Forcepoint ONE

Uma plataforma Data First SASE exclusiva

Forcepoint

Whitepaper

forcepoint.com/pt-br

Sumário

A disrupção cria oportunidades para acelerar a transformação

Há anos, a "transformação digital" está em evidência. Antes de 2020, os aplicativos estavam saindo lentamente dos data centers corporativos para a nuvem. Uma pequena parcela de pessoas trabalhava algumas vezes remotamente, usando geralmente dispositivos móveis, como telefones e tablets, para complementar os notebooks corporativos. Então chegou a pandemia e tudo mudou.

De uma hora para outra, a maioria dos funcionários começou a trabalhar em casa. Com a produtividade em jogo, muitas organizações adaptaram-se acelerando sua migração para aplicativos baseados na nuvem, os quais os usuários poderiam acessar com muito mais facilidade do que ter que lutar com VPNs para conectar-se aos aplicativos de data center tradicionais. Embora tenha facilitado o acesso, isso também reduziu a visibilidade e o controle que as organizações de TI tinham sobre os dados confidenciais.

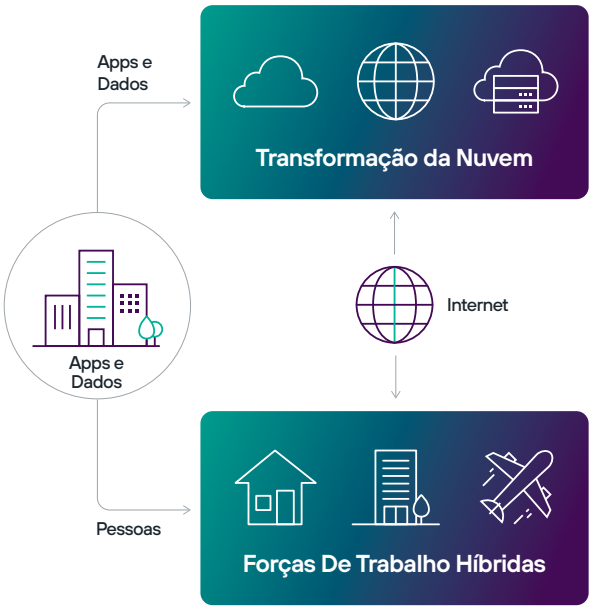
Infelizmente, os ladrões de dados também se adaptaram rapidamente, atacando aplicativos de nuvem de todas as partes do mundo. Enquanto as pessoas tentavam equilibrar sua vida pessoal e profissional nos mundos físico e digital, os "vilões" aproveitaram-se do grande número de indivíduos que não estavam acostumados a trabalhar em um mundo digital hostil. Ações simples, como usar um smartphone para acessar dados de trabalho ou navegar em sites a partir de um notebook de trabalho para fazer compras, criavam oportunidades para phishing, drive-by downloads e outras formas de comprometimento.

Trabalhar a partir de qualquer lugar está mudando tudo. Novamente.

Quando a pandemia abrandou, as pessoas começaram a voltar aos escritórios, mas não como faziam em 2019. Mesmo agora, poucas organizações voltaram aos antigos padrões de trabalho. Embora muitas empresas e órgãos governamentais estejam tentando incentivar as pessoas a passarem mais tempo no escritório, este não é mais o local padrão em que o trabalho é realizado. Muitas pessoas agora veem o escritório como um lugar que visitam, da mesma forma que costumavam considerar as viagens a lugares, parceiros ou clientes distantes.

Além disso, muitos funcionários tornaram-se dependentes de telefones e tablets (BYOD — traga seu próprio dispositivo) para manterem-se conectados quando não estão em sua mesa de trabalho. O que costumava ser uma comodidade para poucos, agora é a forma padrão com que as pessoas se mantêm produtivas em um mundo cada vez mais competitivo.

Os funcionários agora esperam — e devem — poder trabalhar **em qualquer lugar** com dados de negócios localizados **em toda parte**.



Desafio:
Adaptar-se para proteger sua empresa

Mudar onde e como as pessoas trabalham já é difícil o suficiente, mesmo nos melhores momentos. Contudo, as recentes incertezas fizeram com que muitas empresas se concentrassem primeiro em garantir que estavam preparadas para enfrentar quaisquer crises econômicas. Permitir que as pessoas utilizem os recursos de formas inovadoras — tais como usar com segurança IAs generativas, como o ChatGPT, e consumir dados a partir de BYOD, sem colocar esses dados em risco — é crucial para impulsionar as finanças de uma organização. Além disso, com os orçamentos apertados, encontrar novas eficiências em despesas de capital e operacionais é fundamental para proteger os resultados. Naturalmente, tudo isso deve ser feito com segurança, para que os dados confidenciais possam ser usados onde quer que sejam necessários, sem criar mais riscos ou provocar problemas com os auditores.

É aí que entra a Forcepoint. Acreditamos que a abordagem certa e a tecnologia correta podem transformar em oportunidade, e não em um fardo, essas rápidas mudanças na maneira como as pessoas trabalham e como as informações são gerenciadas. Foi por isso que criamos o Forcepoint ONE, nossa plataforma para simplificar o modo como você conecta e protege suas pessoas e seus dados em um mundo moderno, que coloca a nuvem em primeiro lugar. Ele se resume a ajudar você a torná-los mais produtivos e sua empresa mais eficiente, com segurança.

Aumentar a Produtividade

Cortar Custos

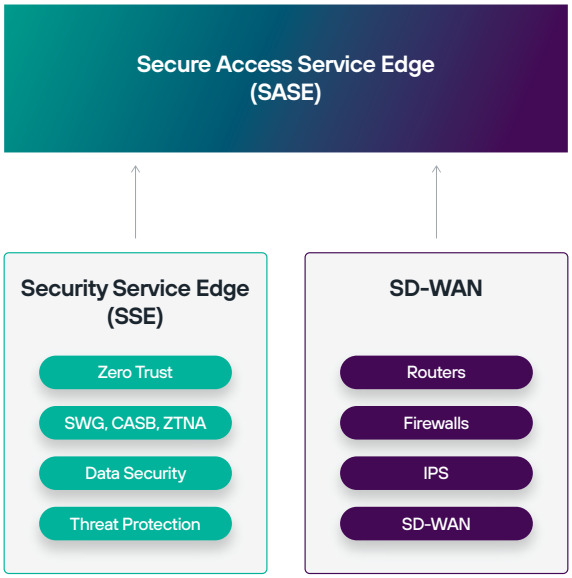
Reduzir Risco

Dinamizar a Conformidade

Solução:
Secure Access Service Edge (SASE)

Em 2019, a Gartner propôs uma nova arquitetura de TI, Secure Access Service Edge (SASE), que reúne segurança e redes, gerenciadas e frequentemente entregues como serviços a partir da nuvem.

