assim por diante.

Crie políticas de Zero Trust

A seguir, você precisa implementar políticas de Zero Trust que farão uso de fontes de dados o máximo possível, para adicionar contexto a conexões ou solicitações.

Monitore e mantenha seus perímetros

Por fim, e talvez o mais importante: você precisa sobrepor tudo com monitoramento detalhado de modo que possa manter nossos parâmetros recém-criados.

Essa é uma das maiores mudanças que os administradores enfrentam. Antes, você podia instalar e configurar um antivírus sem se preocupar em averiguar o painel; com o Zero Trust, você vai precisar mudar seus hábitos.

Você precisa monitorar os eventos que ocorrem, beneficiando-se de ferramentas como EDR para entender a causa raiz de como uma ameaça entra em um ambiente e quais eventos ocorreram antes da detecção ou após uma possível violação.

Serviços como MDR podem realmente ajudar aqui, capacitando os especialistas em segurança cibernética a ajudá-lo a monitorar a sua rede e aniquilar as ameaças para você.

A tecnologia Zero Trust

Você precisa de um grande volume de tecnologias para proteger todos os recursos e ativos que tem na rede. Nenhum fornecedor, produto ou tecnologia resolverá todos os seus problemas.

A tecnologia Zero Trust precisa atender duas áreas principais: o gerenciamento do Zero Trust e a segurança e controle dos seus vários recursos e ativos.

Gerenciamento se divide em três subáreas:

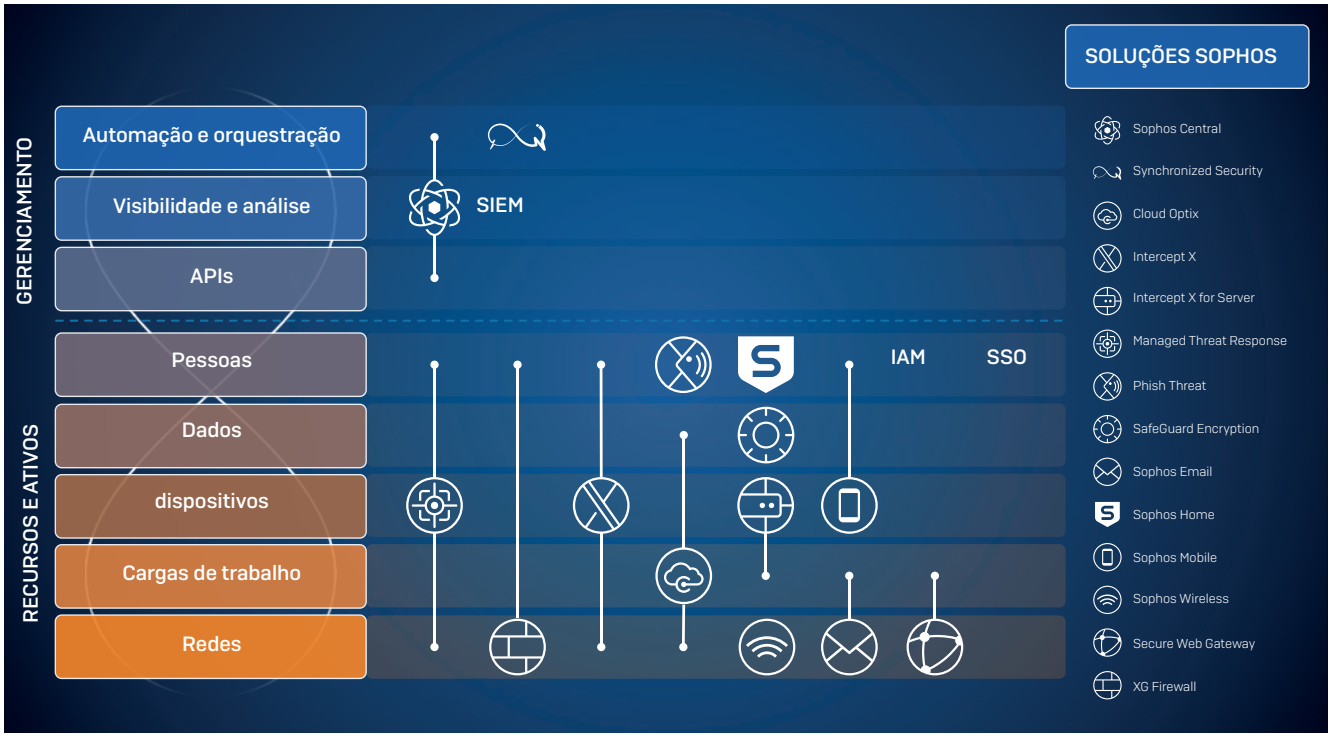
1. Automação e orquestração – por definição são políticas dinâmicas que coordenam todas as diferentes tecnologias e colocam tudo em seu devido lugar
2. Visibilidade e análises – para supervisão de manutenção da rede, assegurando que esteja tudo funcionando, bem como identificar ameaças e violações se ou quando ocorrerem
3. APIs – para integração de suas várias tecnologias, retirando dados de um sistema e colocando em outro

