

## Forcepoint ONE

# Zero Trust Network Access

Simplifique a segurança para apps privados sem uma VPN

### Casos de Uso

- › Substitua as VPNs para acessar aplicativos privados em data centers e nuvens privadas.
- › Forneça acesso seguro e sem agente a aplicativos da Web privados, usando dispositivos BYOD e não administrados.
- › Controle o upload e o download de dados confidenciais em qualquer aplicativo da web privado.
- › Bloqueie malwares ocultos em arquivos de dados corporativos de/para aplicativos da Web privados.
- › Proteja o acesso a servidores privados usando dispositivos Windows e macOS administrados.

### Solução

- › Segurança de apps privados integrada com proteção contra ameaças avançadas e DLP.
- › Controles de acesso sem agente e Zero Trust para aplicativos da Web privados em dispositivos BYOD e administrados.
- › Acesso remoto a aplicativos privados não Web a partir de dispositivos Windows e macOS administrados.
- › Parte de uma plataforma de nuvem com SWG, CASB e outros recursos de segurança.

### Resultado

- › Aumente a produtividade, permitindo que as pessoas acessem aplicativos privados de forma transparente e segura de qualquer lugar.
- › Reduza os custos, simplificando as operações de segurança com um único local para definir políticas.
- › Reduza o risco, com controle de dados confidenciais e malware em trânsito de/para aplicativos da Web privados.
- › Simplifique a conformidade com processos demonstráveis para controlar informações.

O trabalho remoto expôs as limitações, custos e riscos das redes privadas virtuais (VPNs). Depois de conectadas, as VPNs concedem confiança implícita excessiva, permitindo que os usuários verifiquem e sondem outros endereços IP nesse data center privado ou nuvem privada virtual, o que abre a porta para invasões. No entanto, as empresas que desejam migrar de VPNs para soluções Zero Trust Network Access (ZTNA) não precisam enfrentar mais complicações e produtos pontuais: a adoção do acesso Zero Trust deve ser simples e tranquila.

O ZTNA da Forcepoint controla o acesso a aplicativos privados da Web e não Web que cada funcionário, contratado e parceiro tem permissão explícita para usar. O Forcepoint ZTNA oferece controle infinitamente maior com a confiança de permitir que as pessoas usem os dispositivos que funcionam melhor para elas, mesmo dispositivos não administrados e BYOD.

Diferente de outras soluções, o Forcepoint ZTNA também oferece controles contínuos e refinados, o melhor desempenho do setor, proteção integrada contra malware e proteção de dados para oferecer uma ótima experiência ao usuário, apesar das complexidades das redes modernas. Você também pode adicionar facilmente outras soluções de segurança, como Cloud Access Security Broker (CASB) e Secure Web Gateway (SWG), conforme necessário, totalmente integrados como parte da plataforma em nuvem Forcepoint ONE.

#### **Substitua as VPNs para acessar aplicativos privados em data centers e nuvens privadas**

O acesso seguro a aplicativos privados requer controle rápido e preciso. Você pode limitar o acesso a aplicativos privados como ERP ou servidores da cadeia de suprimentos com base em identidade, associação ao grupo, tipo de dispositivo e localização. Para aplicativos não Web, você pode aplicar controles por porta e proteger o acesso em locais ou dispositivos desconhecidos. Se a tentativa de login parecer suspeita, os usuários devem provar sua identidade por meio da autenticação multifatores (MFA). Tudo isso acontece em milissegundos com a plataforma de hiperescala da Forcepoint.

#### **Forneça acesso seguro e sem agente a aplicativos da Web privados acessados em dispositivos de funcionários**

Os usuários podem se conectar com segurança e conveniência pela Internet a aplicativos da Web hospedados atrás de um firewall, mesmo em dispositivos BYOD e não administrados, sem a necessidade de agentes.

#### **Controle o upload e o download de dados confidenciais em qualquer aplicativo da web privado**

Administre um conjunto de políticas de segurança para controlar dados confidenciais, com acesso à verificação de malware e DLP integrado para impedir hackers e violações de dados. A combinação de segurança de dados com políticas de postura e localização de dispositivos facilita o controle de como as pessoas movem dados de/para aplicativos da Web privados em qualquer dispositivo.

#### **Bloqueie malwares ocultos em arquivos de dados corporativos de/para aplicativos da Web privados**

Forcepoint bloqueia ransomware. Detecte e bloqueie malwares em dados em trânsito entre usuários e qualquer aplicativo da web privado usando os mecanismos de verificação Bitdefender e CrowdStrike.