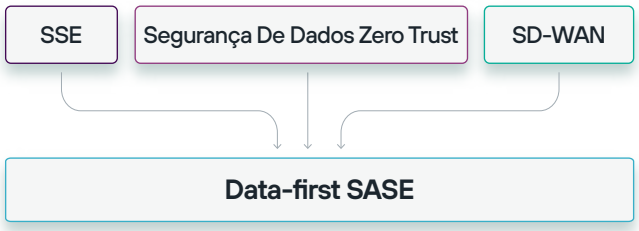
Produtos de conectividade, como firewalls, roteadores, sistemas de prevenção de invasões e redes centradas em aplicativos, já começaram a convergir para uma nova geração de soluções SD-WAN unificadas. Da mesma forma, as arquiteturas SASE facilitam aos gateways de segurança aplicar políticas para proteção contra ameaças baseada em Zero Trust e segurança de dados de forma consistente em todos os acessos da web (SWG), da nuvem (CASB) e de aplicativos privados (ZTNA). Posteriormente, a Gartner começou a se referir a essa abordagem unificada para segurança como Security Service Edge (SSE).



Forcepoint ONE: Uma plataforma Data-first SASE

A Forcepoint foi um dos primeiros proponentes da arquitetura SASE. Ela representa muitos dos princípios e tecnologias que ajudamos a promover para conectar e proteger empresas distribuídas e órgãos governamentais. Quando a pandemia forçou todas as organizações a se tornarem altamente distribuídas, o SASE transformou-se no caminho certo, no momento certo, para entregar a produtividade e a eficiência que nossos clientes estavam pedindo.

No entanto, acreditamos que o SASE é o ponto de partida para uma arquitetura moderna baseada na nuvem, não a linha de chegada. A Forcepoint vai além de apenas proteger o acesso aos recursos de negócios — protegemos o uso contínuo de dados confidenciais em todos os lugares, desde o endpoint até a nuvem. Chamamos essa abordagem de Data-first SASE.



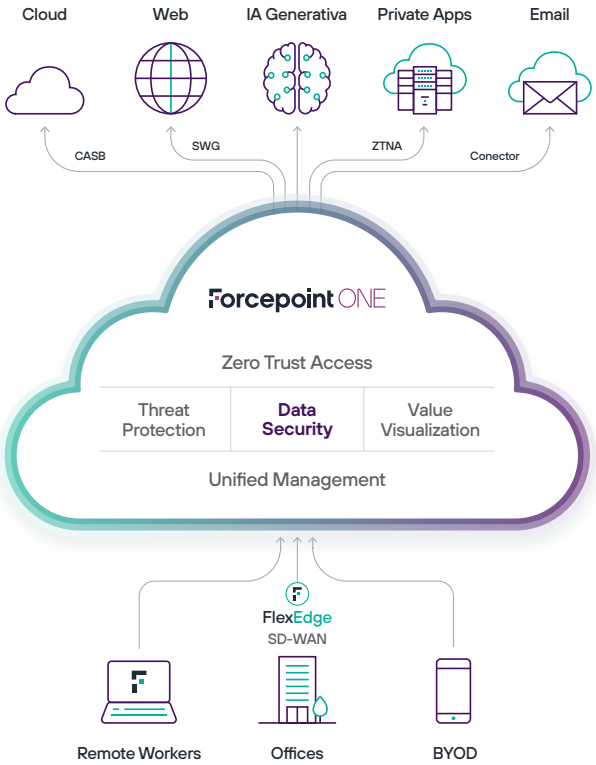
Nossa plataforma Data-first SASE, Forcepoint ONE, une uma ampla gama de tecnologias na nuvem a fim de simplificar a segurança para empresas distribuídas e órgãos governamentais. Ela oferece aos funcionários, prestadores de serviços e outros usuários acesso seguro e controlado às informações de negócios na nuvem, na web e em aplicativos privados, mantendo os invasores fora e os dados confidenciais dentro. Como resultado, os usuários podem ser mais produtivos, seja em casa ou no escritório, enquanto as empresas são mais eficientes.

Usos mais comuns do Forcepoint ONE

Com o Forcepoint ONE, as organizações podem abordar os desafios atuais com facilidade e de maneira gradual. Isso permite que as equipes de TI resolvam problemas imediatos rapidamente e adicionem recursos, conforme necessário, no futuro. Em resumo, é "Segurança Simplificada".

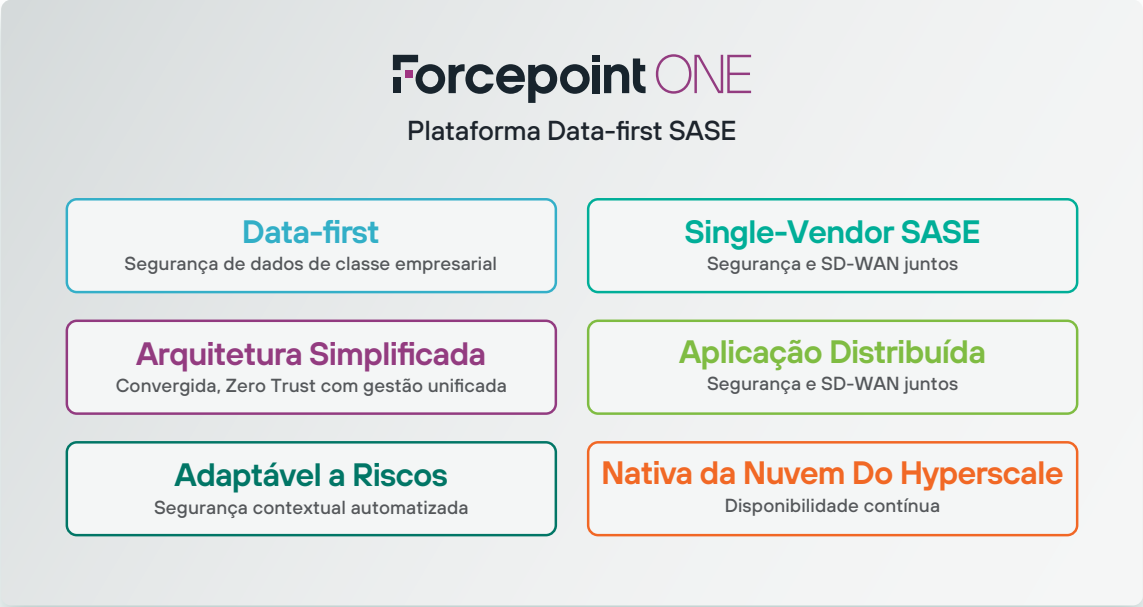
O Forcepoint ONE está sendo usado em todo o mundo para:

- → **Evitar a perda de dados de aplicativos de nuvem** (especialmente Microsoft 365 e Google Workspace) e na web.
- → **Proteger o acesso sem agentes "Traga seu próprio dispositivo "(BYOD, Bring Your Own Device)** à nuvem e a aplicativos privados**.**
- → **Implementar acesso Zero Trust** à nuvem, à web e aos aplicativos privados confere proteção para usuários remotos e de escritório.
- → **Controlar shadow IT, incluindo ChatGPT** e outras IAs generativas, permitindo o uso sem o risco de exfiltração de dados confidenciais.
- → **Simplificar fusões e aquisições.**
- → **Substituir VPNs** para acessar aplicativos internos.
- → **Acelerar o desempenho de aplicativos de nuvem** em filiais.
- → **Permitir que qualquer site ou documento baixado** seja usado com segurança, mesmo se contaminado.
- → **Detectar erros de configuração** e violações de estruturas de conformidade.



