Forcepoint

Datasheet

Forcepoint ONE

Principais benefícios:

- Tempo de atividade verificado de 99,99% desde 2015
- A latência minimizada e a taxa de transferência maximizada com o dimensionamento automático
- Integração flexível com qualquer IdP compatível com SAML
- Console unificada de administração
- Agente de sincronização de AD ou provisionamento de SCIM acelera a integração de usuários
- O proxy reverso com o AJAX-VM permite a proteção de qualquer aplicativo da web gerenciado sem um agente no dispositivo
- A verificação de dados em movimento bloqueia o malware e a exfiltração de dados entre usuários e qualquer aplicativo da web
- A verificação de dados em repouso coloca em quarentena o malware e controla o compartilhamento de dados de risco para muitas ofertas de armazenamento de SaaS e IaaS populares
- A criptografia de dados estruturados e não estruturados em SaaS e IaaS garante a privacidade de dados
- Capacidade de bloquear métodos de requisições HTTP/S específicos, resultando em controle granular das interações do usuário com qualquer aplicativo SaaS ou privado da web

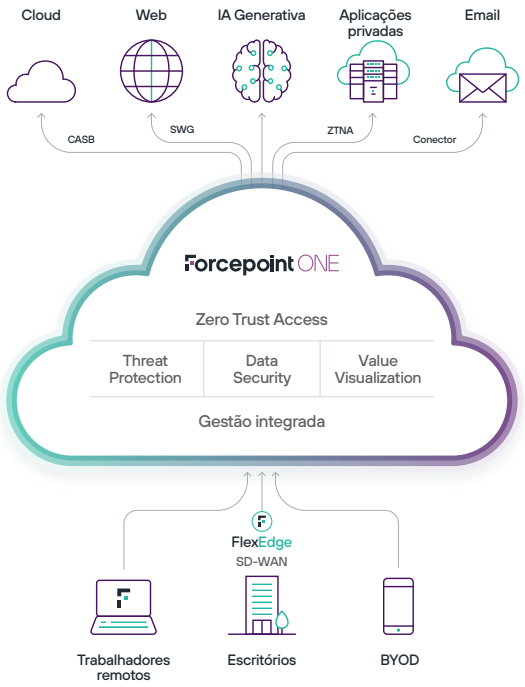
O Forcepoint ONE é um serviço de nuvem que protege os dados em todos os lugares para empresas distribuídas e agências governamentais que precisam se adaptar rapidamente às forças de trabalho remotas e híbridas em mudança. Ele oferece aos funcionários, prestadores de serviço e outros usuários, acesso controlado a informações de negócios na web, na nuvem (SaaS e IaaS) e em aplicativos privados, enquanto mantém os invasores do lado de fora e os dados confidenciais do lado de dentro. Como resultado, o Forcepoint ONE torna os usuários mais produtivos, sejam eles remotos ou no escritório, e as empresas mais eficientes.

O Forcepoint ONE combina as tecnologias de segurança Zero Trust e SASE, incluindo três gateways seguros de acesso e uma variedade de serviços compartilhados de proteção contra ameaças e segurança de dados, todos criados em uma plataforma nativa da nuvem. Essa abordagem permite que as organizações gerenciem políticas unificadas em todos os canais para manter as ameaças fora e os dados confidenciais dentro.

→ **Web Security.** Monitora e controla qualquer interação com qualquer site, incluindo o bloqueio do acesso a sites com base na categoria e pontuação de risco, bloqueio de download de malware, bloqueio de upload de dados confidenciais e detecção e controle de TI invisível.

→ **Cloud Access Security Broker (CASB).** Solução baseada em agente ou sem agente que aplica controles de acesso granulares sobre os aplicativos de SaaS da empresa com base na identidade, local, dispositivo e grupo que aplica controles de acesso granulares para aplicativos privados em tempo real. Verifica os dados em repouso em SaaS e IaaS populares para detectar malware e dados confidenciais e corrige conforme necessário. A opção sem agente facilita o acesso de BYOD e de contratados.