Recursos e ativos se dividem em cinco subáreas:

1. Pessoas – os usuários, administradores e outros que trabalham na sua empresa ou para ela
2. Dados – a força vital de todas as organizações e talvez o ativo mais importante a proteger
3. Dispositivos – os servidores, laptops, máquinas virtuais, etc. que você usa para realizar seus negócios
4. Cargas de trabalho – os serviços e aplicativos que você usa para processar dados, realizar cálculos, gerar relatórios, etc.
5. Redes – os canais de comunicação pelos quais fluem dados, web, e-mail, Wi-Fi, Internet e assim por diante

Como a Sophos pode ajudar

Um único fornecedor não pode levar a sua organização ao modelo Zero Trust, mas a Sophos tem uma ampla linha de tecnologias para ajudar você a chegar lá.



O gerenciamento do Zero Trust

Sophos Central, a nossa plataforma de segurança cibernética nativa na nuvem, lhe permite gerenciar o seu ambiente Zero Trust. Ele coordena todas as suas tecnologias em um único painel, oferecendo uma visão total de todas as tecnologias em um só lugar e APIs para interconectá-las a quaisquer outras tecnologias de terceiros.

Você pode ainda trabalhar com um SIEM para agregar logs de seus produtos Sophos e não Sophos para facilitar a supervisão total do que está acontecendo. Nossas APIs facilitam mover informações de nossa plataforma Sophos Central para os SIEMs que você estiver usando.

O **Sophos Synchronized Security** (controlado através do Sophos Central) também desempenha um papel importante aqui. Com a Segurança Sincronizada ativada, as soluções Sophos compartilham informações entre elas e respondem automaticamente a incidentes. No contexto Zero Trust, as soluções são capazes de se adaptar aos cenários por meio de políticas dinâmicas e automatizar tarefas complexas, como isolar máquinas por exemplo.

Segurança e controle de recursos e ativos

Muitos dos nossos produtos o ajudam a proteger vários recursos e ativos simultaneamente, o que de forma alguma significa que você não possa implantar apenas uma tecnologia e seguir o seu caminho. Proteger as pessoas, por exemplo, requer um grande volume de diferentes tecnologias como parte de uma rede Zero Trust arquitetada com resiliência.

Cloud Optix oferece a análise e visibilidade contínuas de que as organizações precisam para detectar, responder e impedir lacunas em segurança e conformidade da rede que levam à exposição. Em um ambiente Zero Trust, o Cloud Optix pode ajudar a proteger dados, dispositivos, cargas de trabalho e redes na nuvem pública.

Intercept X oferece proteção sem igual para endpoints e dá um basta a uma infinidade de ataques com uma combinação única de detecção de malware, prevenção contra exploração de vulnerabilidades, detecções comportamentais e anti-ransomware por Deep Learning. Em um ambiente Zero Trust, o Intercept X pode ajudar a proteger todos os seus recursos e ativos.

Intercept X for Server foi projetado para proteger ambientes de servidores na nuvem, no local ou híbridos. Em um ambiente Zero Trust, o Intercept X for Server pode ajudar a proteger dispositivos e cargas de trabalho.

Managed Threat Response (MTR) é a nossa solução de resposta a ameaças ditada por nossos especialistas. Ela funde a tecnologia de Machine Learning com o intelecto humano para oferecer serviço 24 horas de caça, detecção e resposta a ameaças. Em um ambiente Zero Trust, o MTR pode ajudar a proteger todos os seus recursos e ativos.