Seis maneiras pelas quais o Forcepoint ONE SASE é diferente

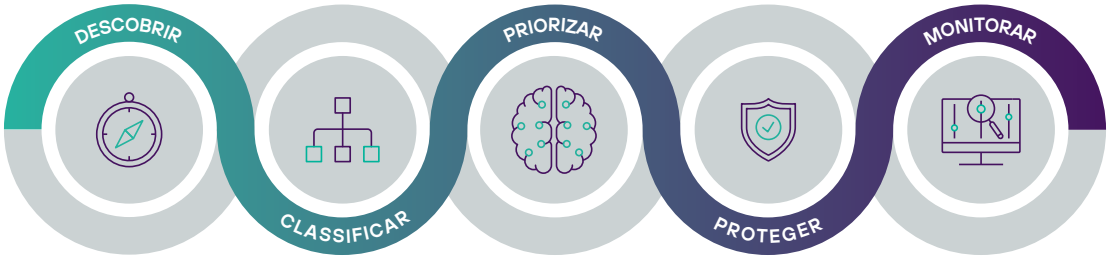
O Forcepoint ONE reúne seis elementos primordiais para oferecer a segurança e as redes de que as organizações precisam para ter sucesso no mundo atual em rápida transformação:



Data-first: segurança de dados de classe empresarial em todos os lugares

A Forcepoint tem um ponto de vista diferente da maioria dos fornecedores. Acreditamos que a segurança digital moderna significa basicamente permitir que dados confidenciais de todos os lugares sejam usados com segurança em qualquer lugar. É por isso que integramos algumas das tecnologias de segurança de dados mais robustas do setor ao núcleo de nossa plataforma Forcepoint ONE e aos nossos gateways SSE — CASB (proxy de encaminhamento, proxy reverso e baseado em API), SWG (baseado na nuvem e em endpoint) e ZTNA (baseado em agente e sem agente).

A tecnologia Data Loss Prevention (DLP) da Forcepoint é utilizada por milhares de organizações em todo o mundo e tem sido chamada de "líder" pelos principais analistas do setor. Faz parte de uma estrutura baseada em Zero Trust, chamada Ciclo de Vida de Segurança de Dados, que implementa as melhores práticas para proteger os dados de forma eficiente e eficaz contra acesso não autorizado, roubo ou perda acidental.



Ciclo De Vida De Segurança De Dados

Automatizamos cada etapa deste ciclo de vida. Com nossas soluções, os clientes podem identificar rapidamente onde residem os dados confidenciais, classificar dados estruturados e não estruturados (na nuvem e no local), determinar onde concentrar seus esforços, impedir a perda de dados em todos os principais canais de exfiltração (aplicativos de endpoint, e-mail, web, rede e nuvem) e monitorar continuamente o que os usuários estão fazendo com os dados confidenciais.

Essa abordagem vai muito além da correspondência de padrões básica que muitas vezes se passa por segurança de dados em outras soluções SASE. Ao classificar os dados e organizá-los em diferentes grupos, é possível escrever e aplicar políticas de segurança de dados que lidam automaticamente com novas instâncias e tipos de dados confidenciais. Para simplificar a definição de políticas, especialmente para atender a requisitos específicos de região ou setor, incorporamos uma das bibliotecas de modelos de políticas mais abrangentes do setor. Além disso, nossos gateways SSE Forcepoint ONE para controlar o acesso à web (SWG), à nuvem (CASB) e a aplicativos privados (ZTNA) permitem que as políticas de DLP sejam especificadas em um só lugar e aplicadas de forma consistente em diferentes canais.

Essa simplicidade não se limita a um conjunto de aplicativos predefinidos. O Forcepoint ONE pode aplicar controles de segurança de dados granulares a qualquer aplicativo baseado na web usando o mesmo mecanismo de script de lógica de SASE programável de campo (FPSL) que a Forcepoint usa em suas próprias políticas. Os administradores podem criar facilmente regras que acionam atributos em uma solicitação de HTTP (domínio, método, URI, string de consulta ou cookie) para detectar interações do usuário, registrar as páginas que estão sendo usadas e bloqueá-las opcionalmente. Por exemplo, o Forcepoint ONE pode facilmente:

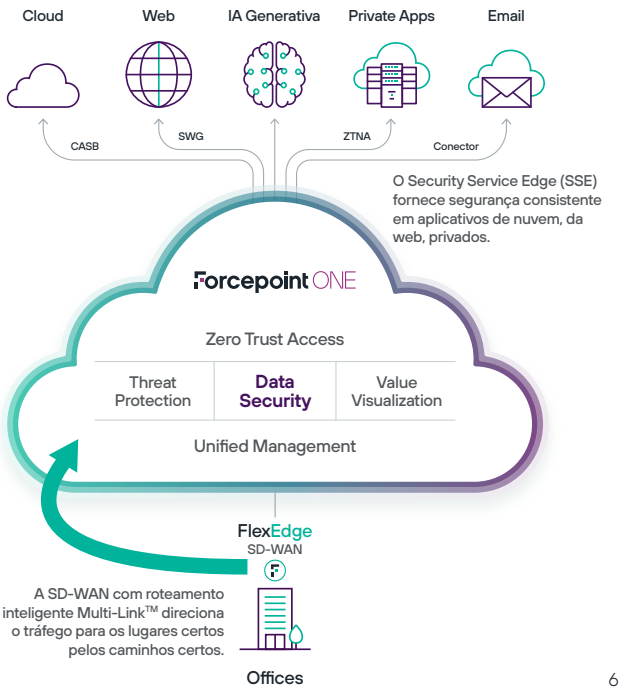
- → Bloquear logins em aplicativos SaaS corporativos usando um endereço de e-mail pessoal.
- → Registrar todos os arquivos carregados em contas pessoais do Google Drive para usuários que fazem parte de um grupo de usuários de risco.
- → Bloquear "likes" no Facebook.
- → Permitir que apenas os membros do grupo de marketing publiquem no LinkedIn.
- → Bloquear conteúdo confidencial em uma publicação do Twitter.

E, como os integrantes da força de trabalho atual geralmente dependem de telefones, tablets e endpoints, como estações de trabalho Linux ou Chromebooks, **o Forcepoint ONE possibilita usar com segurança aplicativos da web privados na nuvem e internos a partir de BYOD e outros dispositivos sem agente para manter as pessoas produtivas sem colocar os dados em risco.**

Sinlge-vendor: segurança e SD-WAN em um só produto

A Forcepoint é pioneira na integração de tecnologias de segurança e rede em um só produto, gerenciado a partir de um único console. As soluções Forcepoint Secure SDWAN foram umas das primeiras a combinar o roteamento SDWAN com firewall de alta segurança e tecnologias de prevenção de invasões.