→ **Zero Trust Network Access (ZTNA).** Solução baseada em agente ou sem agente que permite acesso granular a aplicativos privados sem o uso de uma VPN. Solução baseada em agentes necessária para aplicativos não HTTP/S.



Os recursos comuns para todos os três gateways incluem:

- **Controle contextual de acesso.** O acesso a aplicativos da Web, da nuvem ou privados é controlado com base no tipo de dispositivo, postura do dispositivo, comportamento do usuário e grupo de usuários.
- **Data Loss Prevention (DLP).** Os arquivos e o texto são checados por dados confidenciais após o upload e o download e bloqueados, rastreados, criptografados ou editados, quando apropriado. Mais de 190 regras de DLP predefinidas ajudam a simplificar a conformidade regulatória e fornecer um rápido "time to value". Integração fácil com o Forcepoint DLP Enterprise permite a segurança de dados em todos os lugares: no endpoint, na rede, na Web e em serviços de nuvem.
- **Verificação de malware.** Os arquivos são verificados após o upload e o download quanto a malware e bloqueados quando detectado.
- **Console de gerenciamento integrada.** Para configuração, monitoramento e relatórios.
- **Insights.** Painéis de análises de segurança com widgets e visualizações personalizáveis que mostram o impacto da sua postura de segurança ao longo do tempo, incluindo avaliações do valor econômico.
- **Agente no dispositivo.** Para Windows e macOS.
- **Tempo de atividade do serviço de 99,99%.**

O Forcepoint ONE também inclui esses recursos complementares:

- **Cloud Security Posture Management (CSPM).** Verifica as configurações de inquilinos da AWS, do Azure e do GCP para configurações de risco e fornece correção manual e automatizada.
- **SaaS Security Posture Management (SSPM).** Verifica as configurações de inquilinos do Salesforce, do ServiceNow e do Office 365 para configurações de risco e fornece correção manual e automatizada
- **Remote Browser Isolation (RBI) com Content Disarm Reconstruction (CDR) integrada.** Os usuários são protegidos contra malware transmitido pela Web em seu dispositivo local, rodando o navegador em uma VM hospedada na nuvem. Com o CDR, os downloads de documento e imagens podem ter malwares incorporados removidos e serem reconstruídos antes de serem abertos por um usuário. Isso inclui a remoção de malware incorporado em um arquivo de imagem, usando esteganografia.
- **Forcepoint Classification.** Marcação de classificação de dados com sugestões com tecnologia de IA para aprimorar a precisão de marcação.
- **Advanced Malware Detection and Prevention (AMDP).** Analisa o comportamento de arquivos em uma sandbox de malware controlada para identificar conteúdo escondido e malicioso.

