McAfee MVISION Private Access

O McAfee® MVISION™ Private Access é a primeira solução do mercado em acesso a rede com confiança zero (Zero Trust Network Access ou ZTNA) e reconhecimento de dados, protegendo o acesso a aplicativos privados, de qualquer lugar e em qualquer dispositivo, além de controlar a colaboração de dados com prevenção de perda de dados (DLP) integrada. O Private Access converge com o MVISION Unified Cloud Edge, o que confere à McAfee a exclusividade de ter a melhor solução do gênero em segurança integrada e fornecida via nuvem para distribuições aceleradas de Secure Access Service Edge (SASE).

Principais vantagens do ZTNA

- Conectividade direta com aplicativos para aplicativos privados
- Acesso baseado em contexto e identidade explícita
- Microssegmentação de rede para evitar o movimento lateral das ameaças
- Acesso com o mínimo de privilégios a aplicativos específicos e autorizados
- Blindagem de aplicativos privados contra exposição à Internet
- Redução de custos e aumento do desempenho ao substituir VPN e MPLS
- Experiência de usuário consistente para acesso a aplicativos privados e SaaS

Conecte-se conosco

A necessidade de acesso a rede com confiança zero

A transformação dos negócios e a expansão do trabalho remoto em curso invalidaram o conceito da segurança de perímetro de rede. Com os recursos corporativos saindo dos limites da empresa para múltiplos locais distribuídos, como nuvens públicas e data centers privados, as organizações têm diante de si o desafio de distribuir soluções de segurança para proteger seus dados confidenciais sem deixar de propiciar um acesso fácil, de qualquer dispositivo e localização remota.

O acesso a rede com confiança zero (Zero Trust Network Access ou ZTNA) baseia-se no modelo de segurança "Zero Trust" para impor políticas com reconhecimento de identidade e de contexto para acesso a aplicativos. Isso significa que todo recurso é negado por padrão. Cada usuário e dispositivo, seja interno ou remoto, é considerado inseguro e arriscado e sua postura de identidade e segurança precisa ser verificada antes que seja concedido acesso a recursos privados confidenciais. O ZTNA abandona a arquitetura de segurança baseada em perímetro fixo em prol de uma arquitetura de perímetro mais lógica, definida por software, que abrange um conjunto de usuários e aplicativos. Segundo a Gartner, até 2022, 80% dos novos aplicativos corporativos digitais abertos para parceiros em um ecossistema serão acessados por meio de acesso a rede com confiança zero.[1]