Nossa agregação multi-ISP patenteada de multi-link é usada em todo o mundo para transformar redes legadas de área ampla construídas em circuitos privados, como MPLS, em SD-WAN moderna, baseada em banda larga. Projetada especificamente para escalabilidade massiva, a Forcepoint Secure SD-WAN permite que políticas para nada menos que 6.000 locais sejam gerenciadas a partir de uma única console.



Com a Secure SD-WAN, as organizações distribuídas conectam seus locais remotos e filiais diretamente à internet para fornecer o mais alto desempenho no acesso a aplicativos de nuvem modernos. **Recursos avançados, como direção de aplicativos, monitoramento da integridade de aplicativos e atualização zero-touch, permitem que as organizações de TI ofereçam desempenho e tempo de atividade consistentes de forma proativa, para manter as pessoas produtivas e os gastos de infraestrutura baixos.**

Como resultado, nossa SD-WAN fornece uma base para implementar uma arquitetura SASE convergida. As organizações podem rotear automaticamente o tráfego de vários aplicativos para nossos gateways Forcepoint ONE Security Service Edge (SSE) que funcionam na nuvem. Isso não apenas facilita a proteção de funcionários e dados empresariais, mas também permite que as políticas de segurança sejam definidas e aplicadas para dispositivos não gerenciados, como notebooks convidados em Wi-Fi, telefones e tablets BYOD, até mesmo impressoras e dispositivos de Internet das coisas (IoT).

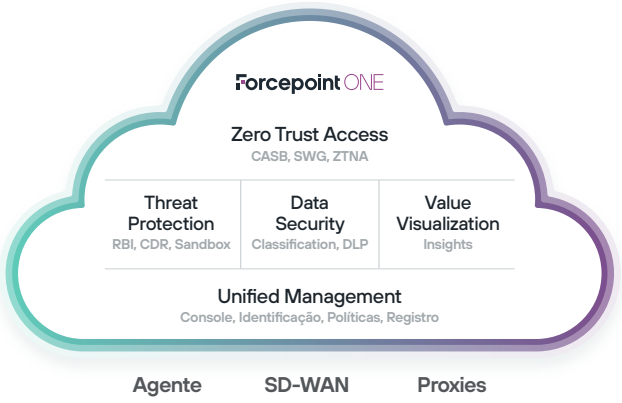
Arquitetura simplificada: gestão convergida e unificada

A missão da Forcepoint é "Segurança Simplificada". Os dias de pessoas que se orgulham da complexidade da infraestrutura de segurança acabaram. Com os ambientes em constante mudança, as equipes de TI são frequentemente pressionadas até o limite e forçadas a fazer mais com menos. **Reduzir a complexidade não é mais apenas uma boa ideia — é a única maneira de manter as empresas produtivas, cortar custos e evitar que o risco saia do controle.**

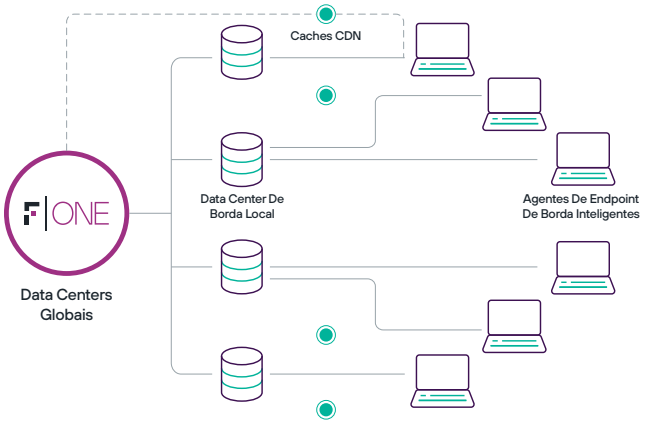
Para ajudar os clientes a simplificar sua própria arquitetura corporativa, o próprio Forcepoint ONE foi projetado para evitar falhas e redundâncias em tecnologias que costumavam ser fragmentadas. Gateways para proteger o acesso a aplicativos de nuvem, à web e aos aplicativos privados internos compartilham código e usam um conjunto comum de microsserviços de segurança subjacentes para manter as ameaças afastadas, os dados confidenciais protegidos e ajudar os líderes de negócios a entender melhor o valor da conectividade e da segurança que estão proporcionando à organização.

Os principais elementos da plataforma Forcepoint ONE incluem:

- → Gateways de acesso baseados em Zero Trust, que controlam como os funcionários e outras pessoas usam a nuvem (CASB), a web (SWG) e os aplicativos privados (ZTNA).
- → Serviços avançados de proteção contra ameaças, como isolamento remoto de navegador, sanitização automática de documentos (conhecida como desarme e reconstrução de conteúdo), sandbox de antivírus e malware.
- → Serviços de segurança de dados de última geração que evitam o roubo de dados confidenciais de forma consistente em cada canal (DLP).
- → Acesso seguro sem agente a partir de BYOD e dispositivos não gerenciados para aplicativos de nuvem (CASB) e web privada (ZTNA).



- → Painéis interativos que apresentam visualmente os principais indicadores de desempenho e o valor econômico dos serviços que o Forcepoint ONE está fornecendo.
- → Uma única console para definir políticas para controlar como os recursos de negócios são acessados e usados.
- → Integração de provedor de identidade SAML patenteado para trabalhar com os sistemas IdP existentes ou complementá-los.



O Forcepoint ONE usa uma arquitetura de várias camadas. Os data centers centrais globais desempenham as principais funções da plataforma, como inspecionar os dados em repouso em SaaS e IaaS, verificar SaaS e IaaS para detectar erros de configuração de segurança e analisar os dados de dispositivos endpoint.

Os data centers de borda locais fornecem políticas e agem como caches de Rede de Entrega de Conteúdo (CDN) para informações solicitadas com frequência, como categorização de inteligência de ameaças. Esses data centers de borda são dimensionados automaticamente para lidar com cargas temporárias, como quando as pessoas convergem em uma conferência.

Os recursos adicionais que complementam os serviços de acesso fornecidos a partir da nuvem são fornecidos por um software de endpoint, chamado SmartEdge, que funciona em notebooks gerenciados e outros dispositivos. O SmartEdge conecta automaticamente os trabalhadores remotos aos serviços de segurança certos e garante que as políticas corretas sejam aplicadas. Atualmente a Forcepoint está integrando essa tecnologia com a telemetria de nossos outros controles de endpoint e rede para permitir que as organizações de TI implantem e gerenciem um único aplicativo de endpoint que fornece a gama completa de conectividade e segurança do Forcepoint ONE.