Recursos e benefícios do Forcepoint ONE

ESCOPO	RECURSO	BENEFÍCIO
Em toda a plataforma	Arquitetura distribuída e de dimensionamento automático na AWS com mais de 300 POPs em todo o mundo.	→ Tempo de atividade de 99,99%. → Latência mínima: muitas vezes ainda mais rápido do que o acesso direto a aplicativos. → Verificação mais rápida de dados em repouso: horas versus dias para verificar todo o conteúdo de um inquilino de aplicativo.
	Integração com qualquer IdP compatível com SAML. Retransmissão de SAML ou modo de proxy de ACS. IdP integrado opcional usando o Microsoft ADFS.	→ Implantação flexível. → Proteção contra negação de serviço ao usar o modo de retransmissão de SAML.
	Agente de sincronização do Active Directory. Sincroniza seus usuários e grupos de AD atuais com usuários e grupos do Forcepoint ONE.	→ Leverage your existing Microsoft AD instance to quickly onboard users and manage the groups they are in.
	Integração com SCIM. Sincroniza seus usuários e grupos do Azure AD atuais com usuários e grupos do Forcepoint ONE.	→ Aproveite sua instância do Microsoft AD existente para integrar rapidamente os usuários e gerenciar os grupos em que eles estão.
	Controle de acesso contextual. Concede acesso de usuários ao Forcepoint ONE com base no grupo de usuários, no tipo de dispositivo, no local ou na hora do dia. Escalonamento opcional para Autenticação multifator com base em "viagem impossível", local não autorizado ou dispositivo desconhecido. Camada adicional de controle de acesso para sites ou aplicativos individuais com base no grupo de usuários, tipo de dispositivo ou local.	→ Detecção e bloqueio de tentativas de login suspeitas reduzem os riscos associados a senhas roubadas. → O controle de acesso granular permite a segmentação de usuários com base no risco e na necessidade de acessar.
	Suporte baseado em agente para SWG, proxy de encaminhamento CASB e ZTNA para aplicativos não-web.	→ Implantação de agentes simplificada, incluindo implantação por meio de sistemas de MDM selecionados. → Baixa CPU e memória. → Os certificados autogerados e autorrotacionados automaticamente garantem a segurança e reduzem a sobrecarga de TI.
	Console de administrador integrada para gerenciar todas as capacidades do sistema em todos os aplicativos, usuários e dispositivos.	→ A console integrado reduz a complexidade e o "time to value" enquanto aumenta a visibilidade e o controle.
	Insights fornece painéis de análise de segurança com widgets e visualizações personalizáveis que mostram o impacto da sua postura de segurança ao longo do tempo, incluindo avaliações do valor econômico.	→ Meça o risco e o fortalecimento da postura de segurança ao longo do tempo. → Calcule o impacto econômico da sua plataforma de segurança na nuvem.
CASB, SWG e ZTNA para aplicativos baseados na web	DLP e exame de malwares para dados em trânsito. Verifica os anexos de arquivos baixados ou carregados para qualquer aplicativo ou site baseado na web em busca de malware ou dados confidenciais. Registra e realiza a ação de correção apropriada, como bloquear (opção única para SWG), quarentena, criptografar, aplicar DRM ou aplicar marca d'água e rastreamento de arquivos. A integração fácil com o Forcepoint Enterprise DLP oferece segurança de dados em todos os lugares — no endpoint, na rede, na web e em serviços de nuvem.	→ Reduz o risco de vazamento de dados e propagação de malware em trânsito entre usuários e qualquer aplicativo da web ou site. → Facilita a extensão das políticas do Enterprise DLP para canais de SSE.
	Lógica de SASE programável no campo. Monitora, registra e bloqueia opcionalmente qualquer método de solicitação de HTTP/S com base em qualquer parte do método de solicitação.	→ Controle mais detalhado do uso de aplicativos. → Capacidade de bloquear o upload de dados confidenciais como postagens de mensagens.
	O Forcepoint ThreatSeeker oferece uma rede de inteligência de segurança baseada na nuvem que usa vários mecanismos de verificação para fornecer visibilidade em tempo real sobre as últimas tendências de ameaças, incluindo malware, ataques de phishing e ransomware.	→ Operando 24/7, o sistema automatizado distribui inteligência de ameaças para as soluções da Forcepoint em todo o mundo a fim de proteger os dados e aplicativos contra as crescentes ameaças.