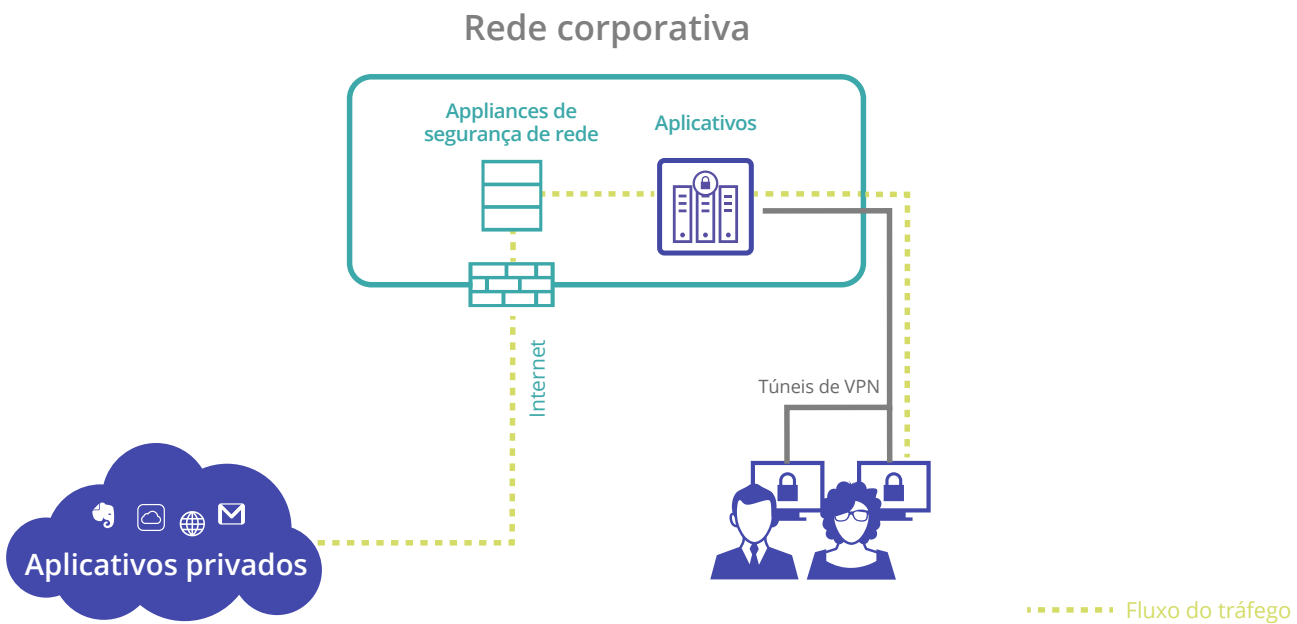

Figura 1. Arquitetura de rede tradicional

1. https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access

Introdução ao MVISION Private Access

O MVISION Private Access é a primeira solução do mercado em acesso a rede com confiança zero acompanhada de capacidades integradas de prevenção de perda de dados (DLP) e Remote Browser Isolation (RBI). Isso permite às organizações viabilizar acesso "Zero Trust" granular aos aplicativos privados, aplicar políticas para prevenir a perda de dados confidenciais durante colaborações e proteger aplicativos privados contra dispositivos não gerenciados e potencialmente arriscados por meio de sessões de Web completamente isoladas.

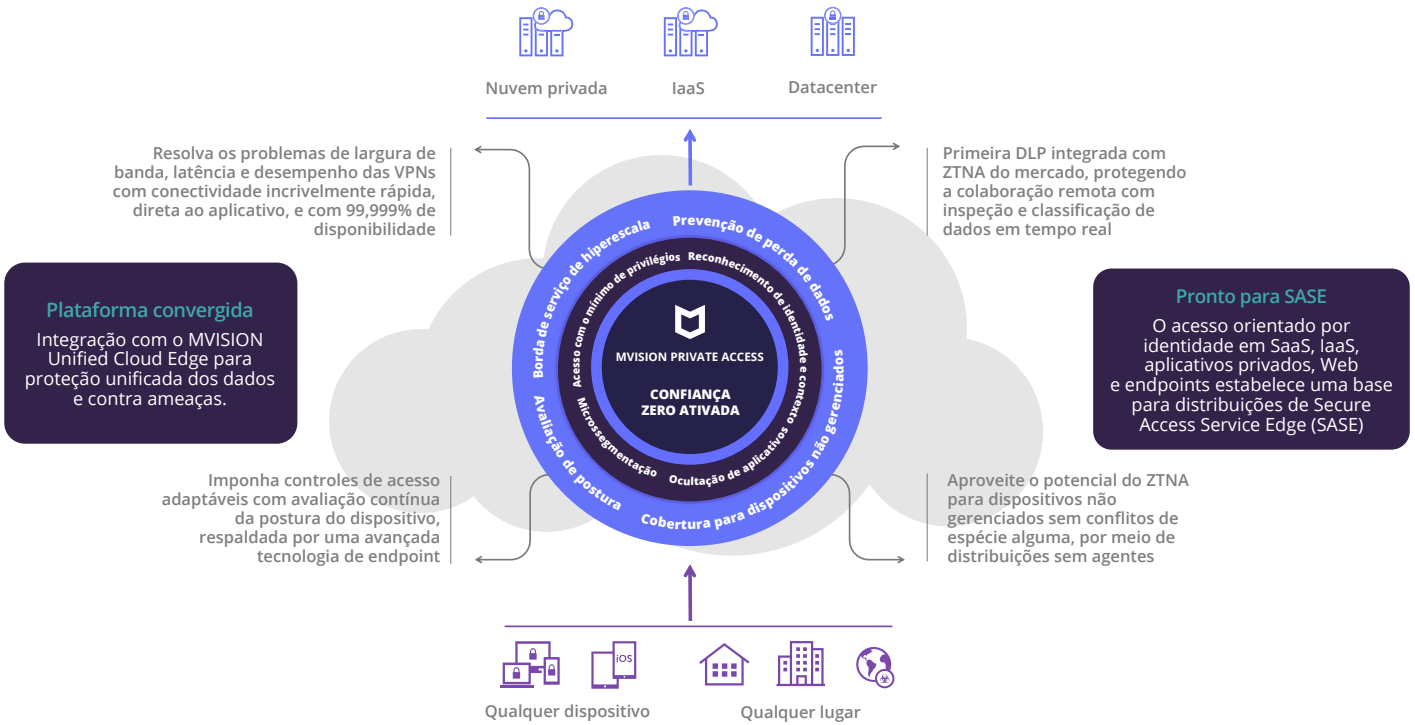

Figura 2. McAfee MVISION Private Access

Substituição da VPN por conectividade direta com o aplicativo

As VPNs não foram projetadas para situações em que a maioria dos funcionários se conecta remotamente a distribuições baseadas na nuvem, o que resulta nos seguintes desafios:

- Os dados e aplicativos corporativos que os usuários precisam acessar encontram-se distribuídos em múltiplos lugares. O roteamento de conexões remotas através de hubs de VPN centralizados cria problemas significativos de latência.
- O aumento exponencial no tráfego dos funcionários remotos consumiu a largura de banda e sobrecarregou a capacidade da infraestrutura.
- Um modelo de confiança implícita excessiva permite total acesso à rede privada a qualquer usuário com chaves de login válidas, aumentando o risco de exposição de dados e movimentação lateral das ameaças.

A solução da McAfee

O MVISION Private Access utiliza a borda de serviço de hiperescala para viabilizar acesso seguro e direto aos aplicativos privados. A conectividade onipresente reduz a latência de rede e propicia uma experiência de usuário consistente e uniforme ao acessar tanto aplicativos privados quanto SaaS.

Vantagens

- A borda de serviço de hiperescala funciona com 99,999% de disponibilidade, oferecendo acesso ininterrupto a recursos corporativos.
- Diferentemente das VPNs, que permitem acesso total à rede para os usuários autenticados, o Private Access microssegmenta as redes e oferece acesso com "privilégios mínimos" a aplicativos autorizados específicos, e não à rede subjacente inteira.

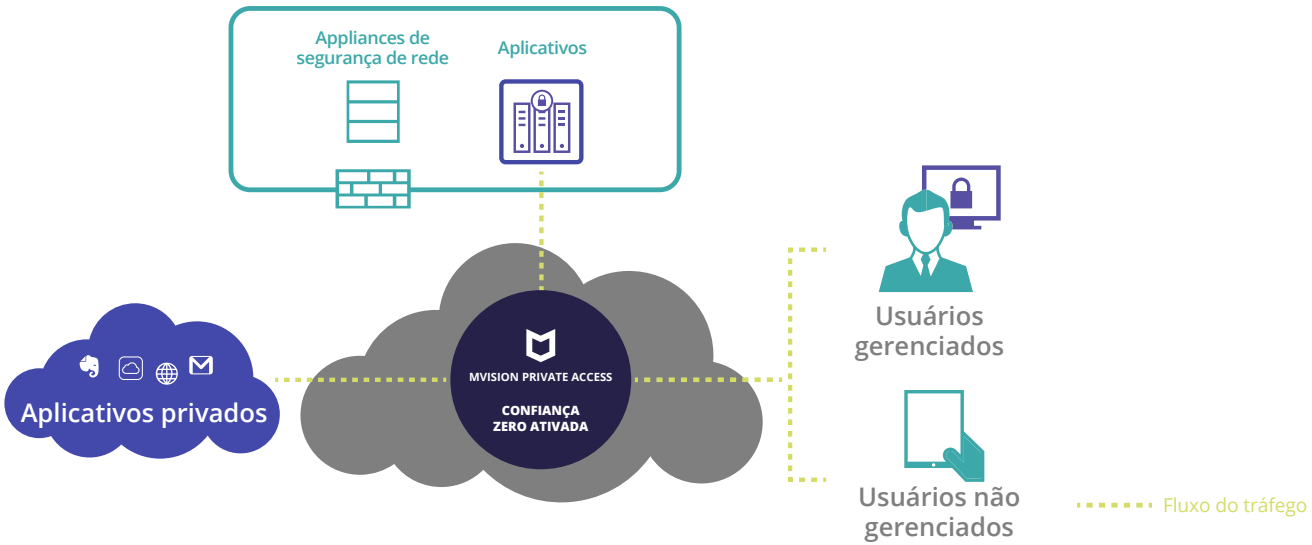

Figura 3. Acesso direto ao aplicativo com o McAfee MVISION Private Access

Proteção de dados integrada para colaboração remota segura

Embora os fornecedores tradicionais de ZTNA enfatizem a proteção de acesso remoto para aplicativos privados, eles não têm a capacidade de proteger os dados confidenciais dentro desses aplicativos. Quando a força de trabalho é distribuída, os dados podem ser acessados e compartilhados entre dispositivos gerenciados e não gerenciados, terceiros ou serviços de nuvem conectados. É da maior importância impor salvaguardas e evitar a perda de dados por parte de qualquer dos entes conectados.