Com base nos princípios Zero Trust

As políticas para os serviços de acesso do Forcepoint ONE são criadas em torno de uma abordagem Zero Trust que especifica a identificação, o aplicativo, os dispositivos e o local para o qual cada ação específica deve ser aplicada:

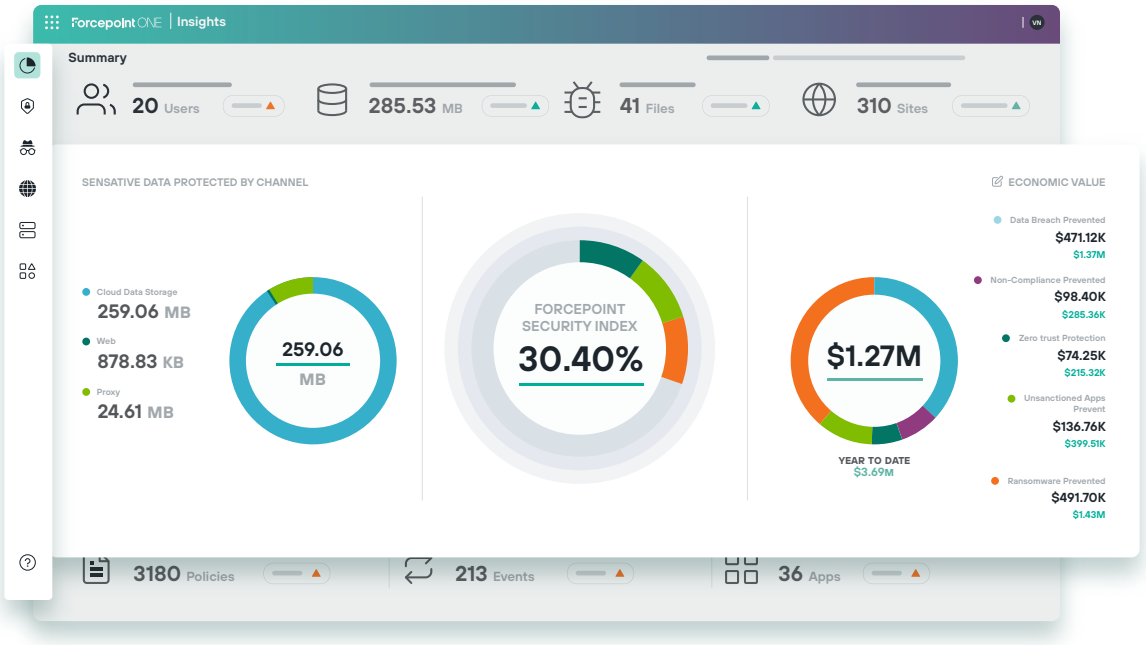
Proxy

ID	Groups	Access Method	Device	Location	Action
7073	Admins	Any	Any	Anonymizers IaaS Provider IPs	Deny
69739	Any	SSO Auth	Managed Win - AV On	Corp Network and VPN	Direct App Access
28475	Any	SSO Auth	Any	Any	Secure App Access DLP Download DLP Upload
188394	Any	Any	Any	NRD-HQ	Secure App Access DLP Download DLP Upload

As políticas de segurança de dados e prevenção de ameaças podem ser especificadas para todos os uploads e downloads e, em seguida, ser combinadas com a notificação e o treinamento do usuário para garantir que os usuários e os dados sejam protegidos.

Ligando os pontos sobre o valor econômico do SASE

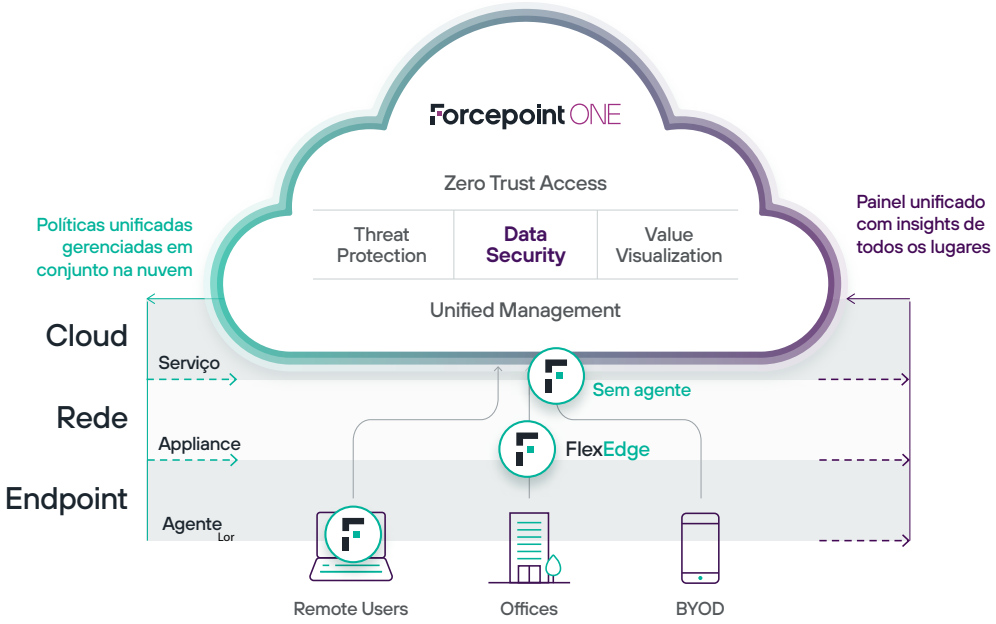
O Forcepoint ONE oferece aos administradores visibilidade completa e relatórios unificados em todos os seus dispositivos gerenciados e não gerenciados. Nossos painéis do Insights oferecem uma visão consolidada do que está acontecendo em diferentes serviços de segurança que esclarece o valor comercial que a Forcepoint está fornecendo.



Aplicação distribuída em vários níveis na nuvem, na borda da rede e no endpoint

A nuvem revolucionou o modo como a segurança é gerenciada e fornecida, enquanto a internet substituiu a rede corporativa como a espinha dorsal das operações de TI. Juntas, elas permitem que um plano de controle consolidado seja acessado com facilidade de qualquer lugar. Mas a nuvem é o começo, não o fim, de uma abordagem moderna para a segurança.