ESCOPO	RECURSO	BENEFÍCIO
CASB e ZTNA para aplicativos baseados na web	Proxy reverso sem agente com o AJAX-VM. O proxy reverso é um software que é executado em nossos POPs de núcleo e de borda, enquanto o AJAX-VM é uma camada de abstração de Java Script executada dentro do navegador do usuário final. Ambos trabalham juntos para garantir que o Forcepoint ONE possa gerenciar o tráfego entre qualquer dispositivo e qualquer aplicativo da web gerenciado, sem a necessidade de software de agente rodando no dispositivo.	→ Funciona com qualquer aplicativo baseado na web, incluindo aplicativos de cauda longa e personalizados que outras soluções de proxy reverso não podem suportar. → Nenhuma instalação de agente é necessária para BYOD ou prestadores de serviços. → Fornece DLP sem agente. → Funciona com qualquer dispositivo que suporte um navegador moderno.
SWG	Monitora, registra e controla o acesso a qualquer website de endpoints Windows e Mac corporativos localizados em qualquer lugar com DLP e checagem de malware, usando as engines de verificação em tempo real do Forcepoint ONE.	→ Aplica política de uso aceitável. → Monitora o uso de shadow IT. → Controla o acesso até o nível do caminho do diretório da URL. → Bloqueia o upload de dados confidenciais para qualquer site. Bloqueia o download de malware de qualquer site. → A arquitetura de aplicação distribuída reduz o tráfego por meio do backplane do Forcepoint ONE e resulta em taxa de transferência com velocidade próxima a do fio.
CASB	DLP e verificação de malware para dados em repouso na nuvem. Verifica os dados estruturados e não estruturados em armazenamento de SaaS e IaaS para detectar malware ou dados confidenciais, e registra e realiza a ação de proteção apropriada, como quarentena, criptografia ou remoção do compartilhamento público.	→ Verifica os dados históricos não apenas os arquivos adicionados recentemente. → Aplica OCR a arquivos de imagem para detectar dados de texto confidenciais. Desativa o compartilhamento público de arquivos que contêm dados confidenciais. Coloca em quarentena o malware armazenado na nuvem. → A extensa biblioteca de padrões de dados predefinidos reduz o tempo de configuração.

ESCOPO	RECURSO	BENEFÍCIO
CASB	Criptografia de dados. Criptografa dados confidenciais estruturados e não estruturados em SaaS e IaaS gerenciados.	→ Garante que os dados confidenciais sejam visíveis apenas para usuários autorizados.
	Descoberta e controle de shadow IT.	→ Use registros de firewalls corporativos e servidores de proxy para descobrir o uso de shadow IT. → Bloqueie os usuários de usar qualquer aplicativo de shadow IT enquanto fornece uma mensagem de treinamento recomendando uma alternativa sancionada pela empresa.
CSPM	Cloud Security Posture Management. Verifica a configuração de ajustes de segurança para AWS, GCP e SaaS do console de administração do Azure de acordo com várias linhas de base do setor e regionais, bem como linhas de base personalizadas.	→ Sinaliza a configuração de risco para correção. Aplique correção por um clique ou correção automatizada, quando aplicável.
SSPM	Gerenciamento de postura de segurança de SaaS. Verifica a configuração de ajustes de segurança para inquilinos de SaaS populares de acordo com várias linhas de base do setor e regionais, bem como linhas de base personalizadas.	→ Sinaliza a configuração de risco para correção. Aplique correção por um clique ou correção automatizada, quando aplicável.
AMDP	Complementa o SWG para analisar o comportamento de arquivos em um ambiente de sandbox para detectar e prevenir malwares.	→ Protege contra downloads de malware e ransomware.
RBI com CDR	Remote Browser Isolation RBI) com Content Disarm and Reconstruction (CDR) O Forcepoint ONE Web Security vem com um nível "essencial" de RBI para sites "não categorizados" e "recém registrados", que podem ser expandidos com licenças opcionais para o RBI para cobrir mais categorias da Web. Fornece uma camada de abstração, rodando um navegador em uma VM hospedada na nuvem, separando o dispositivo do usuário final do risco de malware transmitido pela Web. Quando o usuário baixa um documento ou arquivo de imagem, o CDR é aplicado, extrai as informações de negócios válidas do arquivo, verifica se as informações extraídas estão bem estruturadas e, em seguida, cria um arquivo novo para transportar as informações ao seu destino.	→ A experiência de navegação na web é a mesma que sempre foi. → Capacidade para renderizar um conjunto abrangente de destinos da web—desde apps de nuvem modernos, como o Google Workspace, até sites desenvolvidos com tecnologias antigas. → Mantém os dados confidenciais de apps da web fora de caches de navegadores BYOD, limita as funções de compartilhamento de dados em websites e integra-se com DLP líder de mercado. → Os arquivos processados pelo CDR estão livres de malware. Isso inclui remoção de malware incorporado em arquivos de imagem usando esteganografia.