A solução da McAfee

O MVISION Private Access é acompanhado de prevenção de perda de dados (DLP) integrada para permitir controle total sobre os dados compartilhados através de sessões privadas, com políticas de DLP em linha.

Vantagens

- A inspeção e classificação profunda de dados utilizando DLP em linha impede o manuseio indevido de dados confidenciais por parte de usuários remotos que estejam colaborando, em qualquer lugar ou dispositivo.
- Ao unificar a DLP e a proteção contra ameaças em acesso privado, endpoints, nuvem e Web, as equipes de segurança são beneficiadas pela integração de visibilidade e controle sobre os dados confidenciais.

Possibilidade de controle de acesso adaptável com base nas condições do dispositivo e na avaliação da postura de segurança

Com o aumento de usuários remotos conectando-se de qualquer lugar e dispositivo, as políticas precisam ser mais flexíveis e as organizações devem considerar múltiplos parâmetros contextuais — como perfil de risco do usuário ou postura do dispositivo — antes de conceder acesso aos aplicativos. O contexto do acesso pode incluir tipo de dispositivo, tipo de usuário, sistema operacional do dispositivo, detalhes do antivírus, horário de acesso, localização ou serviços acessados, para citar alguns exemplos.

A solução da McAfee

O MVISION Private Access aproveita o McAfee Endpoint Security, líder do setor e respaldado pela inteligência proativa sobre ameaças obtida por um bilhão de sensores, para avaliar a postura do dispositivo e do usuário, a qual informa, em tempo real, uma decisão com confiança zero baseada em risco. A postura de segurança é determinada por meio de um cliente leve de endpoint instalado no dispositivo remoto que consulta os atributos do dispositivo e permite que os usuários imponham políticas adaptáveis de controle de acesso. Os usuários precisarão autenticar novamente suas sessões quando alguma alteração for detectada na postura do dispositivo.

Vantagens

- O cliente do McAfee Endpoint Security vai além da verificação básica de postura realizada por soluções concorrentes ao obter um conjunto detalhado de dados de telemetria, incluindo tipo de dispositivo, detalhes sobre o usuário conectado, último status de varredura e última atualização de software para ressaltar o contexto completo da sessão do usuário por meio de avaliação de postura.
- A avaliação da postura de segurança do dispositivo do usuário final ajuda na minimização do risco de que malfeitores ou usuários comprometidos inadvertidamente conectem-se a aplicativos privados, criando um ambiente de ZTNA mais resiliente e aprimorando a base geral de segurança das organizações.
- O monitoramento contínuo da postura de risco permite que as organizações encerrem em tempo real as conexões arriscadas com base em insights contextuais adicionais.

Figura 4. Atributos de postura do dispositivo

Suporte sem conflitos para dispositivos não gerenciados

A recente mudança para ambientes de trabalho remoto aumentou significativamente o percentual de usuários que se conectam para trabalhar por meio de dispositivos não gerenciados, pertencentes ao próprio usuário (BYO). Frequentemente, esses dispositivos conectam-se por redes remotas inseguras, contornando os controles dos sistemas de segurança tradicionais. As organizações incentivam a colaboração baseada na nuvem para aumentar a produtividade, mas o acesso não supervisionado aos dados, o compartilhamento de dados por meio de dispositivos não gerenciados e os desafios envolvidos na imposição de políticas de segurança de endpoint, de nuvem e de Web para esses dispositivos introduzem o risco de exposição de dados confidenciais e ataques cibernéticos.

A solução da McAfee

O MVISION Private Access protege dispositivos não gerenciados através de uma distribuição sem agente, baseada em navegador, além de sessões do Remote Browser Isolation (RBI). A conexão iniciada pelo navegador permite colaboração entre funcionários, parceiros externos ou terceirizados sem conflitos de espécie alguma.

Vantagens

- Viabilização de acesso seguro e uniforme a aplicativos privados por meio de dispositivos não gerenciados, sem exigir instalação alguma de agentes consumidores de recursos.
- Isolamento do acesso por meio de sessões do Remote Browser Isolation (RBI) para proteger os aplicativos privados contra dispositivos não gerenciados, arriscados e não confiáveis.
- Definição de políticas contextuais de controle de acesso para limitar o acesso aos recursos privados com base na postura de segurança e na classificação do dispositivo.

Aceleração do roteiro para implementação de SASE

Ao prescrever uma convergência entre rede e segurança de rede em um modelo de serviço unificado fornecido via nuvem, a Secure Access Service Edge (SASE) busca atender os requisitos de acesso seguro e dinâmico dos empreendimentos digitais. Por estabelecer um acesso seguro e orientado pela identidade aos aplicativos, o ZTNA é considerado um componente essencial da arquitetura SASE.