Embora todas as soluções SASE ofereçam a aplicação de políticas com base na nuvem, nós vamos mais além. **O Forcepoint ONE coloca a aplicação de políticas de rede e segurança onde quer que sejam necessárias: perto do usuário no endpoint, perto da infraestrutura na rede, bem como perto de aplicativos na nuvem.**



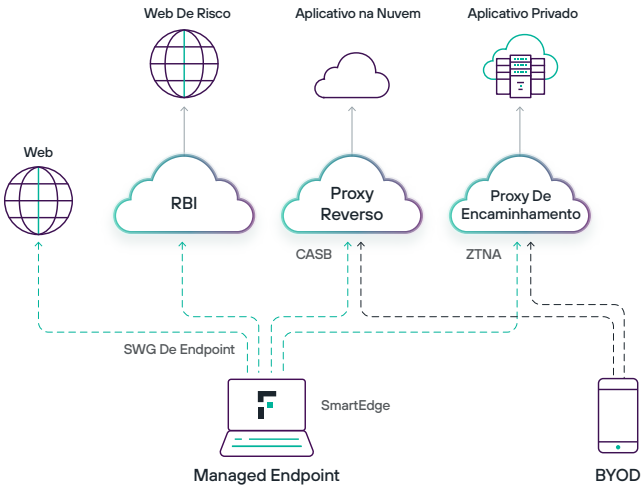
Essa abordagem distribuída otimiza o desempenho dos aplicativos, reduz o uso de largura de banda de rede e elimina os problemas que podem surgir quando o tráfego é redirecionado por meio de chokepoints – seja em data centers privados antigos ou em serviços de nuvem novos e com vários inquilinos. O Forcepoint ONE garante que as mesmas políticas sejam aplicadas em todos os lugares, e os mesmos painéis podem ser usados para monitorar a operação dessas políticas.

O "onramp" de nuvem baseado em endpoint otimiza o desempenho de aplicativos e a experiência do usuário
Por exemplo, as arquiteturas SWG tradicionais que forçam todo o tráfego da web por meio de um proxy de nuvem, embora simples de implementar, geralmente apresentam desafios no mundo real:

- **Latência –** os hops de rede e o processamento extras que são introduzidos reduzem a velocidade de navegação em até a metade. Alguns aplicativos de nuvem (incluindo alguns dos pacotes de colaboração de escritório mais populares) são sensíveis a esses atrasos e podem não funcionar corretamente.
- **Utilização de largura de banda –** as organizações que equipam os sites com vários links de internet podem não ser capazes de tirar o máximo proveito deles para otimizar o desempenho e o preço de aplicativos de nuvem (por exemplo, o envio de videoconferência de alta prioridade em links mais rápidos, enquanto o tráfego de menor prioridade passa sobre os menos caros).
- **Reconhecimento de local –** os aplicativos de nuvem que usam o endereço de internet do endpoint para selecionar conteúdo ou funções específicas (como em qual idioma apresentar uma página) podem não funcionar corretamente, causando confusão do usuário e encargos de suporte técnico.
- **Conformidade –** em algumas situações, o envio de dados confidenciais de um dispositivo de endpoint controlado para a internet (mesmo que estejam indo direto para o proxy) pode acionar procedimentos de violação.

A Microsoft recomenda especificamente que os usuários do Microsoft 365 evitem o uso de proxies, forçando as organizações a escolher entre produtividade e segurança. O Forcepoint ONE aborda esses problemas permitindo que as políticas de segurança web (incluindo aquelas para prevenção de perda de dados) sejam aplicadas em endpoints que executam nosso software SmartEdge.

O SmartEdge fornece um "onramp de nuvem" que encaminha automaticamente o tráfego para o serviço ou aplicativo apropriado com base no que está sendo acessado. Ele complementa os proxies de nuvem que o Forcepoint ONE oferece para proteger dispositivos sem agente, como BYOD e IoT.

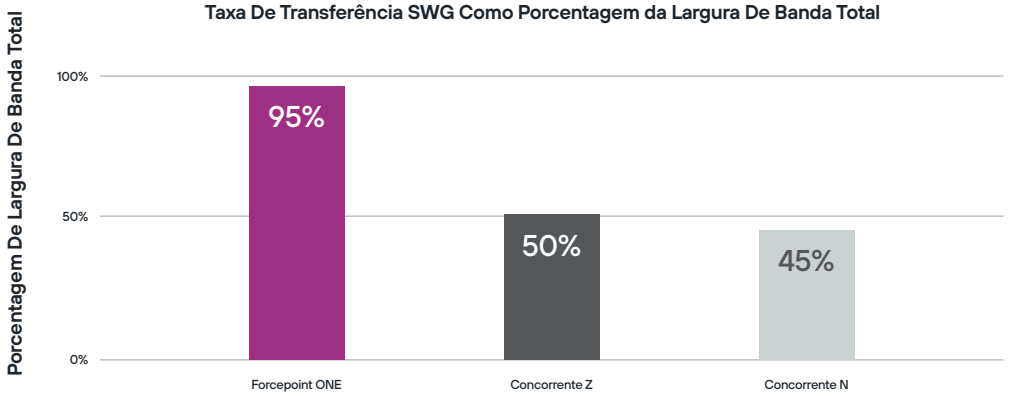


O software de endpoint SmartEdge direciona o tráfego para os lugares certos

O SmartEdge é especialmente valioso para os usuários remotos, pois fornece a experiência de usuário mais natural, produtiva e segura. Ele funciona com nossa plataforma de nuvem para garantir que as políticas sejam aplicadas corretamente em todas as situações, incluindo:

- → **Novo acesso a URL –** quando um usuário tenta acessar um URL pela primeira vez, o SmartEdge SWG consulta o cache CDN do Forcepoint ONE mais próximo para obter a política de navegação na web apropriada para aquela combinação de grupo de usuários, tipo de dispositivo, categoria de URL, local e reputação do URL. Se o resultado da consulta não estiver no nó de cache, a solicitação será encaminhada para o data center de borda local do Forcepoint ONE mais próximo. Supondo-se que o site não esteja bloqueado, todo o tráfego da web é trocado diretamente entre o dispositivo e o site, evitando assim o hairpinning.
- → **Proteção e isolamento de sites SWG de risco –** os sites de risco podem ser especificados no Forcepoint ONE com base em sua Categorização de Site de URL ou nas Pontuações de Reputação de URL. Quando um usuário tenta acessar um site de risco, o SWG isola o acesso e o redireciona por meio do Forcepoint Remote Browser Isolation (RBI). O RBI reduz a superfície de ataque do endpoint escondendo o endereço IP e renderizando remotamente o site em um contêiner temporário, que é específico para a sessão do usuário.
- → **Movimento de arquivos para/de um aplicativo da web seguro e não sancionado –** quando um usuário tenta fazer o upload de um arquivo ou baixar um arquivo de um aplicativo da web não sancionado com uma política de navegação na web que aplica acesso seguro, o Forcepoint ONE bloqueará as tentativas de fazer upload ou download de arquivos com base em regras de política para proteção de DLP ou de malware na política de navegação na web.