**Proteja o acesso a servidores privados não web a partir de dispositivos administrados**

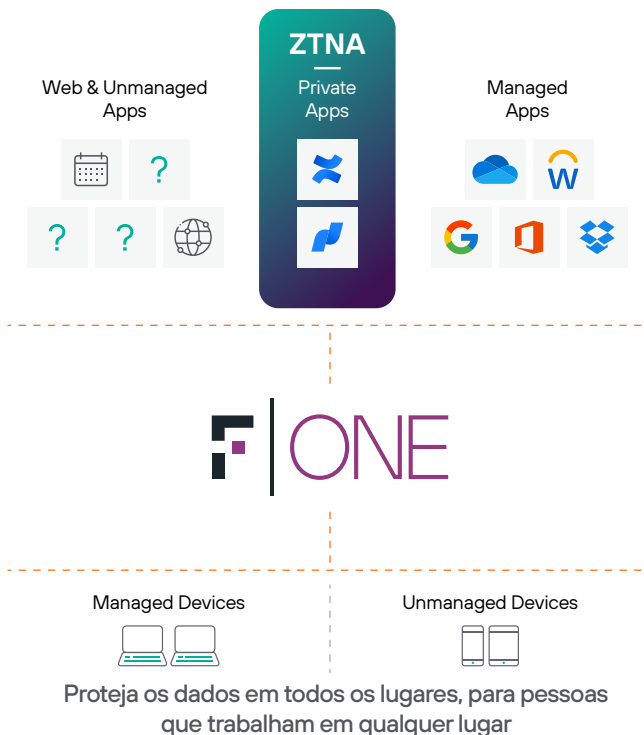
Nosso ZTNA protege o acesso remoto para protocolos fora da Web, como shell seguro (SSH) e protocolo de desktop remoto (RDP) a partir de PCs ou Macs gerenciados com o agente unificado Forcepoint ONE.

**O ZTNA no Forcepoint ONE maximiza o tempo de atividade, a disponibilidade e a produtividade**

O ZTNA faz parte do Forcepoint ONE, nossa plataforma de nuvem baseada em hyperscaler com mais de 300 pontos de presença (PoPs), acessibilidade global e tempo de atividade comprovado de 99,99% para proteger aplicativos privados de forma transparente e preservar a produtividade do usuário. Outras soluções desviam o tráfego de rede por meio de data centers privados em vez de locais próximos aos usuários, o que pode gerar desempenho insatisfatório. O Forcepoint ONE unifica CASB, SWG e ZTNA para proteger o acesso a aplicativos corporativos SaaS, da web e privados, simplificando a segurança.

**Simplificando a segurança de apps privados no mundo real**

A plataforma em nuvem Forcepoint ONE fornece um "botão fácil" para implementar a segurança de apps privados. Em uma console, os administradores podem gerenciar o acesso e controlar downloads e uploads de arquivos para usuários de dispositivos administrados e não administrados (como BYOD e computadores de fornecedores ou parceiros).



**Vamos ver como o recurso ZTNA simplifica a segurança de apps privados quando Carlos, gerente de compras que trabalha em casa, inicia seu dia de trabalho.**

<p><b>Carlos faz login no Forcepoint ONE usando o notebook corporativo.</b></p>	<p>Como Carlos está tentando fazer login em um dispositivo administrado e um local permitido, o acesso é concedido. Uma tentativa de login de um local desconhecido requer uma resposta bem-sucedida por meio de aplicativos MFA.</p>
<p><b>Carlos obtém acesso com um clique ao aplicativo proprietário da cadeia de suprimentos da empresa no portal de usuários Forcepoint ONE.</b></p>	<p>O navegador de Carlos exibe o portal Forcepoint ONE, mostrando blocos para cada aplicativo da web que Carlos e seus parceiros da cadeia de suprimentos podem acessar. (Se a empresa de Carlos usa o CASB do Forcepoint ONE, os aplicativos SaaS administrados de Carlos podem ser acessados no mesmo portal do usuário para uma experiência consistente.)</p>
<p><b>Carlos recebe acesso ao aplicativo administrado.</b></p>	<p>O tráfego entre o notebook de Carlos e o aplicativo de cadeia de suprimentos passa automaticamente pelo proxy reverso do Forcepoint ONE. O Forcepoint verifica uploads e downloads de arquivos em busca de malware e dados confidenciais.</p>
<p><b>Carlos faz upload de um contrato de fornecedor como anexo.</b></p>	<p>Como a política para a conexão de Carlos exige a verificação de arquivos, o upload é permitido se o arquivo estiver livre de malware. Se estiver infectado, o gateway ZTNA bloqueia o upload, alerta Carlos e registra e relata o evento de bloqueio.</p>

## Parte de uma solução de segurança unificada para apps de web, nuvem e privados

Além do ZTNA, a plataforma all-in-one Forcepoint ONE protege o acesso a informações comerciais em qualquer site de Internet e aplicativo privado:

- **Internet:** O SWG monitora e controla as interações com qualquer site de Internet com base no risco e na categoria, bloqueando o download de malware ou uploads de dados confidenciais para compartilhamento de arquivos pessoais e contas de e-mail. Nosso SWG no dispositivo impõe políticas de uso aceitável em dispositivos administrados em qualquer lugar.
- **Nuvem:** O CASB protege e simplifica o acesso a locatários corporativos de SaaS e IaaS enquanto controla a transmissão de dados confidenciais e malware, sem a necessidade de um agente no dispositivo.
- **Recursos adicionais,** como RBI ou varredura de provedores de nuvem para configurações arriscadas (CSPM), conforme necessário.

### Leia o resumo da solução Forcepoint ONE para mais detalhes.



**Pronto para proteger dados em aplicativos na nuvem a partir de qualquer dispositivo?**

**Vamos começar com uma demonstração.**

[forcepoint.com/contact](https://forcepoint.com/contact)