Forcepoint

Datasheet

Forcepoint DLP

Data Loss Prevention líder do setor com gerenciamento unificado em todos os canais

A segurança de dados é importantíssima, mas não precisa ser complicada. Hoje em dia, equipes híbridas são a realidade. Isso requer acesso a informações confidenciais de qualquer dispositivo, em qualquer local. O Forcepoint Data Loss Prevention (DLP) simplifica a proteção de dados para empresas modernas, oferecendo prevenção abrangente contra perda de dados on-premises sem sacrificar desempenho ou produtividade.

Com visibilidade profunda sobre movimentação de dados em endpoints, redes e armazenamento, o Forcepoint DLP protege seus ativos críticos e garante conformidade regulatória. Oferece a capacidade exclusiva de estender políticas do Forcepoint Security Manager (FSM) para canais adicionais, permitindo proteção de dados perfeita em aplicativos SaaS de nuvem e na web, garantindo aplicação de políticas consistentes e unificadas. Beneficie-se de análises forenses avançadas, integração perfeita, escalabilidade e uma solução que evolui com as necessidades de seus negócios.

Agilize a conformidade de dados

- → **Regule a cobertura** para atender e manter a conformidade com mais de 1.800 modelos, políticas e classificadores predefinidos, incluindo mais de 70 que cobrem IDs, credenciais, chaves e tokens específicos de países, aplicáveis às demandas regulatórias de mais de 90 países e mais de 160 regiões.
- → **Localize e corrija dados regulamentados** com descoberta de rede, nuvem e endpoint.
- → **Controle central** e políticas consistentes em todos os canais, incluindo nuvem, endpoint, rede, web e e-mail.

Forneça proteção de dados abrangente

- → **Descubra e controle dados** onde quer que estejam, seja na nuvem ou na rede, por e-mail ou no endpoint.
- → **Treine os funcionários** para que tomem decisões inteligentes, usando mensagens que orientam as ações dos usuários, educam os funcionários sobre políticas e validam a intenção do usuário ao interagir com dados críticos.
- → **Colabore com segurança** com parceiros confiáveis usando criptografia automática baseada em políticas, protegendo dados movimentados fora de sua organização.
- → **Automatize a rotulagem e a classificação de dados** por meio da integração com o Forcepoint Data Classification, bem como com o Microsoft Purview Information Protection.

Utilize recursos e controles avançados

- **O Reconhecimento óptico de caracteres (OCR)** incorporado ao mecanismo de políticas identifica os dados em imagens enquanto estão em repouso ou em movimento em implementações on-premises e na nuvem, simplificando a infraestrutura e garantindo uma aplicação híbrida consistente.
- **Identificação robusta** para Informações de Identificação Pessoal (PII, Personally Identifiable Information) oferece verificações de validação de dados, detecção de nome verdadeiro, análise de proximidade e identificadores de contexto.
- **Identificação de criptografia personalizada** expõe dados ocultos da descoberta e controles aplicáveis.
- **Análise cumulativa** para detecção de drip DLP (ou seja, dados que vazam lentamente ao longo do tempo).
- **Varredura avançada de arquivos** detecta a exfiltração parcial de dados ao examinar seções aleatórias de arquivos grandes, evitando que exfiltradores ocultem informações confidenciais.
- **Integração com a Forcepoint Data Classification**, aproveitando modelos de AI/LLM altamente treinados para fornecer uma classificação precisa para dados em uso e dados armazenados com o Forcepoint Data Security Posture Management (DSPM).
- **IA generativa avançada** permite que os usuários treinem o sistema e construam um modelo de IA de autoaprendizagem, encontrando, categorizando e classificando automaticamente todos os seus dados para economizar tempo e aumentar drasticamente a precisão.
- **Impressão digital** de dados estruturados (como bancos de dados) e não estruturados (como documentos) permite que os proprietários de dados definam tipos de dados e identifiquem correspondências completas e parciais entre documentos de negócios, planos de design e bancos de dados, e depois apliquem o controle ou a política correta, de acordo com os dados.
- Com o **Risk-Adaptive Protection**, o Forcepoint DLP se torna ainda mais eficaz, pois aproveita a análise de comportamento para entender o risco do usuário. Esse risco é usado para implementar a aplicação de políticas automatizadas com base no nível de risco do usuário.