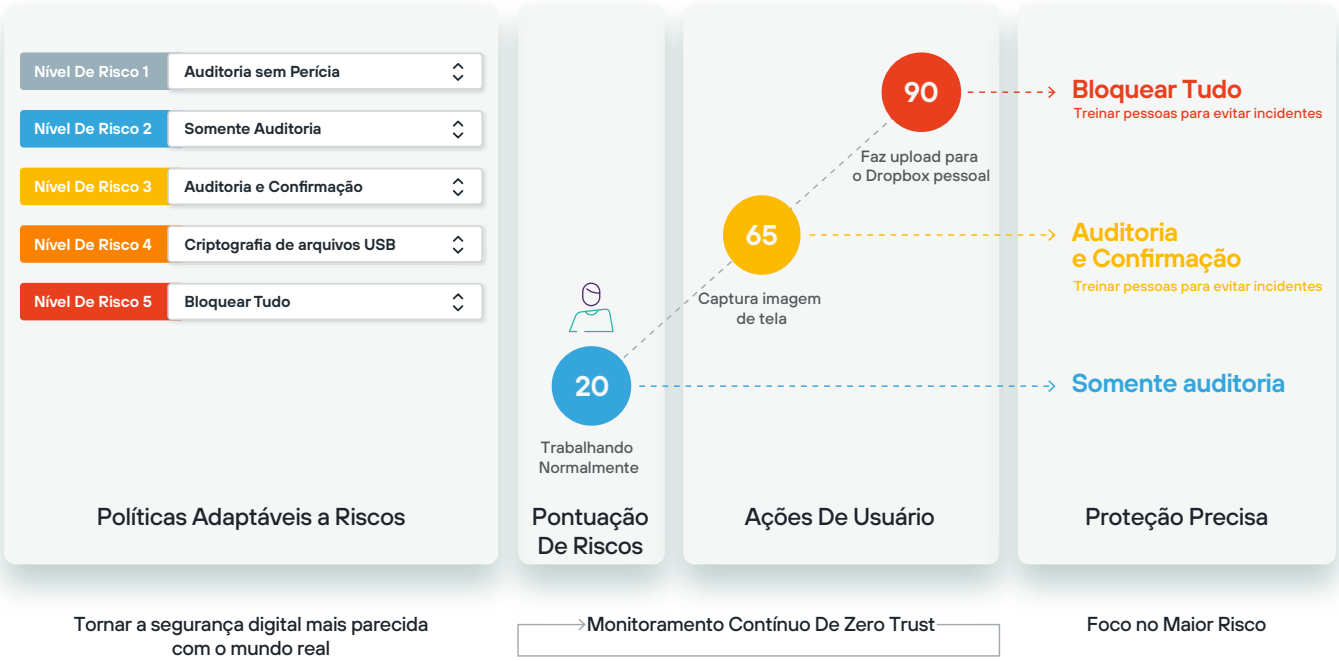
A abordagem de aplicação distribuída no Forcepoint ONE oferece até o dobro do desempenho de navegação de sistemas somente de nuvem com proteção completa contra ameaças transmitidas pela web ou upload inadequado de dados confidenciais



Risk-adaptive protection para segurança contextual

Agora que as pessoas estão trabalhando em qualquer lugar com dados que residem em toda parte, a definição de políticas individuais para cada combinação relevante de usuários, dispositivos, locais, aplicativos e outros atributos é propensa a erros e não escalável. Pior ainda, uma abordagem tão estática não combina com o modo como as organizações operam no mundo real: elas dão às pessoas que demonstram bom senso a capacidade de usar dados confidenciais e recursos com o mínimo de interferência, mas aplicam controles mais rigorosos se forem feitos erros ou escolhas ruins.

A Forcepoint é pioneira nessa proteção "adaptável a riscos", que escolhe dinamicamente quais políticas aplicar com base nas próprias ações dos usuários, se seus dispositivos estão atualizados com as diretrizes corporativas, a sensibilidade dos dados que estão tentando usar, e outros fatores.



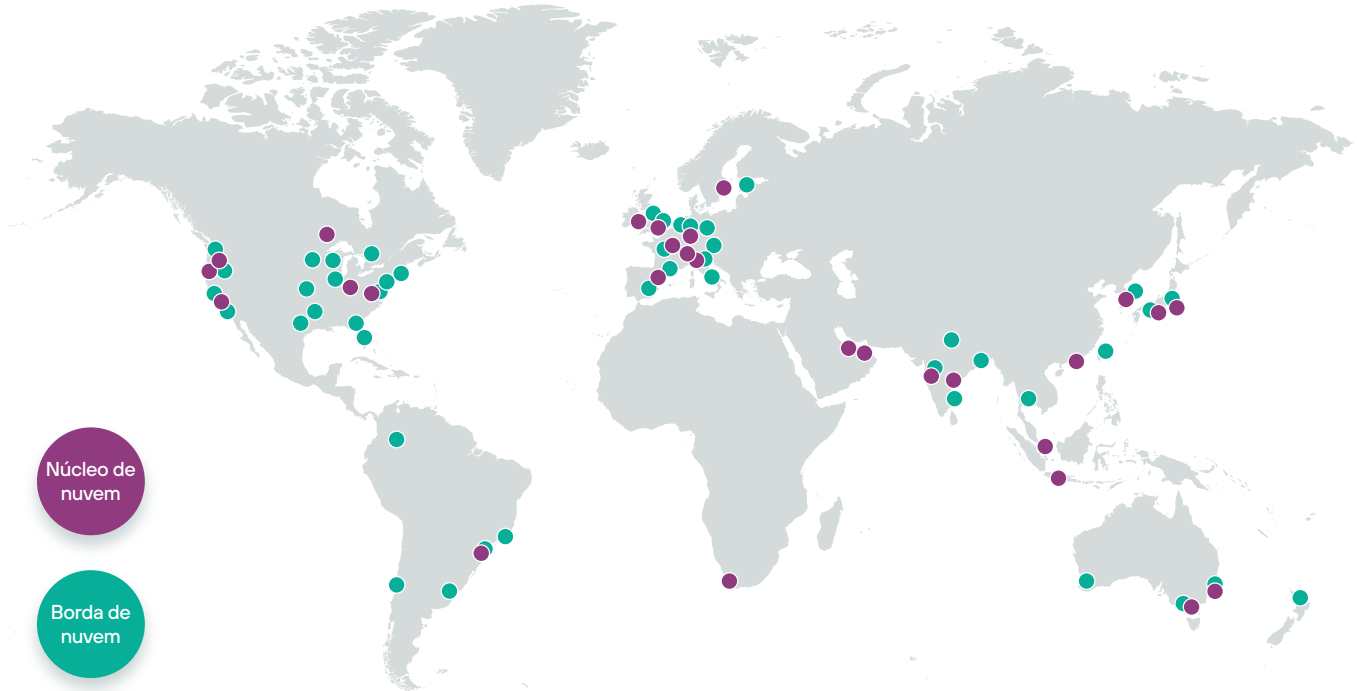
Essa abordagem automatiza e personaliza a segurança, dando às pessoas a liberdade de usar dados confidenciais de maneiras inovadoras, enquanto concentra a aplicação nas situações em que ela é mais necessária. A Forcepoint incorpora essa tecnologia em nossas soluções de DLP enterprise, que podem ser usadas para proteger os dados em uma ampla gama de canais, como em dispositivos de endpoint, em redes e em e-mail, bem como em aplicativos de nuvem e da web que são protegidos com os serviços SSE no Forcepoint ONE. **O resultado é melhor produtividade do usuário, gastos operacionais mais baixos (definição de política mais fácil, menos chamadas urgentes de suporte técnico relativas ao bloqueio de usuários) e menos risco.**