Phish Threat é a nossa solução anti-phishing dedicada. Ela oferece a seus funcionários treinamento no entendimento e conscientização sobre segurança, além de relatórios criados para medir o preparo da sua organização para lidar com ameaças de phishing. Em um ambiente Zero Trust, o Phish Threat pode ajudar a proteger o seu pessoal.

SafeGuard Encryption criptografa o conteúdo assim que é criado. Ele protege proativamente os seus dados ao validar continuamente os usuários, os aplicativos e a integridade de segurança de um dispositivo antes de permitir acesso a dados criptografados e, assim, em um ambiente Zero Trust, pode ajudar a proteger os seus dados.

Secure Web Gateway facilita a proteção avançada da Web, oferecendo níveis inusitados de segurança, controle e insights da Web. Em um ambiente Zero Trust, o Secure Web Gateway pode ajudar a proteger redes e cargas de trabalho.

Sophos Email utiliza inteligência artificial para oferecer segurança de e-mail hábil e preditiva. Em um ambiente Zero Trust, o Sophos Email pode ajudar a proteger suas redes e cargas de trabalho.

Sophos Home foi projetado para proteger computadores em ambientes domésticos e se baseia na mesma tecnologia presente em muitos de nossos produtos comerciais. Em um ambiente Zero Trust, o Sophos Home pode ajudar a proteger o seu pessoal.

Sophos Mobile é a nossa solução UEM (Unified Endpoint Management) que ajuda as empresas a despender menos tempo e esforços para gerenciar e proteger seus endpoints convencionais e móveis. Em um ambiente Zero Trust, o Sophos Mobile pode ajudar a proteger os seus dispositivos, os seus dados e o seu pessoal.

Sophos Wireless oferece uma maneira fácil e eficaz de gerenciar e proteger suas redes sem fio. Em um ambiente Zero Trust, o Sophos Wireless pode ajudar a proteger as suas redes.

XG Firewall oferece ampla proteção de firewall Next Gen que expõe riscos ocultos, bloqueia ameaças desconhecidas e responde automaticamente a incidentes. Em um ambiente Zero Trust, o XG Firewall pode ajudar a proteger todos os seus recursos e ativos.

Empregar essas tecnologias colocará você em posição de vantagem para mudar para o modelo Zero Trust. Contudo, como mencionado anteriormente, nenhum fornecedor ou tecnologia por si só, inclusive a Sophos, pode levar você à plenitude de um ambiente Zero Trust. Para capacitar seus usuários a usarem os serviços da nuvem onde estiverem, você precisará também de uma solução IAM (Identity Access Management) sólida em operação com logon único (SSO) para usar a sua fonte competente de identidade em todos os seus sistemas e serviços – isso é uma parte essencial do Zero Trust.

Você pode obter mais informações e iniciar demonstrações instantâneas de nossos produtos e serviços em www.sophos.com.

Nossa visão da segurança cibernética

Zero Trust e nossa visão da segurança cibernética, a Segurança Sincronizada, compartilham muitos desses objetivos e se complementam.

A Segurança Sincronizada é a segurança virtual como um sistema. Ela analisa, adapta e automatiza continuamente as tarefas mais complexas em TI enquanto monitora dinamicamente toda a atividade do sistema, o comportamento do usuário, o tráfego de rede e as posturas de conformidade em tempo real. As tecnologias compartilham informações entre si, oferecendo insight e visibilidade umas às outras, o que, do contrário, resultaria em tecnologias independentes e desconexas.

A tecnologia fala, e deveria falar, pois só assim podemos obter as políticas adaptativas e dinâmicas de que precisamos, com base em múltiplas fontes de dados, para conquistarmos a rede Zero Trust.

Conclusão

Da maneira como é vista, Zero Trust é uma filosofia voltada à segurança cibernética com apenas alguns poucos prontos para abarcá-la. Contudo, os perímetros de segurança estão se desgastando pouco a pouco, e a necessidade de adoção aumentando e ficando cada vez mais predominante. Os criminosos cibernéticos estão ficando mais e mais inovadores, enquanto as defesas correm atrás com dificuldade para tentar manter o ritmo. O modelo Zero Trust representa uma forma real de minimizar ameaças ao mesmo tempo em que define novos padrões em protocolo de segurança cibernética.

É hora de pensar diferente. É hora de evoluir.

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

20-03-10 WP-PTBR (DD)

SOPHOS