Encontre e mitigue riscos de proteção de dados

- **Concentre as equipes de resposta** no maior risco com incidentes priorizados que destacam as pessoas responsáveis pelo risco, os dados críticos em risco e padrões comuns de comportamento entre os usuários.
- **Use a ferramenta de ajuda Smart Search com tecnologia de IA** integrada diretamente à solução para encontrar rapidamente informações de suporte específicas sem sair da console de gestão.
- **Aumente a conscientização dos funcionários** sobre tratamento de dados confidenciais e IP com treinamento de funcionários em Windows e macOS, além de habilitar os funcionários com soluções de classificação, como Forcepoint Data Classification e Microsoft Purview Information Protection.
- **Aplique recursos avançados de identificação de dados DLP**, como impressão digital, em endpoints de trabalho remoto e em aplicativos de nuvem corporativa.
- **Capacite os proprietários de dados e gerentes de negócios** com um fluxo de trabalho de incidentes distribuídos baseado em e-mail para analisar e responder a incidentes de DLP.
- **Proteja a privacidade do usuário** com opções de anonimato e controles de acesso.
- **Adicione o contexto dos dados** a análises de usuários mais amplas por meio de integrações profundas com o Forcepoint Risk-Adaptive Protection.
- **As integrações de identidade** suportam o Entra ID nativo da nuvem tanto para acesso administrativo quanto para a aplicação de políticas de usuários finais, aumentando a consistência da segurança e simplificando a gestão.

Tenha visibilidade dos seus dados em qualquer lugar

- → **Capacite os administradores** para identificar e proteger dados em aplicativos de nuvem, armazenamentos de dados de rede, bancos de dados e endpoints gerenciados e não gerenciados.
- → **Identifique e previna automaticamente o compartilhamento** de dados confidenciais com usuários externos ou usuários internos não autorizados.
- → **Proteja dados em tempo real** para uploads e downloads de aplicativos de nuvem importantes, incluindo Office 365, Teams, SharePoint, OneDrive, Salesforce, Box, Dropbox, Google Apps, AWS, ServiceNow, Zoom, Slack e muitos mais.
- → **Unifique a aplicação de políticas** usando um único console para definir e aplicar políticas de dados em movimento, e descoberta de dados, em todos os canais – nuvem, rede, endpoints, web e e-mail.
- → **Mantenha a propriedade dos dados** com uma solução DLP on-prem e opções híbridas para estender recursos avançados, como impressão digital, machine learning e aplicação de políticas, para aplicativos de nuvem e canais da web. Ideal para setores altamente regulamentados, garante a soberania dos dados, mantendo com segurança dados de incidentes e análises forenses em seu data center, apoiando os requisitos de conformidade.
- → **Visualize e gerencie incidentes usando ferramentas de terceiros** por meio de APIs REST expostas. Automatize fluxos de trabalho para gerenciamento de incidentes e forneça suporte a processos de negócios que dependem de incidentes de DLP por meio de ferramentas de automação e serviço, como ServiceNow, Nagios e Tableau, bem como soluções SIEM/SOAR, como Splunk e XSOAR.

Para mais informações sobre nossas soluções Enterprise DLP, solicite uma demo.

Apêndice A: visão geral dos componentes da solução DLP

Forcepoint DLP Endpoint	A Forcepoint DLP Endpoint protege seus dados críticos em endpoints Windows e Mac dentro e fora da rede corporativa. Inclui proteção e controle avançados para dados armazenados (descoberta), em movimento e em uso. Integra-se ao Microsoft Azure Information Protection para analisar dados criptografados e aplicar controles DLP apropriados. Habilita a autocorreção do risco de dados pelos funcionários, com base em orientação de diálogos de orientação de DLP. A solução monitora uploads da web, incluindo HTTPS, bem como uploads para serviços de nuvem, como Office 365 e Box Enterprise. Inclui OCR incorporado no mecanismo de políticas, fornecendo visibilidade dos dados em imagens. Integração completa com Outlook, Notes e clientes de e-mail.
Forcepoint CASB	Equipado com o Forcepoint CASB, estenda as análises avançadas e o controle unificado do Forcepoint DLP para aplicativos de nuvem aprovados, incluindo Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack e muitos outros. Obtenha controle contínuo de dados críticos para negócios, não importa onde os usuários estejam ou qual dispositivo usam.
Forcepoint Web Security	O Forcepoint Web Security permite acessar qualquer site ou fazer download de qualquer documento com segurança, mantendo o desempenho de web de alta velocidade que a sua equipe precisa. Integração com RBI para renderização de contêiner seguro de sites arriscados e Zero Trust CDR para limpeza completa de todos os documentos para download.
Forcepoint DLP Discover	A Forcepoint DLP Discovery identifica e protege dados confidenciais em servidores de arquivos, SharePoint (on-premises e nuvem), Exchange (on-premises e nuvem), e detecção em bancos de dados, como SQL Server e Oracle. A tecnologia de impressão digital (fingerprinting) identifica dados regulados e propriedade intelectual armazenados, protegendo esses dados com criptografia e controles apropriados. Inclui OCR incorporado no mecanismo de políticas, fornecendo visibilidade dos dados em imagens.
Forcepoint DLP Network	O Forcepoint DLP Network oferece o ponto de aplicação crítico para impedir o roubo de dados em movimento por e-mail, canais da web e FTP. A solução ajuda a identificar e evitar a exfiltração de dados e perda de dados acidental por conta de ataques externos ou ameaças internas. OCR incorporado ao mecanismo de políticas, fornecendo visibilidade dos dados em imagens. O Analytics fornece o Drip DLP para impedir o roubo de dados um registro de cada vez, bem como outros comportamentos de usuário de alto risco.
Forcepoint DLP for Cloud Email	O Forcepoint DLP for Cloud Email impede a exfiltração indesejada de seus dados e de seu IP por meio de e-mail de saída. Você pode combinar com outras soluções Forcepoint DLP para canais, como Endpoint, Rede, Nuvem e Web para simplificar seu gerenciamento de DLP, escrevendo uma política e implantando essa política em vários canais. Ao contrário de soluções fora da nuvem, o Forcepoint DLP for Cloud Email permite um enorme potencial de escalabilidade contra surtos imprevistos de tráfego de e-mail. Inclui OCR para fornecer aplicação consistente em implementações híbridas. Também permite que o tráfego de e-mails de saída cresça junto com os seus negócios, sem precisar configurar e administrar recursos de hardware adicionais.
Forcepoint DLP App Data Security API	O Forcepoint DLP App Data Security API facilita a proteção de dados para as organizações em seus aplicativos e serviços personalizados internos. Permite a análise de tráfego de arquivos e dados e aplica ações de DLP, como permitir, bloquear, solicitar confirmação com um pop-up personalizado, criptografar, cancelar compartilhamento e quarentena. É uma API REST fácil de entender e simples de usar, sem necessidade de treinamento extenso ou conhecimento de protocolos complexos. Também é neutra em relação à linguagem, permitindo desenvolvimento e consumo em qualquer linguagem de programação ou plataforma.