Disponibilidade contínua nativa da nuvem do hyperscaler

Os serviços de nuvem são tipicamente implantados de uma entre várias maneiras:

- → **Data centers proprietários –** nos primórdios da web, os fornecedores que queriam oferecer Software-as-a-Service precisavam construir e manter seus próprios data centers. Embora isso forneça o maior nível de controle, e inicialmente fosse, muitas vezes, a única opção, agora o preço que ele exige o torna muito incomum.
- → **Instalações de compartilhamento de localização –** hoje, quando os fornecedores falam sobre "seus" data centers, eles geralmente estão se referindo a instalações de compartilhamento de localização, de propriedade e operadas por terceiros. Isso requer menos esforço do que a construção de um data center proprietário, mas ainda exige uma quantidade significativa de complexidade e custos de operação.
- → **Nuvens públicas de hyperscalers –** cada vez mais, quando as organizações decidem colocar aplicativos na nuvem, a maneira mais rápida é utilizar ambientes de nuvem pública, como Amazon (AWS), Microsoft (Azure), Google (GCP), Oracle (OCI) e outros. Conhecidos como "hyperscalers" devido ao seu foco no fornecimento de ambientes altamente escaláveis, esses sistemas também oferecem uma gama de serviços que os fornecedores de aplicativos podem usar para simplificar seu próprio desenvolvimento. Além disso, os hyperscalers geralmente já estão disponíveis na maioria das localizações geográficas que os fornecedores desejam atender e são construídos com alguns dos mais altos níveis de segurança física.

O Forcepoint ONE foi projetado desde o início para funcionar em hyperscalers. Construído na AWS, ele oferece uma presença regional em todos os continentes, exceto na Antártida:



Sua escalabilidade elástica permite que os serviços sejam dimensionados para cima ou para baixo dinamicamente. Por exemplo, se um grande número de usuários se reunir em um único local, o Forcepoint ONE pode ativar capacidade adicional sem exigir a implantação de hardware físico. Além disso, com tantos aplicativos agora hospedados em hyperscalers (50% dos 10 mil principais sites, 40% dos 100 mil principais sites, 23% do 1 milhão de sites principais estão na AWS), ter o Forcepoint ONE baseado lá também mantém a segurança perto de aplicativos e seus dados.

A plataforma Forcepoint ONE foi projetada para fornecer disponibilidade contínua, sem necessidade de tempo de inatividade de manutenção planejada. **Ele usa uma estratégia de implantação "azul/verde" que permite que atualizações e novos recursos sejam enviados ao vivo, sem tirar o serviço do ar.**

O resultado: melhor produtividade e menos chamadas desesperadas para o suporte técnico.

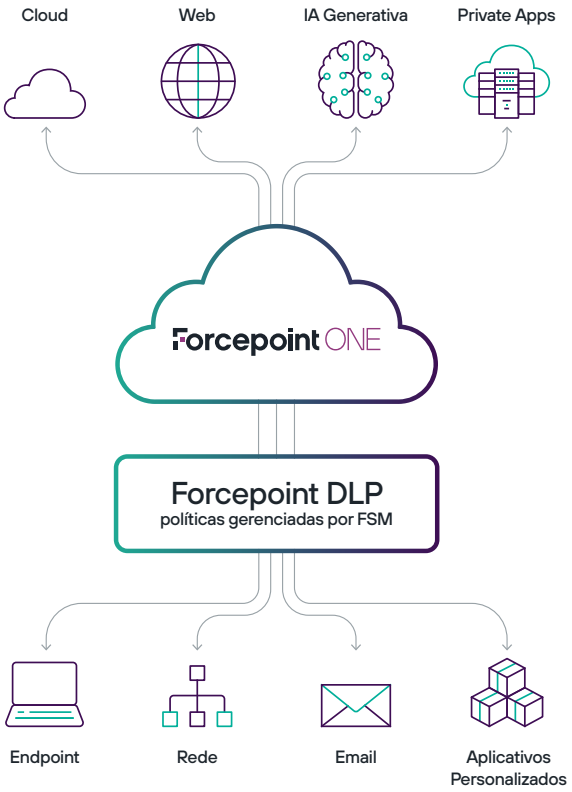
Fornecendo segurança de dados em todos os lugares — mesmo para IAs generativas

As soluções da Forcepoint trabalham juntas para permitir que as mesmas políticas de segurança de dados sejam aplicadas com perfeição, desde o endpoint até a nuvem – e em qualquer lugar entre eles. Isso permite que as organizações gerenciem a segurança de dados a partir de um único console, com visibilidade e controle consistentes. Ele vai além da correspondência de padrões básica da maioria dos gateways SSE, fornecendo segurança de classe empresarial completa, com a proteção adaptável a riscos pioneira da Forcepoint e o monitoramento contínuo baseado em Zero Trust.

Com o rápido surgimento de inovações, como o ChatGPT e outras, a segurança de dados robusta é mais importante agora do que nunca. As IAs generativas são a forma mais recente de "shadow IT": elas oferecem enormes ganhos de produtividade, mas têm potencial para colocar os dados confidenciais em grande risco.

A Forcepoint permite que você aproveite as IAs generativas, mantendo o controle de quem pode usá-las e como:

- → Limitar o acesso a grupos ou indivíduos específicos que estão autorizados a testar ou usar IAs.
- → Controlar os uploads de arquivos, bem como cortar e colar.
- → Inspecionar e proteger os dados confidenciais contra vazamentos.



Forcepoint ONE: Data-first SASE para o mundo moderno

O SASE deixou rapidamente de ser uma arquitetura acadêmica para se transformar na forma mais comum que as organizações planejam conectar e proteger suas forças de trabalho modernas. O Forcepoint ONE reúne mais de uma década de experiência em cada um dos serviços de segurança focados em dados, redes diretas para a internet e de nuvem, para oferecer uma plataforma abrangente para fornecer aos usuários, com segurança, acesso rápido e eficiente aos recursos de negócios em todas as etapas da jornada de uma organização para a nuvem.

Forcepoint

forcepoint.com/pt-br/contact

Sobre a Forcepoint

A Forcepoint simplifica a segurança para empresas e governos globais. A plataforma all-in-one verdadeiramente nativa de nuvem da Forcepoint facilita a adoção de Zero Trust e a prevenção de roubo ou perda de dados confidenciais e propriedade intelectual, não importa onde as pessoas estejam trabalhando. Com sede em Austin, Texas, a Forcepoint cria ambientes seguros e confiáveis para clientes e seus funcionários em mais de 150 países. Entre em contato com a Forcepoint em www.forcepoint.com/pt-br, Twitter e LinkedIn.

[FP-Whitepaper-Forcepoint ONE: uma plataforma Data-First SASE exclusiva-PT] 17agosto2023