O MVISION Private Access foi projetado utilizando as diretrizes da estrutura de segurança da McAfee, integrando-se perfeitamente com outros componentes do McAfee Unified Cloud Edge (UCE), os quais incluem Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) e proteção de endpoints. A solução integra-se com provedores de identidade, como Microsoft Active Directory e Okta, para autenticação SAML baseada em SSO para autenticar e validar continuamente a identidade dos usuários que acessam aplicativos privados.

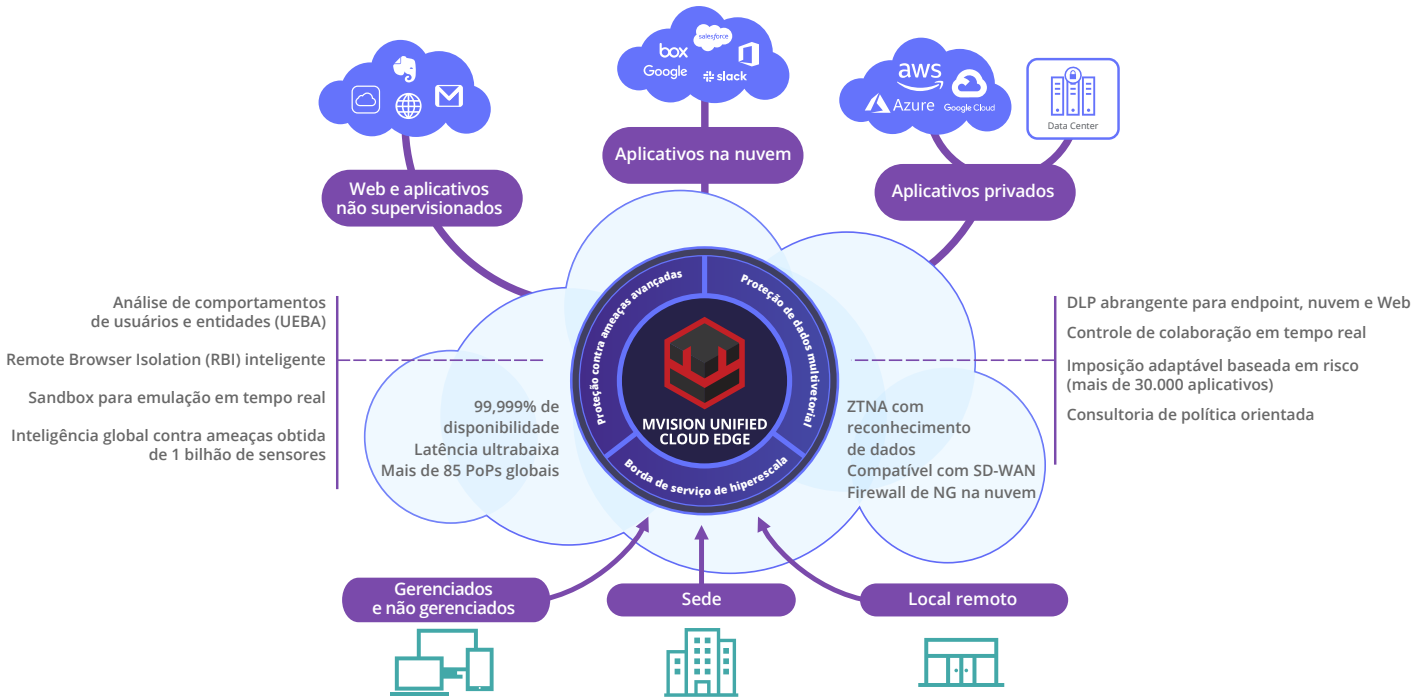

Figura 5. McAfee MVISION Unified Cloud Edge

Isso dá à McAfee o privilégio de resolver o quebra-cabeça da segurança de rede da SASE com uma solução unificada que leva em consideração a complexidade das distribuições de forças de trabalho remotas com gerenciamento centralizado de incidentes e visibilidade, controle de acesso adaptável e granular, proteção de dados de ponta a ponta e proteção contra ameaças avançadas do dispositivo à nuvem.

Ao fazer parceria com os maiores fornecedores de SD-WAN, a McAfee reúne uma segurança de rede onipresente a um fornecimento de serviços simplificado, confiável e de baixa latência para estabelecer um roteiro para implementação de distribuições aceleradas de SASE.

Saiba mais

Para obter mais informações, visite-nos em **www.mcafee.com/br**.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br