Apêndice B: visão geral dos componentes da solução DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT CASB	FORCEPOINT WEB SECURITY	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
Qual é a função principal?	Descoberta de dados e aplicação de políticas de proteção de dados no endpoint do usuário por meio de aplicativos, web, impressão, mídias removíveis e outros.	Descoberta de dados e aplicação de políticas na nuvem ou com aplicativos entregues na nuvem	Visibilidade e controle para dados em trânsito por e-mail externo	Descoberta, exame e correção de dados armazenados em datacenters e outros ambientes on-prem	Visibilidade e controle para dados em trânsito por web e webmail na rede	Visibilidade e controle para dados em trânsito por web e webmail na rede	Visibilidade e controle de dados em aplicativos e serviços personalizados internos
Onde os dados são descobertos/ protegidos quando armazenados?	Endpoints Windows Endpoints MacOS	OneDrive, Sharepoint Online, Exchange Online, Google Drive, Box, DropBox, Salesforce, ServiceNow	Servidores de arquivos e armazenamentos de rede on-premises, servidor Sharepoint, servidor Exchange, bancos de dados como Microsoft SQL Server, Oracle e IBM DB2				
Onde os dados em trânsito são protegidos?	E-mail, Web: HTTP(S), Impressoras, Mídia removível, Servidores de arquivos / NAS	Uploads, downloads e compartilhamento para Office 365, Google Apps, Salesforce.com, Box, Dropbox e ServiceNow via API e TODOS os outros principais aplicativos via proxy	HTTP(S)		E-mail, Impressoras, FTP, Web: Http(S), ICAP	Email	Aplicativos personalizados internos e serviços personalizados
Onde os dados em uso são protegidos?	Zoom, Webex, Google Hangouts, mensagens instantâneas, compartilhamentos de arquivos VOIP, compartilhamentos do M365 Teams, aplicativos (clientes de armazenamento de nuvem), área de transferência do sistema operacional	Durante atividades de criação, modificação e colaboração usando aplicativos de nuvem					Aplicativos personalizados internos e serviços personalizados

Apêndice B: comparação de recursos de componentes da solução DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT CASB	FORCEPOINT WEB SECURITY	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
Risk-Adaptive Protection	Add-on		Add-on; atualmente suportados com túneis GRE/ IPSec com Forcepoint Web Security	Add-on	Add-on	Add-on	
Reconhecimento óptico de caracteres				Incluído	Incluído	Incluído	
Integrações de classificação e Data Classification	Forcepoint Data Classification e Microsoft Purview Information Protection.						
Quais dados podem receber impressão digital?	Dados estruturados (bancos de dados), não estruturados (documentos), binários (arquivos não textuais)						
Administração unificada de políticas	Configuração e aplicação de políticas com console único dos endpoints para aplicativos de nuvem						
Biblioteca robusta de políticas	Descoberta e aplicação da maior biblioteca de políticas de conformidade do setor						